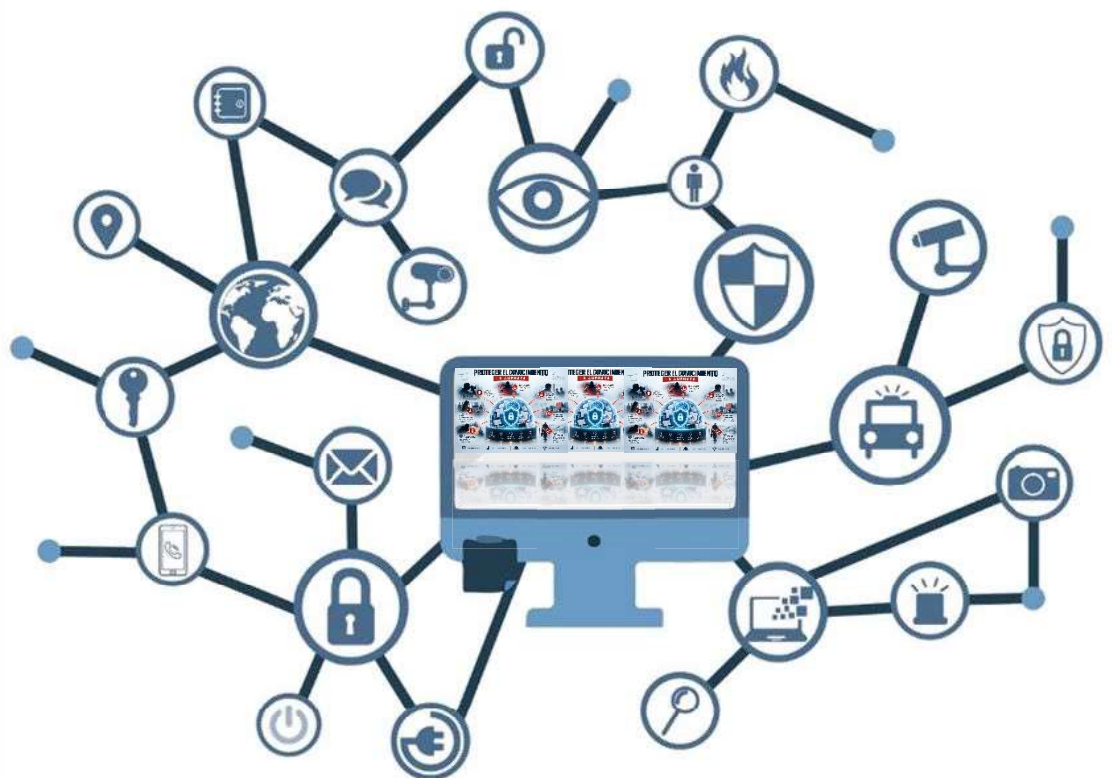


Proteger el Conocimiento (I)

LA AMENAZA

El conocimiento como nuevo activo
estratégico: de proteger Información a
proteger Ventaja tecnológica



Autor: Pedro Sebastián CEO, Founder & ESRM Consulting®

Octubre 2026

Tabla de contenido

1. ¿Dónde está realmente el valor de una empresa tecnológica?	4
2. Del dato al conocimiento	5
3. El adversario no necesita robarnos todo	6
4. Las patentes: proteger publicando	7
4. Algoritmos y software: el conocimiento invisible	8
5. Los procesos industriales: el secreto que no aparece en los planos.....	9
6. Y después están las personas.....	10
7. El talento como activo estratégico.....	11
8. Las “Crown Jewels” tecnológicas	12
9. No todo debe protegerse igual.....	13
10. De la clasificación documental a la clasificación del conocimiento	14
11. Una responsabilidad que supera al CISO.....	15
12. Un nuevo paradigma de seguridad	16
13. Reflexión final.....	17

El conocimiento como nuevo activo estratégico: de proteger información a proteger ventaja tecnológica

SERIE | PROTEGER EL CONOCIMIENTO — I

Por: Pedro Sebastián CEO, Founder & ESRM Consulting®

Durante décadas hemos construido sistemas de seguridad alrededor de una idea aparentemente sencilla:

Proteger la información.

Hemos clasificado documentos, protegido servidores, establecido controles de acceso, desplegado sistemas de ciberseguridad y desarrollado políticas de confidencialidad.

Todo ello continúa siendo necesario.

Pero ya no es suficiente.

En una economía basada en la innovación, el verdadero activo estratégico de muchas organizaciones no es la información que almacenan.

Es el conocimiento que les permite hacer aquello que otros todavía no saben hacer.

Y esa diferencia obliga a cambiar el paradigma:



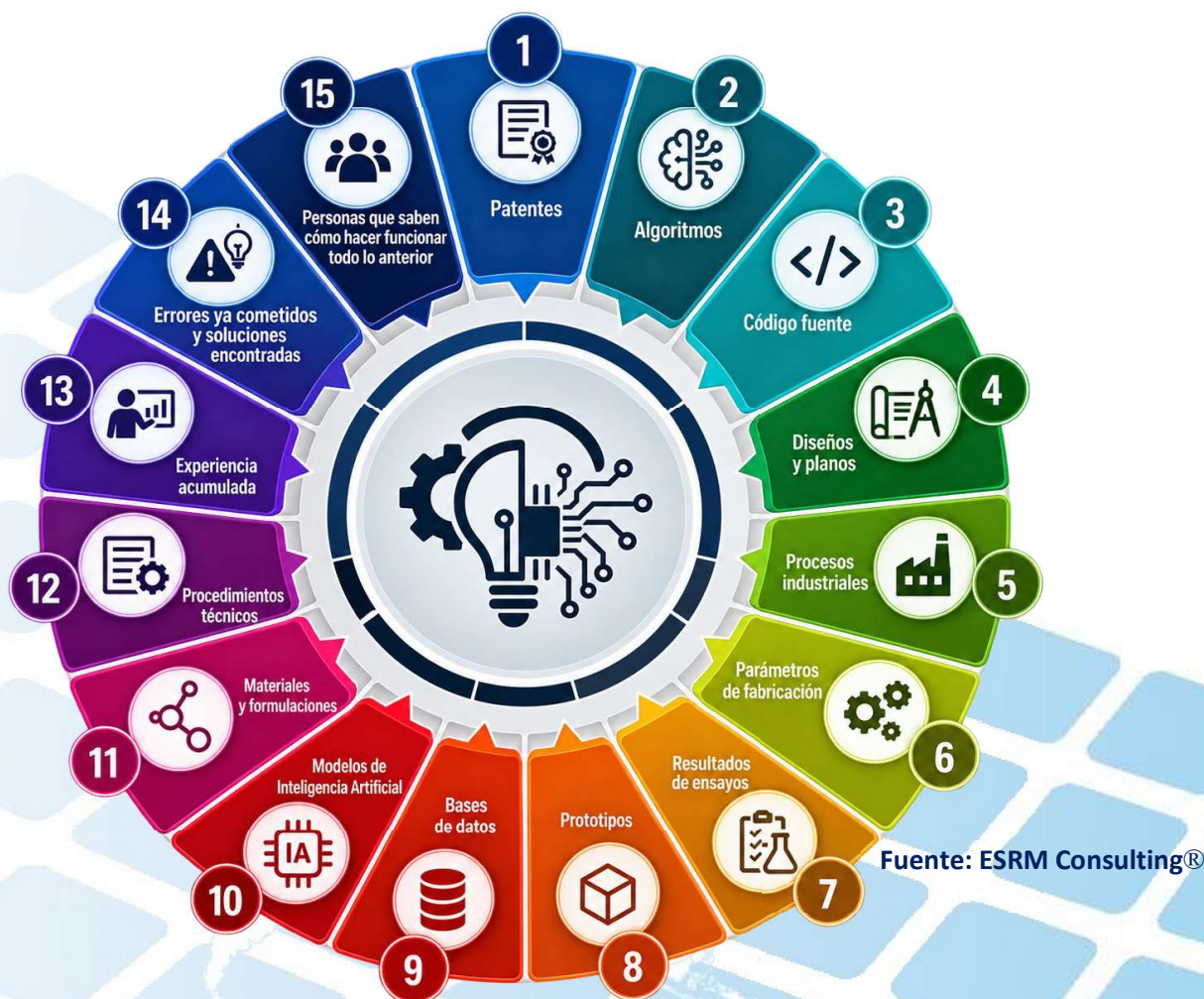
Fuente: ESRM Consulting®

1. ¿Dónde está realmente el valor de una empresa tecnológica?

Pensemos en una organización que lleva diez años desarrollando una determinada tecnología.

Su ventaja competitiva probablemente no esté contenida en un único documento denominado “**CONFIDENCIAL**”.

Está distribuida entre múltiples activos:



Ese conjunto constituye el verdadero capital tecnológico de la organización.

2. Del dato al conocimiento

No toda información tiene el mismo valor.

Podemos imaginar una cadena sencilla:



Fuente: ESRM Consulting®

Un conjunto de datos puede tener un valor limitado de forma aislada.

Pero cuando esos datos se combinan con experiencia, procesos, tecnología y conocimiento humano pueden convertirse en una capacidad industrial.

Y una capacidad industrial difícil de reproducir puede convertirse en una **ventaja estratégica**.

Por eso, cuando hablamos de espionaje tecnológico, no debemos pensar únicamente en el robo de archivos.

El objetivo puede ser comprender **cómo funciona una organización**.

3. El adversario no necesita robarnos todo

Este es probablemente uno de los aspectos menos intuitivos del problema.

Un actor interesado en nuestra tecnología no necesita necesariamente obtener:
“el documento secreto”.

Puede reconstruir conocimiento mediante múltiples piezas aparentemente independientes:



Individualmente, muchas de estas piezas pueden parecer poco relevantes.

Combinadas pueden revelar mucho más.

Es el denominado **efecto mosaico**: diferentes fragmentos de información permiten reconstruir una capacidad que nunca estuvo contenida completamente en una única fuente.

4. Las patentes: proteger publicando

Existe además una aparente paradoja.

Una patente protege jurídicamente una innovación, pero al mismo tiempo obliga a describirla públicamente.

Por ello, la estrategia de propiedad intelectual debe decidir cuidadosamente:

PROTECCIÓN DEL CONOCIMIENTO CRÍTICO



Fuente: ESRM Consulting®

La protección tecnológica requiere, por tanto, coordinar:

I+D+i + Propiedad Intelectual + Legal + Seguridad + Inteligencia + Negocio

Patentar no es únicamente una decisión jurídica.

En determinados sectores también puede convertirse en una decisión estratégica de seguridad tecnológica.

4. Algoritmos y software: el conocimiento invisible

Una parte creciente del valor empresarial reside en activos intangibles.

Algoritmos, modelos de IA, código fuente, arquitecturas, datasets, metodologías de entrenamiento o sistemas de optimización pueden concentrar años de investigación.

Y existe una característica especialmente relevante:

pueden copiarse en segundos.

Una máquina industrial puede pesar varias toneladas.

Un algoritmo capaz de optimizar esa máquina puede caber en un dispositivo de almacenamiento.

Esta asimetría convierte al conocimiento digital en un activo extraordinariamente valioso y extraordinariamente fácil de transferir si los controles fallan.

5. Los procesos industriales: el secreto que no aparece en los planos

Dos empresas pueden disponer de maquinaria similar y producir resultados completamente diferentes.

¿Por qué? Por el **know-how**.



Fuente: ESRM Consulting®

En muchas industrias, *conocer el proceso puede ser incluso más importante que conocer el producto.*

El plano explica **qué** fabricar.

El know-how explica **cómo** conseguir fabricarlo correctamente, de forma **repetible, rentable y a escala.**

6. Y después están las personas

Este es probablemente el elemento más importante.

Una organización puede cifrar documentos.

Puede segmentar redes.

Puede controlar dispositivos.

Puede proteger laboratorios.

Pero una parte significativa de su conocimiento reside en la memoria y experiencia de sus empleados.

Personas que conocen:

qué funcionó,

qué fracasó,

qué problemas aparecieron,

cómo se resolvieron,

qué proveedores son críticos,

qué tecnología se está desarrollando,

qué líneas de investigación se abandonaron,

y cuál será probablemente el siguiente producto.

Por eso debemos incorporar una idea fundamental:

Proteger el conocimiento significa también proteger a quienes poseen el conocimiento.



Fuente: ESRM Consulting®

7. El talento como activo estratégico

Las organizaciones suelen gestionar el talento desde Recursos Humanos.

Pero determinados perfiles deberían analizarse también desde una perspectiva de **riesgo tecnológico**.

No porque debamos desconfiar de nuestros empleados.

Sino porque algunas personas concentran un conocimiento extraordinariamente difícil de sustituir.

Un investigador principal.

Un arquitecto de sistemas.

Un ingeniero responsable de un proceso crítico.

Un especialista en materiales.

Un desarrollador que conoce profundamente un algoritmo.

Puede existir una enorme dependencia de una sola persona sin que la organización sea plenamente consciente de ello.

Esto plantea dos riesgos diferentes:

pérdida de talento

y

pérdida de conocimiento.

No son exactamente lo mismo.

Una persona puede abandonar legítimamente una empresa.

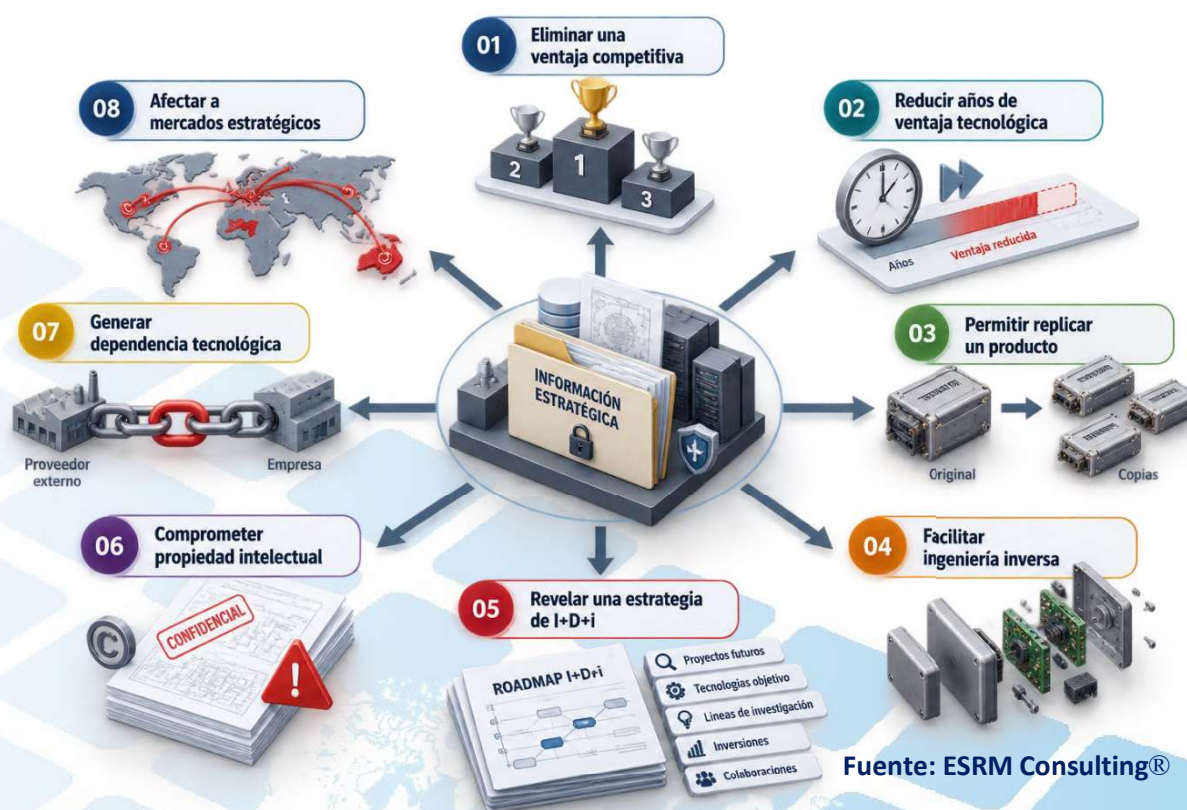
La cuestión estratégica es determinar cuánto conocimiento crítico abandona la organización con ella y qué mecanismos existen para preservar el conocimiento corporativo y proteger los secretos empresariales.

8. Las “Crown Jewels” tecnológicas

Toda organización debería identificar sus auténticas **Crown Jewels**.

No simplemente sus documentos confidenciales.

Sino aquellos conocimientos, tecnologías y capacidades cuya pérdida podría:



Una pregunta puede ayudar a identificarlas:

¿Qué conocimiento, si mañana estuviera en manos de un competidor, cambiaría nuestra posición competitiva?

La respuesta probablemente señale dónde se encuentran los activos que requieren mayor protección.

9. No todo debe protegerse igual

Uno de los errores habituales consiste en intentar proteger toda la información con la misma intensidad.

Eso genera costes, burocracia y, finalmente, pérdida de eficacia.

Una estrategia madura debe diferenciar entre:



Fuente: ESRM Consulting®

Cuanto mayor sea el impacto potencial de su pérdida, mayores deberán ser los controles.

La seguridad debe seguir al valor.

10. De la clasificación documental a la clasificación del conocimiento

Esto supone también evolucionar nuestros modelos tradicionales.

No basta con clasificar documentos.



Porque una organización puede tener perfectamente protegidos sus documentos y continuar exponiendo su conocimiento mediante personas, proveedores, viajes, colaboraciones o información pública.

11. Una responsabilidad que supera al CISO

La protección del conocimiento no puede recaer únicamente sobre Ciberseguridad.

Tampoco exclusivamente sobre Seguridad Corporativa.

Requiere integrar:



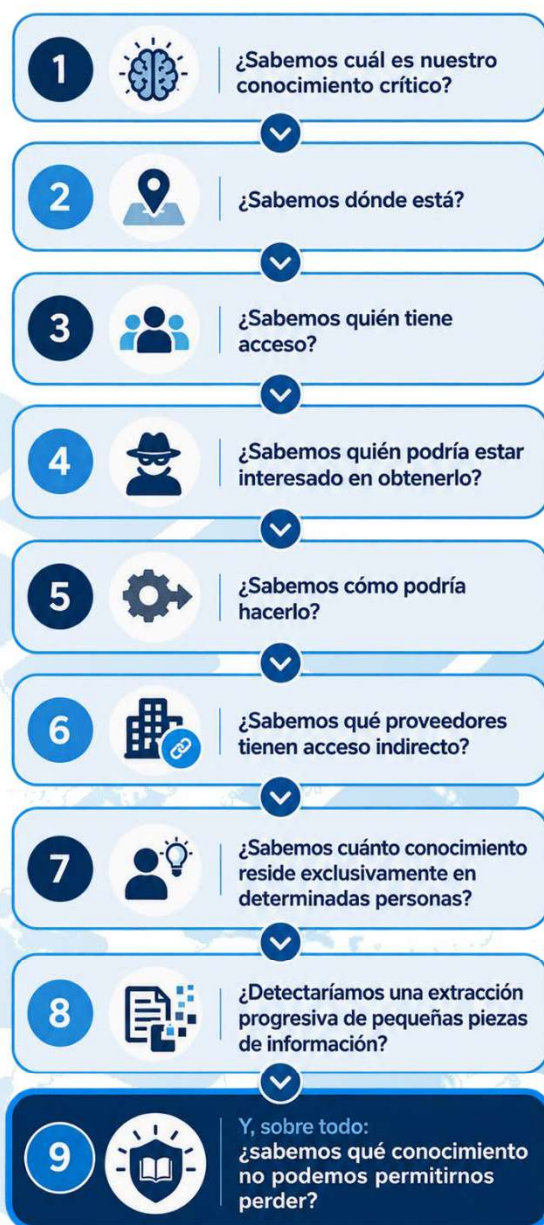
Esta visión transversal es precisamente uno de los principios fundamentales de una **Estrategia Corporativa de Protección del Conocimiento y la Tecnología (ECPT)**.

12. Un nuevo paradigma de seguridad

Durante años hemos preguntado:

¿Está nuestra información protegida?

Quizá deberíamos empezar a formular preguntas diferentes:



Fuente: ESRM Consulting®

13. Reflexión final

En la economía industrial, proteger activos significaba proteger fábricas, maquinaria y mercancías.

En la economía digital y tecnológica debemos proteger algo mucho menos visible:

el conocimiento.

Porque una fábrica puede reconstruirse.

Una máquina puede sustituirse.

Un servidor puede restaurarse.

Pero recuperar años de investigación, experiencia, errores, aprendizaje y know-how puede resultar extraordinariamente difícil.

El verdadero patrimonio tecnológico de una organización no está únicamente en aquello que posee.

Está en aquello que **sabe hacer mejor que los demás.**

Por ello, el siguiente gran paso de la Seguridad Corporativa debería ser evolucionar desde:

PROTEGER INFORMACIÓN

hacia

PROTEGER CONOCIMIENTO

para finalmente alcanzar el verdadero objetivo:

PROTEGER LA VENTAJA TECNOLÓGICA

Porque proteger el conocimiento es proteger la capacidad de **innovar, competir y decidir nuestro propio futuro.**

Pregunta para la Alta Dirección

Si mañana un competidor pudiera acceder a una sola parte del conocimiento de su organización, ¿cuál sería la que nunca querría que obtuviese?

Probablemente ahí se encuentren sus verdaderas **Crown Jewels** tecnológicas.

#ProteccionDelConocimiento #ECPT #SeguridadCorporativa #Inteligencia
#Contrainteligencia #EspionajeTecnologico #EspionajeIndustrial #Ciberseguridad
#PropiedadIntelectual #KnowHow #Innovacion #IDi #InsiderThreat
#ThreatIntelligence #SeguridadEconomica #RiskManagement #SupplyChainSecurity
#InteligenciaArtificial #Tecnologia #SoberaniaTecnologica #SeguridadNacional
#Resiliencia

El conocimiento como nuevo activo estratégico: de proteger información a proteger ventaja tecnológica

Cambio de paradigma: PROTEGER INFORMACIÓN → PROTEGER CONOCIMIENTO → PROTEGER VENTAJA TECNOLÓGICA

SECUENCIA: DEL CONOCIMIENTO AL VALOR ESTRATÉGICO



PRINCIPALES ACTIVOS DE CONOCIMIENTO QUE DEBEN PROTEGERSE

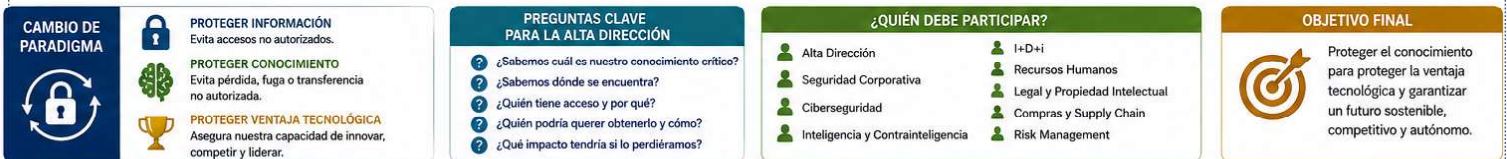


EL EFECTO MOSAICO
El adversario no necesita robarlo todo. Pequeñas piezas de información pueden reconstruir grandes capacidades.

VECTORES DE OBTENCIÓN Y EXPOSICIÓN DEL CONOCIMIENTO



RIESGO CLAVE
El adversario atacará al eslabón más débil con acceso a nuestro conocimiento.



El verdadero patrimonio tecnológico de una organización no está en lo que posee, sino en lo que sabe hacer mejor que los demás.

Fuente: ESRM Consulting®