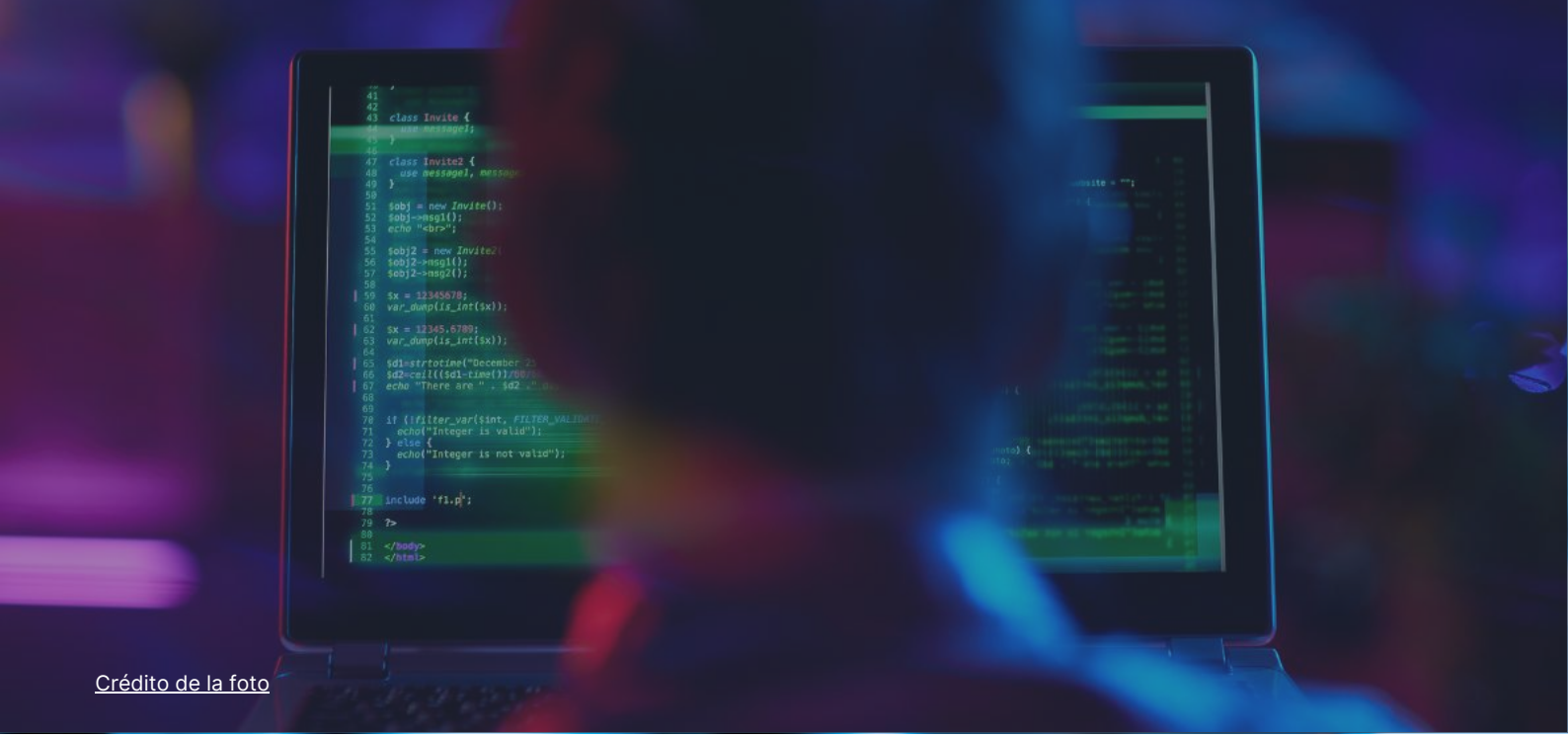
Timly

Gestión de activos de ciberseguridad y cumplimiento

Inventario centralizado para reducir riesgos y facilitar auditorías

Crédito de la foto

El índice



Crédito de la foto

Introducción y objetivos del informe

Si no sabes qué activos tienes, no puedes protegerlos. Esta es precisamente la realidad en muchas empresas hoy en día: existen inventarios, pero están fragmentados, desactualizados o carecen de contexto de seguridad.

El resultado son puntos ciegos en la superficie de ataque, respuestas tardías ante incidentes y evidencias de cumplimiento que requieren un esfuerzo considerable de recopilación. Este informe muestra por qué un inventario centralizado de activos constituye la base operativa de una ciberseguridad eficaz y cómo puedes construirlo y gestionarlo en la práctica.

1.1 Por qué la gestión de activos de ciberseguridad es ahora un tema prioritario

La superficie de ataque de las empresas crece más rápido de lo que muchos modelos de seguridad y de operaciones pueden seguir. Además de los activos de TI clásicos, como portátiles, servidores y componentes de red, hoy también forman parte del panorama real de seguridad los recursos en la nube, aplicaciones de software ofrecido como servicio (SaaS), identidades, proveedores externos, dispositivos IoT y sistemas OT conectados.

En sectores como TI, construcción, fabricación, gestión de instalaciones (facility management) y servicios técnicos, esto da lugar a entornos muy dinámicos, con ubicaciones cambiantes, dispositivos móviles, infraestructuras temporales y responsabilidades compartidas entre TI, operaciones y áreas de negocio.

El problema de fondo rara vez es únicamente la falta de tecnología. En muchas empresas ya existen inventarios aislados, bases de datos de gestión de la configuración (CMDB), escaneos de red, portales en la nube o herramientas de seguridad para endpoints. Sin embargo, las preguntas clave siguen quedando a menudo sin respuesta: **¿qué activos relevantes para la seguridad existen realmente, a quién pertenecen, cuán críticos son y en qué estado de seguridad se encuentran en este momento?**

Precisamente esta brecha convierte una simple gestión de inventario en un tema clave de ciberseguridad. Esta importancia también queda reflejada en los datos.

- Según el «Data Breach Investigations Report 2025» de Verizon, el 46 % de los sistemas comprometidos con posibles credenciales corporativas en un conjunto de datos analizado no **están integrados en la gestión central de la empresa.**[1]

- El «Cost of a Data Breach Report 2025» de IBM indica además que el 40 % de las brechas de datos analizadas afectan a datos en varios entornos, y que estos casos tardan de media 283 días en identificarse y contenerse.[2]

Un ejemplo sencillo muestra por qué esto es tan importante: un acceso sospechoso, por ejemplo, a través de un sistema externo o de una cuenta en la nube mal inventariada, deja claro de inmediato hasta qué punto la transparencia sobre todos los activos es decisiva.

Sin una vista centralizada de los activos, el equipo de respuesta a incidentes carece de respuestas claras a preguntas como: ¿qué sistemas están afectados, quién es responsable, qué datos se ven implicados y qué debe aislarse? Esto retrasa la reacción y aumenta el riesgo. Con un registro de activos sólido, en cambio, puedes identificar los sistemas afectados de forma inmediata, priorizarlos y asignarlos a sus responsables.

La siguiente ilustración muestra cómo la información sobre el estado de los parches, la criticidad, los segmentos, las identidades, las interfaces y las ubicaciones pasa a estar disponible de forma centralizada, lo que permite una respuesta rápida y auditable.

Así, la gestión de activos de ciberseguridad deja de ser una disciplina marginal de la inventarización para convertirse en un requisito clave para reducir eficazmente el riesgo, garantizar una respuesta sólida ante incidentes y asegurar un cumplimiento normativo robusto.

1.2 A quién va dirigido este informe

Este informe está dirigido a **empresas que quieren basar sus procesos de seguridad y cumplimiento en una gestión de activos sólida y fiable**.

Resulta especialmente relevante para los siguientes perfiles:

- CISO y responsables de ciberseguridad
- Dirección de TI y equipos de operaciones de TI
- Responsables de OT y de producción
- Dirección de gestión de instalaciones
- Responsables de cumplimiento normativo, riesgos y auditoría
- Equipos de auditoría interna y de gobierno corporativo

En muchos casos, los estándares básicos de seguridad y los requisitos regulatorios, como ISO 27001, NIS2 o normativas sectoriales específicas, ya se conocen y están, al menos en teoría, implementados. **Lo que suele faltar es un enfoque pragmático sobre cómo construir y operar en la práctica un inventario de activos completo y seguro**. En este punto es donde entra en juego este informe.

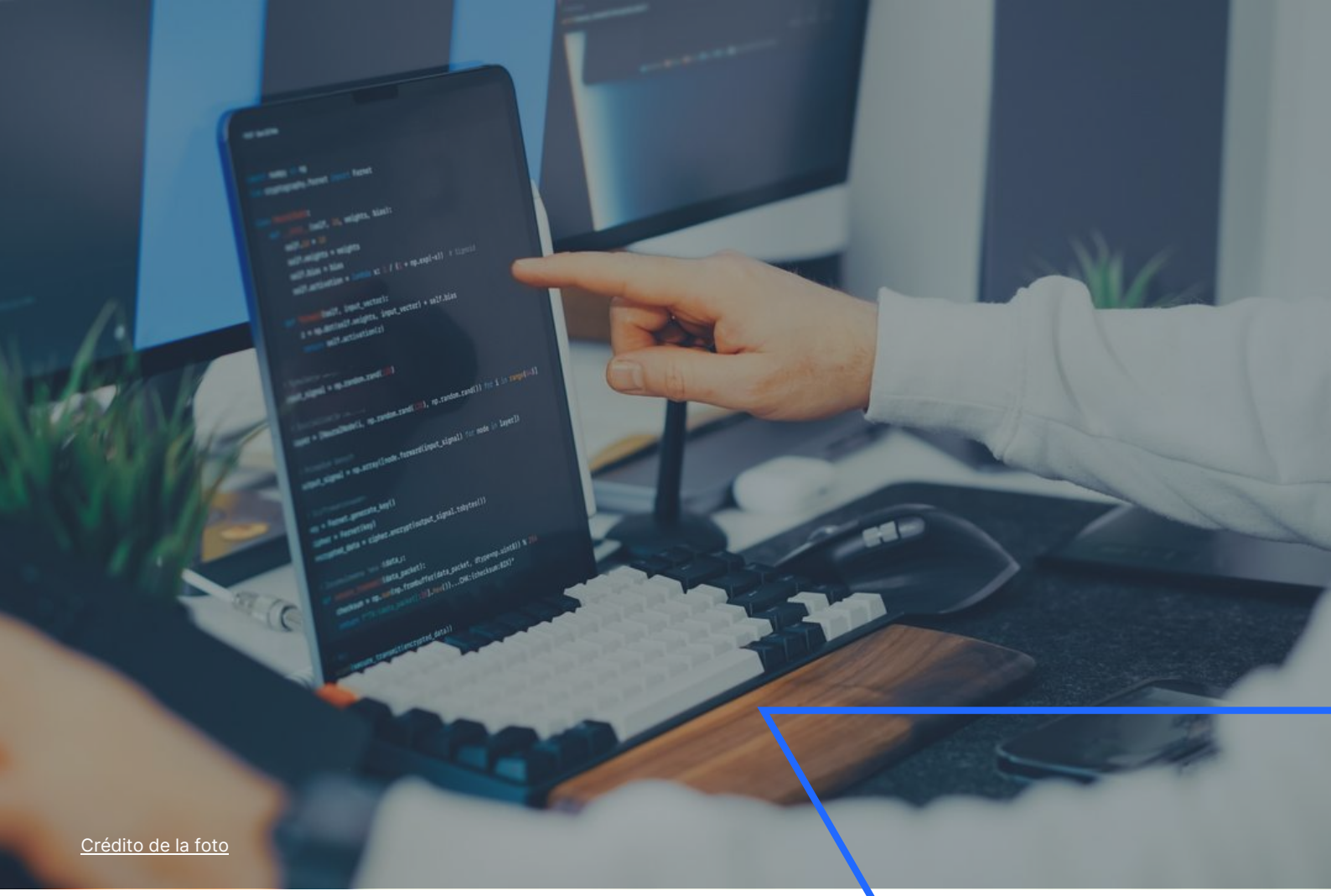
Integra perspectivas técnicas, organizativas y de procesos, y muestra cómo las empresas pueden establecer un registro centralizado de activos como fundamento de su estrategia de seguridad.

1.3 Objetivos y estructura del informe

El informe muestra por qué un inventario de activos incompleto no es solo un problema de gestión, sino también un **factor de riesgo directo para la ciberseguridad y el cumplimiento normativo**. Explica por qué los activos desconocidos, la falta de responsables claros y los datos de inventario fragmentados debilitan la gestión de parches, la respuesta a incidentes, la capacidad de auditoría y el reporting a la dirección.

A partir de ahí, el informe detalla **qué requisitos derivan de las normas y de los marcos regulatorios** para contar con un registro de activos sólido y, además, ofrece un objetivo pragmático y alcanzable para construirlo: con clases de activos relevantes, roles y responsabilidades definidos, un modelo de madurez sencillo, procesos de seguridad clave y ejemplos de KPI. En las secciones siguientes, a partir de esta base, se presenta un plan de 90 días con el que las empresas pueden evaluar su nivel de madurez actual y priorizar mejoras concretas.

Crédito de la foto



Crédito de la foto

¿Qué es la gestión de activos de ciberseguridad (CSAM)?

Conceptos y alcance

¿Qué es la gestión de activos de ciberseguridad (CSAM)? Conceptos y alcance

Antes de poder construir un registro de activos, es necesario tener una respuesta clara a la pregunta: ¿qué se incluye exactamente en la gestión de activos de ciberseguridad y en qué se diferencia de la gestión tradicional de activos de TI?

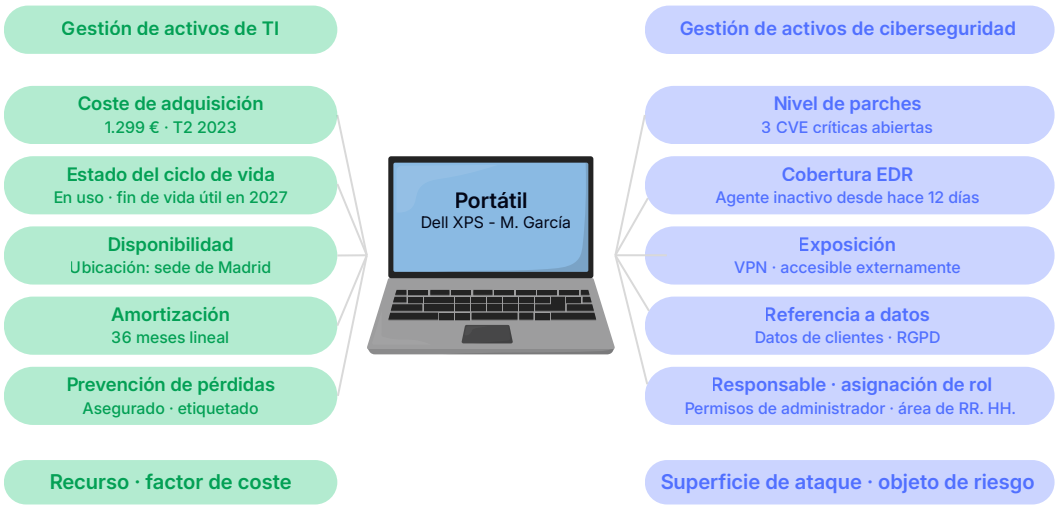
2.1 Definición y delimitación

> La gestión de activos de ciberseguridad es el proceso continuo de identificar, registrar y clasificar todos los activos relevantes para la seguridad de una empresa, asignarles responsables y vincularlos con información de seguridad y de riesgos.

A diferencia de la gestión tradicional de activos de TI (ITAM), el foco no está en el ciclo de vida operativo o financiero, sino en comprender qué riesgos, dependencias y superficies de ataque están asociados a cada activo.

Mientras que ITAM se centra principalmente en los activos como recursos operativos o elementos de coste, el CSAM amplía esta perspectiva incorporando el contexto de seguridad y cumplimiento, como el estado de los parches, la exposición, la criticidad, las identidades, las vulnerabilidades o las responsabilidades. De este modo, un dispositivo gestionado pasa a convertirse en un objeto de seguridad controlable.

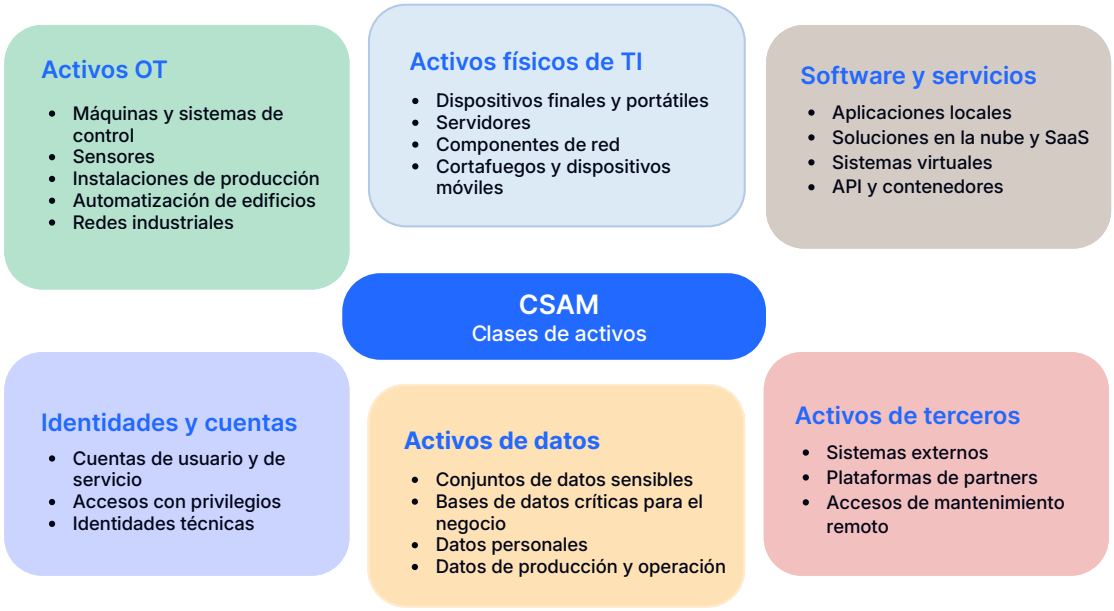
La siguiente ilustración muestra este cambio de perspectiva mediante un ejemplo concreto: mientras que, en el contexto de ITAM, un portátil se considera principalmente un dispositivo operativo gestionado, en el contexto de CSAM el foco se sitúa en su perfil de seguridad y riesgo, como la responsabilidad, el estado de los parches, la exposición o los controles de seguridad existentes.



2.2 ¿Qué clases de activos abarca el alcance?

Una gestión de activos de ciberseguridad eficaz abarca mucho más que los dispositivos finales clásicos o los servidores. En términos generales, deben registrarse todos los objetos que puedan generar riesgos de seguridad, de cumplimiento o de operación.

Las clases de activos típicas en el CSAM son las siguientes:



Lo importante no es únicamente que el activo exista, sino comprender su contexto.

- Criticidad
- Responsabilidad
- Estado de seguridad
- Dependencias
- Relevancia para el cumplimiento

Solo así una simple lista de inventario se convierte en un registro de activos fiable.

2.3 Roles y responsabilidades en el CSAM

Un registro central de activos solo funciona de forma fiable si **las responsabilidades correspondientes están claramente definidas**. Cada activo y objeto relevante para la seguridad necesita un responsable claro, ya sea a nivel funcional, técnico u organizativo; si falta esta asignación, el mantenimiento será incompleto y la reacción ante cambios o incidentes se retrasará.

Una gestión de activos de ciberseguridad eficaz distribuye las responsabilidades de forma consciente entre **niveles estratégicos, operativos y de control**. La siguiente ilustración muestra un modelo de roles típico en el que convergen estos niveles.

En este modelo, el CSAM conecta el papel estratégico del CISO y del área de seguridad de TI con las tareas operativas de los equipos de TI/OT y de las unidades de negocio, así como con la función de control de los equipos de cumplimiento normativo y de auditoría interna.

En la ilustración, el color ámbar marca las responsabilidades operativas y de control descentralizadas, mientras que el verde indica las responsabilidades estratégicas y operativas centrales.

¿Qué es la gestión de activos de ciberseguridad (CSAM)?

Conceptos y alcance

Modelo de roles en la gestión de activos de ciberseguridad

CSAM integra responsabilidades estratégicas, operativas y de control en un modelo común.

2.4 Modelo de madurez para la gestión de activos de ciberseguridad

Las empresas modernas se encuentran en niveles de desarrollo muy distintos en lo que respecta a la gestión de activos de ciberseguridad. Por eso, antes de implantar nuevas soluciones de software, merece la pena analizar en qué estado se encuentra actualmente la organización. **Un modelo de madurez sencillo ayuda a situar de forma realista el punto de partida propio**.

Nivel 1 – Fragmentado

- Los datos de activos se encuentran en archivos de Excel o en herramientas aisladas
- No existe una visión completa de los sistemas de TI y OT
- Las responsabilidades son poco claras o inexistentes
- Los datos suelen estar desactualizados

Pregunta típica:

«¿Podemos afirmar con seguridad qué sistemas existen realmente?»

Nivel 2 – Consolidado

- Existen primeros inventarios centrales o estructuras de CMDB
- Captura parcialmente automatizada de activos
- Se integran datos de seguridad básicos
- Aun así, persisten lagunas y roturas de medios

Pregunta típica:

«¿Son nuestros datos lo suficientemente actuales y completos para tomar decisiones de seguridad?»

Nivel 3 – Gestionado

- Los procesos y responsabilidades están claramente definidos
- Los KPI de seguridad se supervisan de forma activa
- Los datos de activos respaldan los procesos de parcheo, riesgo e incidentes
- Existen controles de calidad periódicos

Pregunta típica:

«¿Podemos identificar los activos afectados en un incidente en un plazo breve?»

Nivel 4 – Integrado

- La gestión de activos está plenamente integrada en los procesos de seguridad y cumplimiento
- Alta calidad de los datos y actualización continua
- Flujos de trabajo y procesos de gobierno automatizados
- Evidencias auditables disponibles en todo momento

Pregunta típica:

«¿Estamos utilizando los datos de activos de forma activa para gestionar riesgos y cumplimiento?»

Crédito de la foto

Gestión de activos de ciberseguridad

Ámbito del problema y contexto

Gestión de activos de ciberseguridad: Ámbito del problema y contexto

En la mayoría de las empresas no falta información, sino consolidación. Las CMDB, las herramientas de descubrimiento, los portales en la nube y las listas locales suelen coexistir en paralelo sin que exista una visión global coherente. Al mismo tiempo, los entornos de TI y OT crecen más rápido de lo que pueden actualizarse los inventarios: nuevas sedes, recursos en la nube de corta duración, proveedores externos y dispositivos no gestionados.

El resultado son responsabilidades poco claras, crecientes puntos ciegos de seguridad y una superficie de ataque que casi nadie puede abarcar por completo. Este capítulo muestra dónde fallan los enfoques clásicos y qué riesgos concretos se derivan de ello.

3.1 Creciente complejidad de los entornos de TI y OT

La mayoría de las empresas ya no operan en un mundo de TI claramente delimitado y controlado de forma centralizada. En su lugar, sus entornos están formados por una **combinación de TI de oficina fija, servicios en la nube, dispositivos móviles, plataformas SaaS, identidades, infraestructuras de red y accesos de socios y, según el sector, también por componentes OT** como máquinas, sistemas de control, sensores o automatización de edificios. Esta heterogeneidad es especialmente marcada en sectores como la construcción, la fabricación, la gestión de instalaciones y las organizaciones de servicios técnicos.

A esto se suma la **dinámica operativa**. Se ponen en marcha nuevas obras, se crean redes temporales, los proveedores obtienen acceso, se utilizan nuevas herramientas SaaS sin aprobación central, se aprovisionan recursos en la nube a corto plazo y los sistemas existentes permanecen en uso más tiempo del planificado inicialmente. Como resultado, los conjuntos de activos cambian de forma constante, a menudo más rápido de lo que pueden actualizarse los inventarios centrales o los procesos de gobierno.

Esta dinámica genera responsabilidades poco claras y crecientes puntos ciegos de seguridad. Un sistema existe técnicamente, pero no aparece en los registros centrales. Un dispositivo es conocido, pero no está asignado a un responsable actual. Una aplicación está en uso, pero su criticidad o su estado de parches no están documentados de forma fiable. Aquí es donde surge el principal desafío de la gestión de activos de ciberseguridad.

3.2 Por qué los inventarios clásicos (Excel, islas de CMDB, herramientas de red, portales en la nube) ya no son suficientes

En la mayoría de las empresas ya existen numerosas fuentes de datos: desde CMDB y herramientas de descubrimiento hasta plataformas en la nube y de endpoints, pasando por sistemas de gestión de identidades y accesos (IAM) y soluciones de seguridad. El problema no suele ser la falta de información, sino la ausencia de consolidación.

> Los inventarios clásicos suelen fallar no por carencia de datos, sino por su falta de actualización, de consistencia y por la ausencia de un contexto de seguridad adecuado.

Gestión de activos de ciberseguridad: Ámbito del problema y contexto

Como se describió en el capítulo 2.1, el foco del CSAM está en una representación coherente y orientada al riesgo de los activos relevantes para la seguridad. Y precisamente en esto es donde muchos enfoques tradicionales fracasan en la práctica, especialmente cuando las actualizaciones se realizan de forma manual o cuando surgen nuevos tipos de activos fuera de los modelos de datos históricos.

Esto se aprecia con especial claridad en los enfoques centrados en la CMDB: en modelos estáticos o con esquemas rígidos, los activos nativos de la nube (cloud native), de corta duración, externos o cercanos a las unidades de negocio tienden a quedar invisibles.

Al mismo tiempo, a menudo faltan vínculos directos con el estado de los parches, las vulnerabilidades, la exposición, las identidades, el historial de incidentes o la criticidad de los datos. Incluso las plataformas de seguridad suelen ofrecer solo perspectivas parciales sobre los activos y, por tanto, deben consolidarse.

> Un registro central de activos, por ejemplo mediante una solución de gestión de inventario como Timly, crea a partir de todo ello una visión coherente y operativamente utilizable para seguridad, cumplimiento y gobierno corporativo.

3.3 Consecuencias para la seguridad y el cumplimiento

Los atacantes se aprovechan específicamente de los sistemas que no se supervisan, que se han olvidado o que están insuficientemente protegidos. Especialmente críticos son:

- Componentes OT sin una responsabilidad claramente definida
- Sistemas obsoletos
- Dispositivos de red desconocidos
- Servicios en la nube no documentados
- Dispositivos de usuario final no gestionados

Consecuencias típicas:

Alta proporción de activos desconocidos

Las empresas a menudo no pueden determinar de forma fiable qué sistemas están realmente conectados a la red.

Lagunas de auditoría y cumplimiento

Las evidencias sobre la titularidad, las medidas de seguridad o la cobertura deben recopilarse manualmente en muchos casos.

Mayor superficie de ataque

Los activos desconocidos o no gestionados aumentan directamente la superficie de ataque.

Tiempos de respuesta ante incidentes más largos

En caso de incidentes de seguridad, a menudo faltan datos rápidos sobre los sistemas afectados, las responsabilidades y las dependencias.

Cobertura de parches incompleta

Algunos sistemas permanecen sin parchear porque no se conocen o no están claramente asignados a ningún equipo.

La falta de transparencia sobre los activos se convierte así en uno de los factores de riesgo estructurales más importantes en los entornos modernos de TI y OT, con un impacto directo en **la detección de ataques, la velocidad de respuesta y la capacidad de cumplimiento**.

Crédito de la foto

Normas y requisitos regulatorios para el registro de activos

Normas y requisitos regulatorios para el registro de activos

Los requisitos regulatorios para la gestión de activos hace tiempo que han dejado de ser una cuestión futura y abstracta para muchas empresas. Normas y marcos como **ISO 27001, NIS2, KRITIS** y otros marcos normativos tienen algo en común: todas exigen que las organizaciones puedan demostrar qué activos poseen, quién es responsable de ellos y en qué estado de seguridad se encuentran.

Un registro central de activos no es, por tanto, un extra opcional ni algo accesorio sino una condición regulatoria básica. Este capítulo muestra qué exigen concretamente los principales estándares y en qué puntos se solapan sus requisitos.

4.1 ISO 27001: inventario de información y activos

ISO/IEC 27001 deja claro que la seguridad de la información no puede aplicarse de forma eficaz si no se conoce con precisión qué activos deben protegerse. En particular, el Anexo A 5.9 exige la **gestión sistemática del inventario de información y de los activos asociados**, así como la asignación de responsabilidades claras.

Un registro de activos no es, por tanto, una herramienta opcional en el contexto de ISO, sino **un requisito fundamental** para el análisis de riesgos, la definición de medidas de protección y la asignación de responsabilidades dentro de un sistema de gestión de la seguridad de la información (SGSI, por sus siglas en inglés ISMS).

Lo importante no es solo la existencia de un inventario, sino también su calidad. El Anexo A 5.9 presupone que los inventarios se gestionen de forma **consistente, actualizada y trazable a lo largo de todo el ciclo de vida del activo**. En la práctica, esto significa que el registro debe mantenerse de forma rigurosa, contener atributos mínimos definidos y contrastarse periódicamente con otras fuentes de datos.

Un registro de activos sólido, en el sentido de ISO, debería poder responder, entre otras, a las siguientes preguntas:

- ¿Qué activos están incluidos en el alcance del SGSI?
- ¿Quién es responsable de cada activo?
- ¿Cómo se clasifican la criticidad y las necesidades de protección?
- ¿Cómo se registran en el inventario los activos nuevos, modificados o retirados?
- ¿Cómo se vinculan de forma sistemática los datos de los activos con riesgos, controles y evidencias?

Preguntas típicas de auditoría son, por ejemplo:

- ¿Cómo garantizan la integridad y la actualidad del registro de activos?
- ¿Cómo se mantiene la responsabilidad a lo largo de todo el ciclo de vida del activo?
- ¿Qué clases de activos están incluidas en el alcance del SGSI y por qué?
- ¿Cómo se relacionan los datos de los activos con las medidas de gestión de riesgos y de control?

4.2 NIS2: gestión de activos como base para la gestión de riesgos y de incidentes

También los requisitos normativos, como la Directiva europea NIS2, elevan de forma considerable las exigencias en materia de transparencia y gestión de riesgos. La NIS2 no prescribe ninguna herramienta concreta ni un tipo específico de sistema de inventario. Sin embargo, sí exige la implantación de «medidas técnicas y organizativas adecuadas» para gestionar los riesgos de ciberseguridad.[3]

En la práctica, esto presupone una visión **fiable de sistemas, servicios y responsabilidades**. Sin una vista de activos consolidada, solo puede cumplirse de forma limitada con requisitos clave, especialmente en los ámbitos de:

- Evaluaciones de riesgos
- Respuesta a incidentes
- Gestión de vulnerabilidades
- Continuidad de negocio
- Obligaciones de notificación de incidentes

Especialmente relevante es la capacidad de **identificar con rapidez los sistemas afectados en una situación de emergencia**. Las empresas deben poder determinar:

- qué activos se ven afectados
- qué nivel de criticidad tienen
- qué ubicaciones están implicadas
- qué dependencias existen

De este modo, la gestión de activos de ciberseguridad se convierte en un factor clave para la resiliencia regulatoria.

4.3 Otros estándares y requisitos de clientes (visión general)

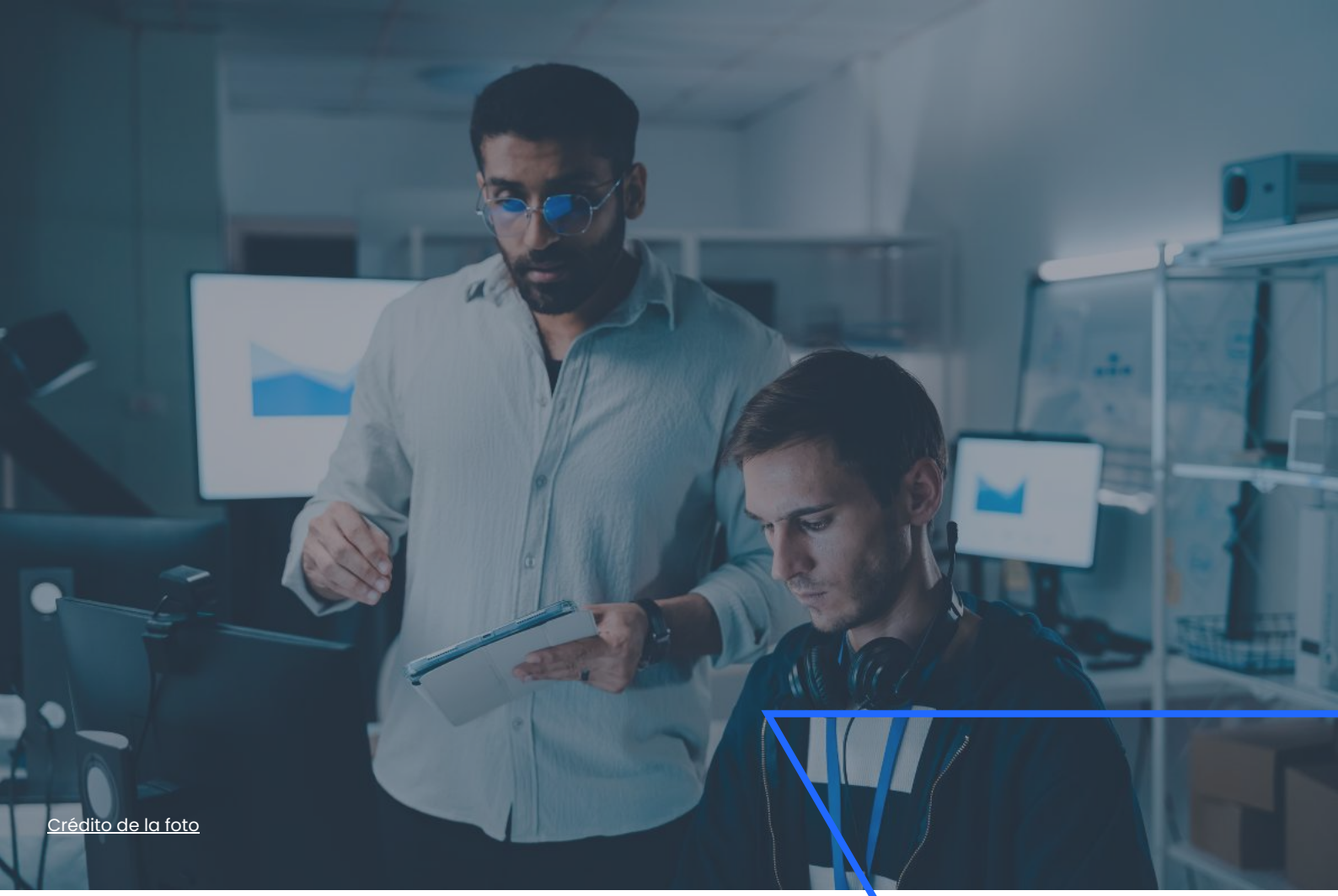
Además de ISO 27001 y de la Directiva NIS2, existen **numerosos estándares** y requisitos de clientes que, de forma indirecta, presuponen un registro de activos sólido. Entre ellos se encuentran, por ejemplo:

- SOC 2
- TISAX
- Estándares de seguridad específicos del sector
- Requisitos derivados de KRITIS
- Auditorías de clientes
- Directrices internas de gobierno corporativo

Aunque los requisitos se formulen de manera diferente, en casi todos los marcos subyace la misma premisa básica: **las empresas deben saber con precisión qué sistemas, datos y accesos poseen realmente** y deben proteger. Un registro central y actualizado de activos se convierte así en la base común para seguridad, cumplimiento normativo y gestión operativa. En organizaciones internacionales se añaden además requisitos específicos de cada país, por ejemplo:

- Requisitos alineados con INCIBE en España
- Requisitos del BSI y de KRITIS en Alemania
- Marcos de referencia de la ANSSI en Francia

Por ello, las empresas necesitan cada vez más un modelo de gestión de activos escalable y estandarizado que pueda dar soporte tanto a la gobernanza global como a las exigencias locales.



Crédito de la foto

Plan de 90 días para un registro de activos orientado a la seguridad

Plan de 90 días para un registro de activos orientado a la seguridad

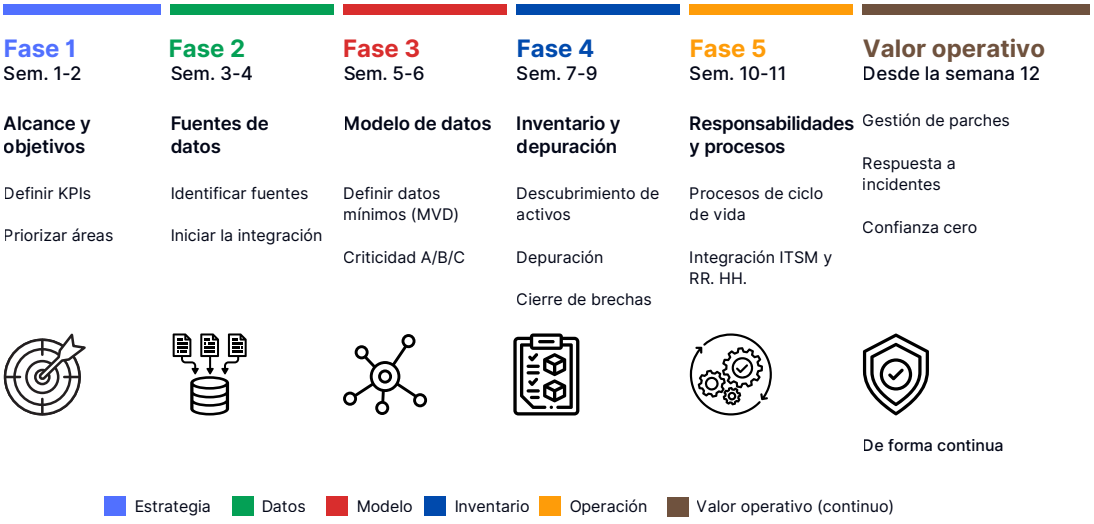
Un registro de activos orientado a la seguridad rara vez surge en la práctica a partir de una única herramienta. Lo decisivo es definir con claridad **qué sistemas se van a inventariar, de dónde proceden los datos, quién es responsable** y cómo se mantiene todo esto en el día a día.

Los activos desconocidos o no gestionados se encuentran entre los problemas de seguridad más frecuentes, como muestra, entre otros, un análisis de Trend Micro.[4] Por eso, la creación de un registro de activos no debe entenderse únicamente como un inventario de TI. El objetivo principal es:

- hacer más visibles las superficies de ataque
- poder reaccionar más rápido ante incidentes
- reducir el esfuerzo necesario en auditorías

El siguiente plan de 90 días ofrece una forma pragmática de empezar. En las primeras 11 semanas (fases 1 a 5) se definen el alcance, las fuentes de datos, el modelo de datos, el inventario y los procesos. A partir de la semana 12, el registro se utiliza de forma continua en la operación de seguridad. Lo importante no es documentar desde el principio cada activo al detalle. La clave es **comenzar con un enfoque basado en riesgos**, centrándose primero en las áreas más críticas desde el punto de vista de la seguridad.

Plan de 90 días: creación de un registro de activos orientado a la seguridad



5.1 Fase 1 – Definir alcance y objetivos (semanas 1–2)

Muchos proyectos fracasan ya en la fase inicial porque se intenta crear desde el principio un inventario completo que abarque todos los sistemas, ubicaciones y clases de activos. En la práctica, esto conduce a largas rondas de coordinación y a un gran esfuerzo antes de que exista un resultado realmente utilizable. **Para un registro de activos orientado a la seguridad, resulta por tanto más adecuado comenzar con un enfoque basado en riesgos**.

Durante las primeras una o dos semanas, el foco debería estar en **definir un alcance claro y establecer objetivos medibles**. En primer lugar, deben incluirse los sistemas y entornos que son especialmente importantes para la detección de ataques, la respuesta a incidentes, la gestión de parches y el cumplimiento normativo.

La siguiente ilustración muestra áreas de inicio típicas que han demostrado su eficacia en la práctica.

Plan de 90 días para un registro de activos orientado a la seguridad

Áreas de inicio típicas para el registro de activos

Sistemas de TI críticos

Servidores
Bases de datos

Dispositivos expuestos

Dispositivos móviles
Dispositivos utilizados en varias ubicaciones

Servicios en la nube

Datos sensibles
Permisos de amplio alcance

Componentes centrales de red

Routers
Switches

Sistemas OT cercanos a la producción

Sistemas de control
Sensores

Cuentas con privilegios elevados

Administradores
Responsables de sistemas

> *«Al principio lo importante no es la exhaustividad, sino la capacidad de integrarse en los procesos existentes. Un conjunto de datos sencillo con responsable, ubicación y nivel de criticidad suele ser suficiente para generar valor en seguridad desde el primer momento.»*
>
> **EQUIPO DE CUSTOMER SUCCESS DE TIMLY**

En entornos distribuidos, como en **la construcción, la fabricación o la gestión de instalaciones, también puede ser útil incluir desde el principio los activos móviles o físicamente dispersos**. Precisamente en estas áreas suelen aparecer problemas de transparencia y responsabilidades poco claras. Paralelamente, los objetivos deben formularse de la forma más concreta posible. Afirmaciones generales como «más transparencia» no son suficientes. **Es más útil definir un pequeño conjunto de indicadores con los que se puedan medir el progreso y el beneficio práctico**. Resultan especialmente valiosos los KPIs que hacen visibles los puntos débiles típicos de un inventario incompleto:

- activos desconocidos
- responsabilidades no asignadas
- estado de parches poco claro
- tiempos de reacción lentos ante incidentes de seguridad

Al inicio basta con un **conjunto reducido de KPIs** que ponga de manifiesto las brechas de transparencia y las mejoras operativas. Estos indicadores deberían reflejar tanto la calidad del registro de activos como el valor práctico que aporta a los procesos de seguridad.

KPI	Por qué es relevante	Valor objetivo práctico
Porcentaje de activos desconocidos	Muestra puntos ciegos y superficie de ataque potencial	< 5 %
Activos con responsable asignado	Requisito para medidas, escalado y evidencias de auditoría	> 90 %
Transparencia de parches	Indica en qué porcentaje de activos se conoce con fiabilidad el estado de los parches.	> 95 %
Activos críticos con clasificación actualizada	Base para priorizar en los procesos de seguridad y de auditoría	> 90 %
MTTR en incidentes de seguridad	Mide la rapidez con la que se identifican los activos afectados y se ponen en marcha	< 4 h (incidentes críticos)

Plan de 90 días para un registro de activos orientado a la seguridad

Estos valores no deben entenderse como un requisito rígido de cumplimiento normativo, sino como una **referencia para los primeros 90 días**. El verdadero valor reside en mostrar desde el principio dónde se encuentran las mayores brechas y si el registro de activos ayuda realmente, en el día a día, a gestionar mejor los procesos de seguridad.

Consejo práctico

Sin un alcance claramente definido, es fácil acabar con un registro lleno de datos pero con poco valor real. Un enfoque basado en riesgos ayuda a cerrar primero las brechas más importantes en cuanto a transparencia y seguridad.

5.2 Fase 2 – Identificar y consolidar fuentes de datos (semanas 3–4)

Una vez definido el alcance, el siguiente paso consiste en **conectar las principales fuentes de datos y reunirlas en una vista común**. Esta fase debería estar completada, por lo general, entre la semana 3 y la semana 4. En la mayoría de las empresas ya existe mucha información sobre los activos, pero repartida entre distintos sistemas, como Active Directory, plataformas en la nube, herramientas de red, sistemas OT o listas de inventario locales.

> *El reto no suele ser la falta de datos, sino agrupar estos fragmentos en una vista consistente.*

Para empezar, basta con **integrar primero las fuentes que aportan mayor valor** para la seguridad y la transparencia. Normalmente se incluyen:

- Active Directory o el proveedor de identidad para usuarios y permisos
- Herramientas de descubrimiento de red para dispositivos activos
- Plataformas en la nube para recursos y servicios virtuales
- Listas de activos o inventarios ya existentes

Estas fuentes ya proporcionan una gran parte de la información relevante para la seguridad y ayudan a hacer visibles los activos desconocidos o no gestionados. La combinación de procedimientos de descubrimiento automatizado, registro manual y escaneo mediante códigos QR o de barras se describe en detalle en la fase 4.

Ejemplo práctico con Timly

Soluciones como Timly permiten combinar datos técnicos de descubrimiento con procesos de inventario móviles, registro mediante códigos QR o de barras e información de activos actualizada de forma sencilla por los equipos, especialmente en entornos distribuidos como la construcción, la producción o la gestión de instalaciones.

El objetivo de esta fase no es recopilar todos los datos posibles, sino disponer de una **vista central y utilizable de los activos más importantes**. Más importante que centralizar toda la información en un único sistema es garantizar que los datos procedentes de distintas fuentes puedan consolidarse de forma consistente.

Consejo práctico

Muchas empresas empiezan con demasiadas integraciones a la vez. Para una primera vista operativa suelen bastar unas pocas fuentes centrales, como Active Directory, el descubrimiento de red, las plataformas en la nube y los inventarios existentes. A partir de ahí, el registro puede ampliarse de forma gradual.

5.3 Fase 3 – Definir modelo de datos y datos mínimos (semanas 5–6)

Una vez integradas las principales fuentes de datos, el siguiente paso consiste en definir **qué información se necesita realmente por cada activo**. Esta fase debería completarse en las semanas 5 y 6. Precisamente en este punto muchos inventarios se vuelven innecesariamente complejos, porque se definen demasiados campos que luego no se mantienen en el trabajo diario.

Para un registro de activos orientado a la seguridad basta, en un primer paso, con un modelo común de datos mínimos: solo se registran aquellos datos que son realmente relevantes para la identificación, la asignación de responsabilidades, la priorización y la gestión de la seguridad.

Este principio puede describirse como «**datos mínimos viables**» (Minimum Viable Data, MVD): tantos datos como sean necesarios, no tantos como sea posible.

Plan de 90 días para un registro de activos orientado a la seguridad

Datos mínimos por activo

Campo mínimo	Por qué es importante
ID del activo o denominación única	Crea una referencia clara y evita duplicados
Tipo de activo	Distingue, por ejemplo, entre TI, OT, software, recursos en la nube o identidades
Ubicación o contexto lógico	Muestra dónde se utiliza un activo o a qué área está asignado
Rol responsable	Aclara la responsabilidad para evaluación, medidas y escalado
Criticidad	Ayuda a priorizar según el riesgo y el impacto en el negocio
Estado de seguridad	Hace visibles, por ejemplo, el estado de parches, el estado de revisión o posibles anomalías
Estado del ciclo de vida	Muestra si un activo está activo, en cambio o fuera de servicio

Estos campos constituyen la base común para los distintos tipos de activos. **Según el entorno, más adelante pueden añadirse otros datos**, como fabricante, número de serie, versión de firmware, clasificación de la información o vulnerabilidades vinculadas.

Entre los campos mínimos más importantes se incluye además una **valoración sencilla de la criticidad**, que ayuda a priorizar los activos de forma adecuada en los procesos de seguridad y de auditoría.

Para empezar, suele bastar con un modelo pragmático de tres niveles:

Niveles de criticidad

Alta criticidad
sistemas centrales, accesos con privilegios elevados, datos sensibles.

Relevante
activos operativos con impacto apreciable en caso de fallo.

De apoyo
activos que deben inventariarse, pero con baja prioridad en el contexto de seguridad.

Esta clasificación crea una base común para las evaluaciones de riesgo, la priorización de parches y la respuesta a incidentes.

La criticidad no depende solo del tipo de activo, sino de su función en el contexto del negocio y de la seguridad. Por eso, dos dispositivos técnicamente similares pueden valorarse de forma diferente, por ejemplo si uno de ellos accede a datos sensibles o soporta un proceso crítico.

Consejo práctico

Unos pocos campos clave bien mantenidos suelen ser, en la práctica, más valiosos que un modelo de datos complejo que nadie utiliza de forma consistente.

5.4 Fase 4 – Realizar el inventario inicial y la depuración (semanas 7–9)

La fase 4 suele abarcar unas tres semanas (de la semana 7 a la 9) y es **la fase con mayor carga de trabajo**. Una vez conectadas las fuentes de datos y definido el modelo mínimo de datos, comienza el inventario propiamente dicho.

En esta etapa se combinan **métodos de registro técnicos y manuales; aquí, la app de inventario de Timly puede ayudar** a construir rápidamente una base inicial de activos utilizable.

La siguiente ilustración muestra métodos de registro típicos y cómo se combinan en esta fase.

MÉTODOS DE REGISTRO EN LA FASE 4

Tras el primer registro, ya sea mediante descubrimiento automático, registro manual o procesos OT independientes, los datos deben depurarse y unificarse. Esto incluye:

- resolver duplicados
- completar campos obligatorios como responsable, criticidad o ubicación
- cerrar lagunas evidentes

El objetivo no es un registro perfecto, sino **una base de trabajo operativa** con la que ya se puedan respaldar de forma útil los procesos de seguridad y cumplimiento. Las lagunas restantes pueden cerrarse de forma gradual una vez que el registro se utilice en el día a día.

Consejo práctico

El primer inventario no tiene por qué ser completo: un registro con alrededor del 80 % de cobertura y datos clave bien mantenidos suele ser más valioso que la aspiración al 100 %, que puede retrasar los proyectos durante meses.

5.5 Fase 5 – Consolidar responsabilidades y procesos (semanas 10–11)

En las semanas 10 y 11 se trata de aclarar las responsabilidades y definir los procesos estándar.

Un registro central de activos solo genera un verdadero valor añadido si está claramente establecido **quién es responsable de cada activo y cuándo deben actualizarse los datos**. Sin responsabilidades vinculantes, incluso los registros inicialmente bien mantenidos se vuelven rápidamente incompletos u obsoletos. Por ello, en esta fase no solo deben definirse los responsables, sino también los procesos clave a lo largo del ciclo de vida de los activos.

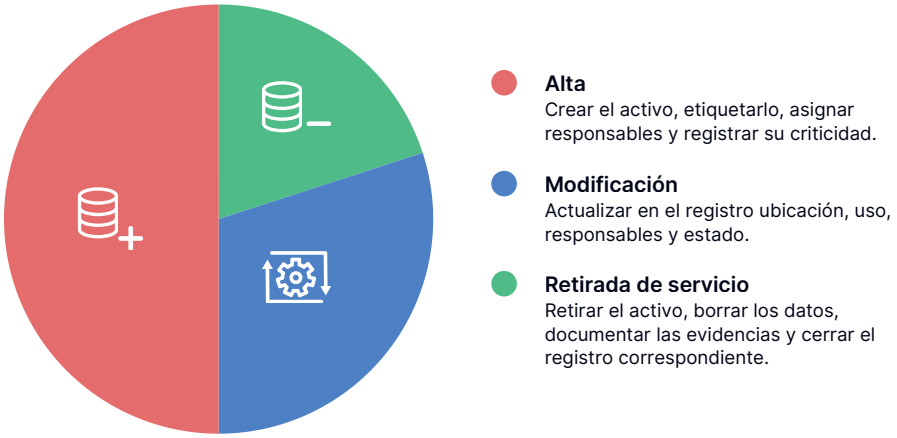
En la práctica, hay tres situaciones decisivas:

1. **Alta (onboarding)**
2. **Modificación**
3. **Retirada de servicio (decommissioning)**

En cada una de estas fases, el registro de activos debe mantenerse de forma rigurosa: desde el alta, pasando por las modificaciones, hasta la retirada definitiva. Siempre que sea posible, este mantenimiento debe integrarse directamente en los procesos existentes de gestión de servicios de TI (ITSM), compras y RR. HH., de modo que las actualizaciones se generen automáticamente a lo largo del ciclo de vida del activo.

La siguiente ilustración muestra estos tres momentos de proceso:

Ciclo de vida del activo: los tres momentos clave del proceso



Ejemplo práctico con Timly

Para que los datos de activos se mantengan actualizados a largo plazo, los procesos de mantenimiento deben integrarse lo más estrechamente posible en los flujos de trabajo existentes. Las soluciones móviles de gestión de activos, como Timly, facilitan el trabajo de los equipos descentralizados, los procesos de mantenimiento y la gestión de responsabilidades sobre activos en múltiples ubicaciones.

Los retos típicos surgen por responsabilidades poco claras, falta de priorización y escasa visibilidad operativa del beneficio. Por ello, debe definirse con claridad qué evento desencadena qué actualización y quién es responsable de llevarla a cabo. Solo unas **responsabilidades y procesos de actualización claramente definidos garantizan la calidad de los datos** a largo plazo.

Consejo práctico

La responsabilidad sobre los activos solo funciona de forma fiable cuando el mantenimiento de la información de los activos forma parte de los procesos existentes. Especialmente eficaz es la integración con los flujos de trabajo de ITSM, compras y RR. HH.

5.6 Uso operativo: casos de seguridad (a partir de la semana 12)

Tras finalizar la fase de implantación (fases 1–5, semanas 1–11), el registro de activos pasa a utilizarse de forma continua a partir de la semana 12.

Un registro central de activos aporta su mayor valor en la operación de seguridad del día a día. Procesos como la gestión de parches, la respuesta a incidentes o el control de accesos solo funcionan de manera eficiente cuando se dispone de **información actualizada y fiable sobre los activos relevantes**.

Sin esta base, los equipos de seguridad tienen que recopilar manualmente la información desde distintos sistemas y hojas de cálculo en caso de incidente. Con un registro central bien mantenido, es posible **identificar, priorizar y tratar de forma trazable los sistemas afectados mucho más rápidamente**.

A continuación se presentan tres casos de uso clave en los que se aprecia de forma especialmente clara este valor práctico.

Gestión de parches

En el caso de vulnerabilidades críticas, sin un registro central de activos el trabajo suele empezar con una búsqueda laboriosa: ¿qué sistemas se ven afectados, qué versiones se ejecutan dónde y quién es el responsable? La información está dispersa en distintas herramientas, listas y equipos.

Con un registro central de activos, **los sistemas afectados pueden filtrarse y priorizarse directamente**, por ejemplo según la versión de software, la ubicación, la criticidad o la persona responsable. Así queda claro qué sistemas deben tratarse primero y quién debe ejecutar las acciones. El estado de los parches y el avance de la implementación se mantienen de forma transparente y trazable.

Respuesta a incidentes

Ante un incidente de seguridad, como un acceso sospechoso o una alerta de malware, al principio no está claro qué sistemas están implicados ni cuán crítica es la situación. Sin una base de datos central, a menudo se inicia una investigación manual a través de varios sistemas.

Plan de 90 días para un registro de activos orientado a la seguridad

Con un registro de activos, **el contexto necesario está disponible de inmediato**: sistema afectado, responsable, ubicación, criticidad y posibles dependencias. Esto permite iniciar más rápidamente las primeras medidas y gestionar con claridad las vías de escalado.

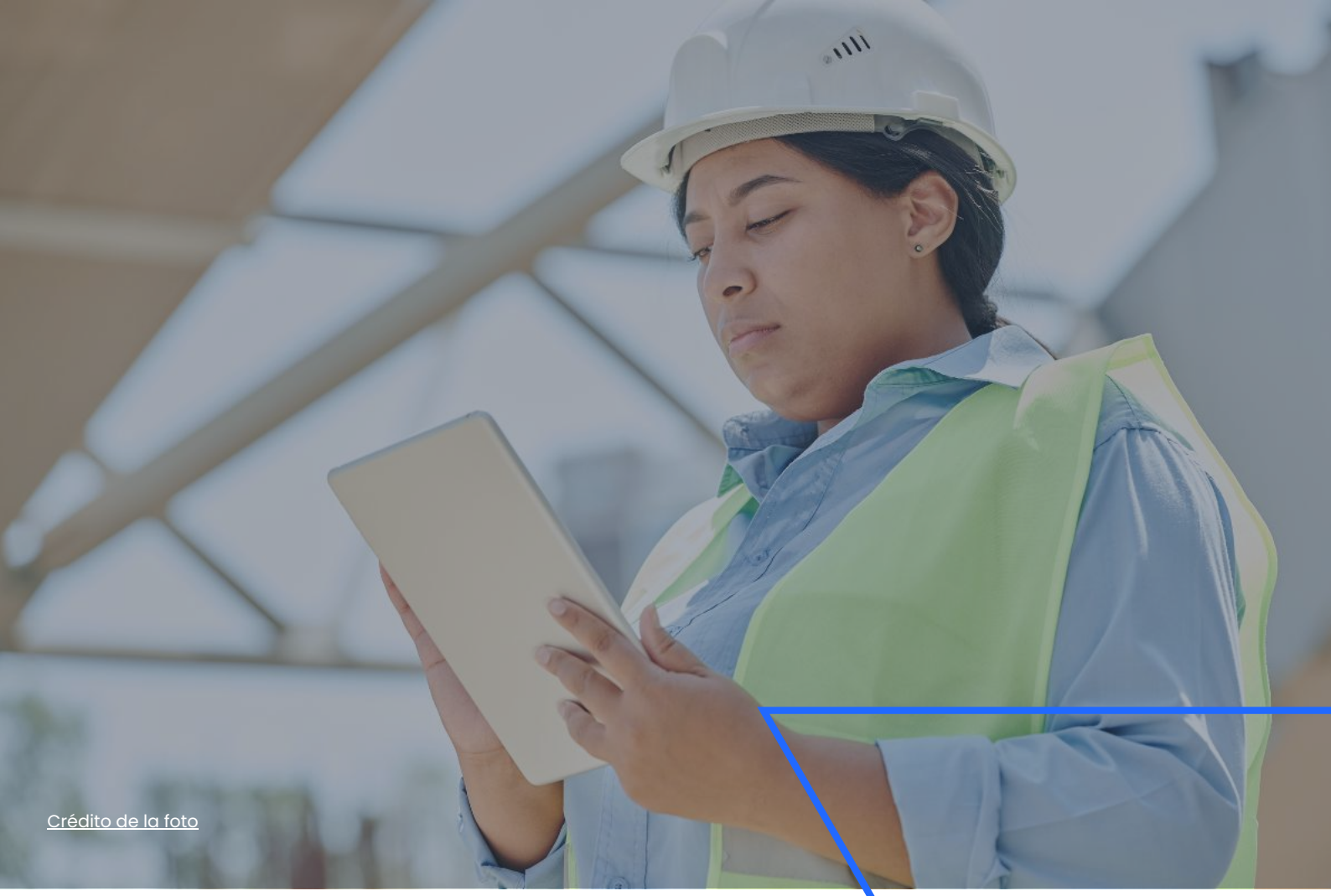
Control de accesos y modelo de confianza cero (Zero Trust)

En muchos entornos, las decisiones de acceso siguen basándose en supuestos simples, como la pertenencia a una red o la conexión por VPN. El contexto del sistema que intenta acceder suele ser insuficientemente conocido.

Un registro de activos proporciona la base necesaria para decisiones basadas en el contexto: **tipo de dispositivo, ubicación, criticidad, estado de parches y responsable**. De este modo, los accesos pueden controlarse de manera más diferenciada, por ejemplo restringiendo aquellos desde sistemas desconocidos o no actualizados.

Consejo práctico

El valor operativo de un registro de activos no se mide por la cantidad de datos, sino por la rapidez y la calidad de las decisiones. La clave es disponer del contexto necesario de forma inmediata ante un incidente, una actualización crítica o una solicitud de acceso.



Crédito de la foto

Ejemplos prácticos de construcción, producción, TI y gestión de instalaciones

Ejemplos prácticos de construcción, producción, TI y gestión de instalaciones

Los capítulos anteriores han mostrado cómo construir paso a paso un registro de activos adecuado para la seguridad de la información. Los siguientes ejemplos ilustran cómo se refleja esta estructura en la operación diaria, en los ámbitos de construcción, producción, IT y gestión de instalaciones.

6.1 Proveedor de servicios de construcción y gestión de instalaciones

Proveedor de servicios de construcción y gestión de instalaciones – 400 empleados, 30 sedes

Activos móviles, gestión descentralizada mediante Excel y correo electrónico

SITUACIÓN INICIAL

Las responsabilidades no estaban claras, las ubicaciones no eran trazables y las auditorías presentaban lagunas de forma recurrente. Varios miles de activos móviles (herramientas, equipos de prueba, equipamiento de TI) se gestionaban mediante listas descentralizadas, sin una visibilidad fiable sobre su estado ni su paradero.

MEDIDAS

- Registro de activos basado en códigos QR directamente in situ, entre distintas sedes
- Asignación central de responsables por activo
- Integración con la gestión de identidades y el sistema de tickets
- Modelo de criticidad A/B/C para priorizar las tareas de mantenimiento

RESULTADOS

Activos no asignados:
~18% → <3%

Respuesta a incidentes:
De varios días → <4 horas

Preparación para auditorías:
Por primera vez completa
Evidencias de inspecciones y de responsabilidades generadas directamente desde el sistema

«El momento decisivo no suele ser la implementación en sí, sino el inventario completo. A partir de ahí se hace visible muy rápidamente dónde no existen responsabilidades claras.»

– equipo de Customer Success de Timly

6.2 Empresa de producción con foco en OT

Empresa de producción – foco en OT, varias plantas

Entornos OT complejos, inventarios paralelos, versiones de firmware desconocidas

SITUACIÓN INICIAL

No estaba documentado qué instalaciones eran realmente críticas, por lo que en caso de avería era imposible priorizar de forma fundada. Los inventarios paralelos no estaban actualizados ni eran coherentes entre sí, y en muchos casos se desconocían las versiones de firmware.

MEDIDAS

- Alcance deliberadamente acotado: primero solo las instalaciones críticas para la producción
- Descubrimiento de red como base técnica de referencia
- Complemento manual de datos específicos de OT (firmware, fabricante, área)
- Asignación de responsables y criticidad A/B/C, integración con el sistema de mantenimiento

RESULTADOS

Activos críticos para la producción:
>90% registrados de forma completa

Versiones de firmware desconocidas:
De un nivel elevado → <5%

Análisis de vulnerabilidades:
Por primera vez priorizable
Sistemas afectados identificados en poco tiempo y ordenados según su criticidad

«En los entornos OT, el problema de fondo rara vez es la tecnología en sí, sino la falta de una visión compartida sobre qué sistemas son realmente críticos.»

– equipo de implementación de Timly

Ejemplos prácticos de construcción, producción, TI y gestión de instalaciones

6.3 Proveedor de servicios de TI / Managed Service Provider (MSP)

Proveedor de servicios de TI / MSP – 50 clientes

Entornos de TI heterogéneos, activos en sistemas de tickets, monitorización y Excel distribuidos

SITUACIÓN INICIAL

En caso de incidente faltaba una vista consolidada que abarcara clientes, sistemas y responsabilidades. Los activos estaban distribuidos en distintas herramientas y la elaboración de informes requería combinar manualmente la información por cada cliente.

MEDIDAS

- Registro central para activos internos y orientados al cliente
- Sincronización automática mediante herramientas RMM y APIs de la nube
- Asignación de cada activo a clientes y responsables internos
- Informes estándar para clientes generados automáticamente a partir del registro

RESULTADOS

Activos registrados de forma coherente
>95% con responsable asignado y vinculación al cliente

Identificación de incidentes
De horas → a minutos

Reporting
Totalmente automatizado
Los informes periódicos a clientes se generan sin esfuerzo manual

«La mayor diferencia no viene de disponer de más datos, sino de reducir el tiempo de búsqueda en caso de incidente.»

– equipo de Customer Success de Timly

Conclusión práctica

Los ejemplos muestran un patrón recurrente: el mayor beneficio no proviene de una exhaustividad perfecta, sino de contar pronto con una estructura utilizable, con responsabilidades claras y datos clave consolidados. Una vez establecida esta base, mejoran de forma notable tanto la seguridad operativa como la rapidez en el día a día.

Crédito de la foto

Anclaje organizativo y gestión del cambio

Anclaje organizativo y gestión del cambio

Un registro de activos no genera valor únicamente por la implementación de una herramienta, sino sobre todo por su **integración en las estructuras existentes de responsabilidades y procesos**. Lo decisivo es el anclaje organizativo del registro dentro de los procesos operativos y de gobierno ya establecidos.

De este modo, el registro deja de ser solo una base de datos y se convierte en una referencia operativa para seguridad, operación de TI y cumplimiento normativo.

7.1 Gobernanza y modelo de roles

La responsabilidad estratégica del registro de activos suele recaer en la dirección de TI o en la función de CISO. En esta función se definen el alcance, el modelo mínimo de datos, la lógica de criticidad y la conexión con los requisitos de riesgo y cumplimiento.

> Lo decisivo no es el mantenimiento operativo, sino la definición de reglas vinculantes según las cuales se evalúan y gestionan los activos en la organización.

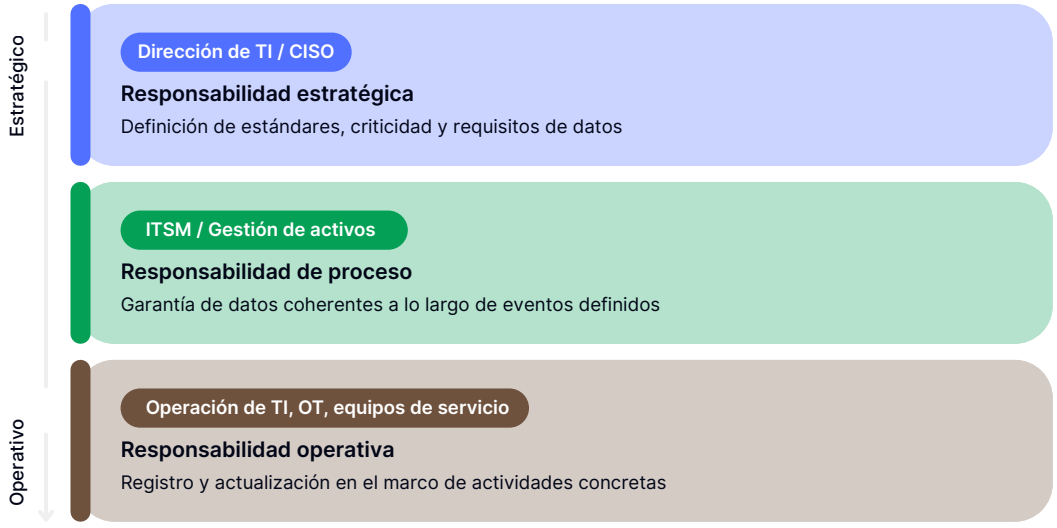
La responsabilidad operativa se sitúa allí donde surgen realmente los cambios, es decir, en:

- operación de TI
- equipos de OT
- organizaciones de sede o de planta
- unidades técnicas de servicio

Estos grupos son responsables de que los **eventos relevantes para los activos se reflejen de forma inmediata en el sistema**, por ejemplo en la puesta en servicio, el cambio de ubicación, las actividades de mantenimiento o la retirada de servicio.

En la práctica, la mayoría de las incoherencias no se deben a la falta de responsables, sino a desencadenantes poco claros: ¿quién registra un cambio cuando un equipo se traslada «solo temporalmente» o cuando un servicio es prestado por un proveedor externo? **Un modelo de roles sólido no solo separa niveles, sino también tipos de responsabilidad**. La siguiente representación muestra los tres niveles centrales de responsabilidad en el registro de activos.

Niveles de responsabilidad en el registro de activos

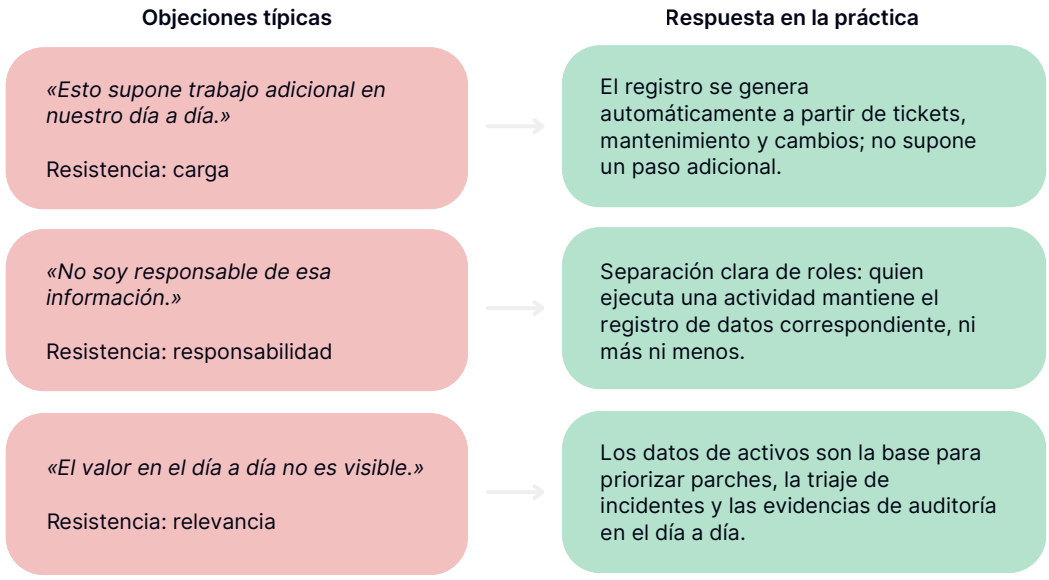


7.2 Habilitación y aceptación en el día a día

La implementación de un registro de activos rara vez fracasa por la tecnología, sino por la **carga adicional que genera en el trabajo operativo diario**. Comentarios típicos desde la práctica son:

- «Esto supone trabajo adicional en nuestro día a día.»
- «No soy responsable de esa información.»
- «El valor operativo para nosotros no es visible.»

La aceptación surge sobre todo cuando los datos de activos pueden mantenerse directamente en el contexto de trabajo operativo. La siguiente representación muestra **tres objeciones típicas y cómo pueden abordarse en la práctica**.



El modelo solo resulta eficaz cuando el registro y la actualización de datos se integran en los procesos existentes.

En la práctica, la información relevante sobre activos debería generarse idealmente directamente en el marco de procesos ya establecidos, como tickets, tareas de mantenimiento, solicitudes de cambio o compras.

Son especialmente eficaces aquellos procesos con la menor barrera operativa posible:

- **El registro móvil y el escaneo mediante códigos QR o de barras** simplifican las tareas de inventario y mantenimiento en el día a día.
- **Un conjunto reducido de atributos básicos obligatorios** facilita el inicio y mejora la calidad de los datos.
- **La contextualización en el trabajo diario**: los datos de activos respaldan decisiones operativas, por ejemplo, en la priorización de incidentes, la priorización de parches o las evidencias de auditoría.

> *«La aceptación no se logra mediante formaciones, sino mediante la simplicidad. Cuando los equipos pueden registrar un activo en 10 segundos mediante un escaneo de QR y el resultado es visible de inmediato en el ticket o en la planificación de mantenimiento, el mantenimiento de los datos se convierte en un hábito, no en una tarea adicional.»*
>
> **EQUIPO DE CUSTOMER SUCCESS DE TIMLY**

7.3 Integración en los sistemas de gestión existentes

Un registro de activos despliega su mayor valor cuando funciona como **referencia central entre los sistemas de operación, seguridad y cumplimiento ya existentes**.

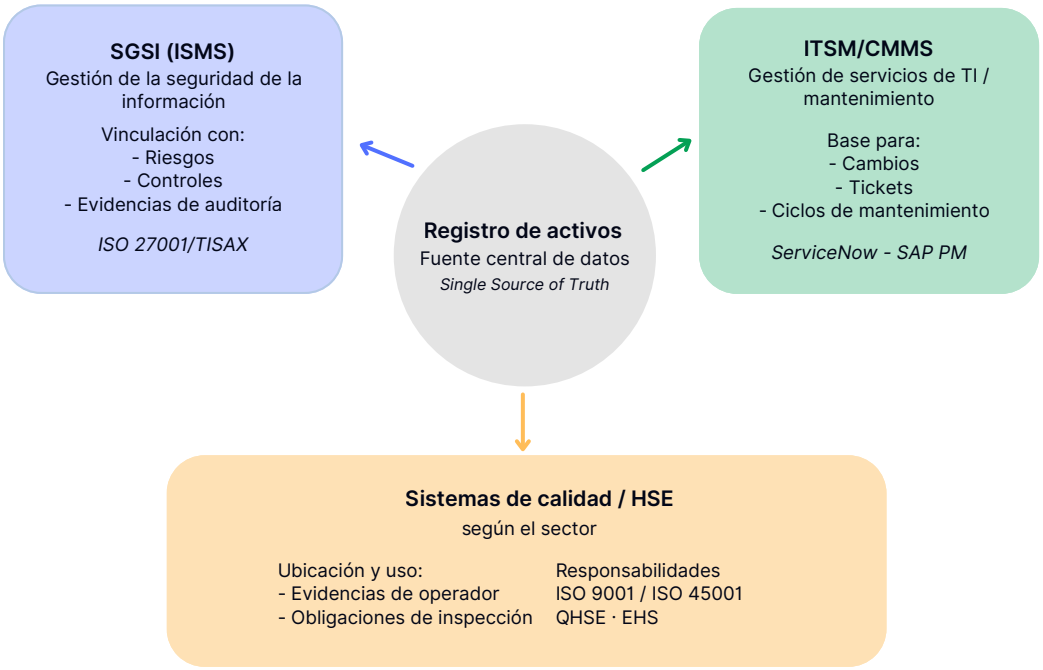
En el centro se sitúa su integración en tres áreas de sistema:

SGSI vincula los activos con riesgos, medidas de seguridad y evidencias de auditoría.

ITSM/CMMS
utiliza el registro de activos como base para solicitudes de cambio, tickets y ciclos de mantenimiento.

Sistemas de calidad / HSE
garantizan, según el sector, la trazabilidad de ubicación, uso y responsabilidades.

La siguiente representación muestra cómo el registro de activos actúa como fuente central de datos entre estos sistemas.



Es esencial una asignación clara de **qué sistema es el de referencia para cada categoría de datos**. Si esta asignación falta, surgen rápidamente inconsistencias entre ITSM, CMMS y el registro de activos.

Lo decisivo son roles bien definidos y una interacción nítida entre los sistemas: el registro de activos sirve como referencia central, mientras que los sistemas operativos registran cambios y eventos del ciclo de vida.

Factores organizativos típicos de éxito en el despliegue

- Responsabilidades claras a lo largo de todo el ciclo de vida del activo (desde el alta hasta la retirada de servicio).
- Integración en los procesos de alta, cambio y retirada de servicio.
- Reducción de las barreras de entrada mediante un número mínimo de atributos obligatorios.
- Beneficios operativos visibles desde el principio (por ejemplo, auditorías más rápidas, menos consultas en la operativa diaria).

Crédito de la foto

Conclusiones clave y recomendaciones para decisores

Conclusiones clave y recomendaciones para decisores

Las siguientes conclusiones y recomendaciones condensan los principales hallazgos de este informe y muestran qué medidas deberían priorizar ahora las empresas para establecer una gestión de activos de ciberseguridad eficaz y sostenible.

8.1 Las cinco ideas principales de un vistazo

Un registro de activos sólido constituye la base operativa de los procesos modernos de ciberseguridad y cumplimiento normativo. **Las siguientes conclusiones condensan los principales hallazgos de este informe**:

1. Sin **datos de activos consistentes y actualizados** de forma continua, una gestión eficaz del riesgo cibernético solo es posible de manera limitada. Los sistemas no registrados o gestionados de forma insuficiente figuran entre las causas más frecuentes de brechas de seguridad, retrasos en la respuesta a incidentes y una cobertura de parches incompleta.
2. **Requisitos regulatorios como NIS2 o ISO 27001** exigen datos de activos trazables y verificables, responsabilidades claras y evidencias fiables. En entornos dinámicos de TI y OT, listas de inventario aisladas ya no resultan suficientes para ello.
3. El verdadero valor se genera en la **operación diaria**: un registro de activos central mejora de forma directa la respuesta a incidentes, la gestión de parches, la preparación para auditorías y los informes de seguridad en el día a día.
4. Una gestión eficaz de activos de ciberseguridad es, por tanto, menos una cuestión de herramientas que una **combinación de gobernanza, procesos integrados y mantenimiento continuo de los datos**.
5. Resultan especialmente eficaces los **modelos de inicio pragmáticos**, con clases de activos claramente priorizadas, pocos procesos clave y mejoras medibles dentro de los primeros meses.

8.2 Recomendaciones concretas para los próximos 6–12 meses

La creación de un registro de activos adecuado para la seguridad de la información no debe entenderse como un proyecto de TI aislado, sino como una evolución gradual hacia un modelo operativo orientado a la seguridad. **La siguiente hoja de ruta resumida muestra qué medidas han demostrado ser especialmente eficaces en la práctica.**

Resultados rápidos (0–3 meses)
(corresponde a las fases 1–3 del plan de 90 días)

- Definir las clases de activos críticas y el alcance
- Consolidar las fuentes de datos centrales
- Establecer el modelo de datos mínimo y las responsabilidades
- Definir los primeros KPIs de seguridad

Estabilización operativa (3–6 meses)
(corresponde a las fases 4–5 del plan de 90 días)

- Realizar el inventario inicial y la depuración de datos
- Conectar el registro de activos con los procesos de parches e incidentes
- Anclar las responsabilidades a lo largo de todo el ciclo de vida
- Asegurar la calidad de los datos y su actualización continua

Desarrollo estratégico (6–12 meses)
(desarrollo más allá del plan de 90 días inicial)

- Integrar por completo el registro de activos en el SGSI
- Automatizar los informes de auditoría y cumplimiento
- Ampliar el control basado en el modelo de Zero Trust y en el riesgo
- Mejorar continuamente el modelo de madurez y la gobernanza

Consejo práctico

Las empresas no deberían intentar crear desde el principio un inventario completo de todos los activos. Son mucho más eficaces los modelos iterativos, con clases de activos priorizadas y procesos clave claramente integrados.

8.3 Perspectivas

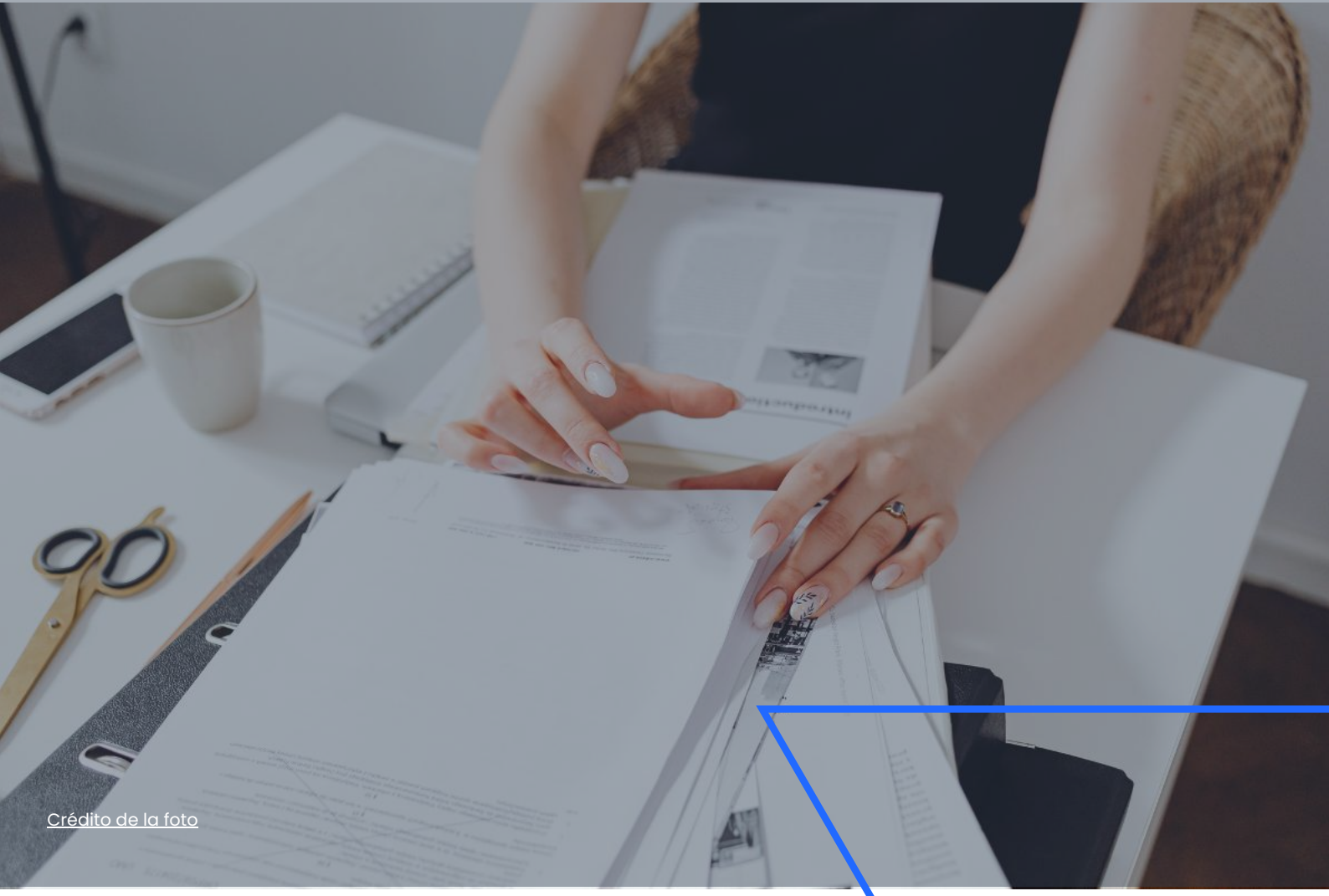
La gestión de activos de ciberseguridad está dejando de ser un proyecto puntual de inventario para convertirse cada vez más en una **capa central de control para la seguridad, el cumplimiento normativo y la resiliencia operativa**.

Con el aumento de los requisitos regulatorios derivados de NIS2, ISO 27001, KRITIS y otras normativas sectoriales, crece la presión sobre las empresas para demostrar una transparencia completa sobre los activos relevantes para la seguridad. Al mismo tiempo, siguen ganando peso los entornos híbridos de TI/OT, el uso de la nube, los modelos de trabajo móvil y los accesos externos. En este contexto, un registro de activos sólido se convertirá aún más en la base para:

- la gestión del riesgo y del cumplimiento
- las arquitecturas de confianza cero
- la gestión automatizada de vulnerabilidades
- la respuesta a incidentes y la resiliencia operativa
- la capacidad de auditoría y de demostración del cumplimiento
- los procesos integrados de operación y mantenimiento

A largo plazo, los enfoques modernos de CSAM evolucionarán hacia un **modelo operativo integral** que conecte entre sí la seguridad, TI, OT, mantenimiento, cumplimiento normativo y los procesos relevantes para los objetivos ESG.

Crédito de la foto



Crédito de la foto

Sobre Timly y la metodología

Timly

Sobre Timly y la metodología

Timly ayuda a las empresas a gestionar de forma centralizada, móvil y transparente los activos físicos, los medios técnicos de operación y los recursos relevantes para la seguridad. La plataforma se utiliza especialmente en **sectores con estructuras de activos distribuidas y dinámicas**, como la construcción, la industria, el sector TI, la gestión de instalaciones, los servicios técnicos y los entornos industriales de operación.

Un foco especial se centra en vincular la transparencia sobre los activos físicos con los procesos operativos y los requisitos relacionados con la seguridad. Entre otros, esto incluye:

- la gestión centralizada de activos físicos y medios de operación
- la captura móvil de datos mediante smartphone o tableta
- la inventarización basada en códigos QR y de barras
- el soporte de ubicaciones distribuidas y equipos móviles
- la integración de activos cercanos a OT y de instalaciones técnicas
- los procesos de ciclo de vida y mantenimiento
- las responsabilidades basadas en roles y la trazabilidad de las acciones

Gracias a la combinación de una captura de datos sencilla, el uso móvil y una base de datos central, Timly ayuda a las empresas a **reducir brechas de transparencia y a hacer operativos los datos sobre activos**, tanto en el contexto de TI/OT como para los requisitos de seguridad, auditoría y cumplimiento normativo.

Descubre en una demostración gratuita cómo puede implementarse en la práctica la transparencia sobre los activos en entornos de TI y OT distribuidos.

RESERVAR DEMO

9.1 Metodología

Este informe se basa en una combinación de:

- estudios y análisis de mercado de acceso público
- requisitos regulatorios y normativos
- experiencias prácticas procedentes de proyectos con clientes
- conocimientos internos obtenidos en talleres, implementaciones y feedback de usuarios
- observaciones operativas en sectores con estructuras de activos distribuidas

Se han tenido en cuenta, entre otras, las siguientes referencias y requisitos:

- ISO 27001 / Anexo A
- la Directiva NIS2
- publicaciones de Verizon, IBM y otros análisis de ciberseguridad
- experiencias en proyectos de TI, OT y gestión de instalaciones

Los niveles de madurez, los ejemplos de KPIs y las recomendaciones prácticas presentados se entienden deliberadamente como un modelo objetivo pragmático y no como un marco de cumplimiento rígido. El objetivo del informe es ofrecer a las empresas **un punto de partida práctico para la creación de un registro de activos adecuado para la seguridad de la información**, con foco en la reducción de riesgos, la viabilidad operativa y una transparencia apta para auditorías.

9.2 Fuentes

[1] https://www.verizon.com/business/resources/infographics/2025-dbir-infographic.pdf
[2] https://www.ibm.com/reports/data-breach
[3] https://eur-lex.europa.eu/eli/dir/2022/2555/oj
[4] https://www.trendmicro.com/explore/aichangingcyberrisk