CENTRO DE ESTUDIOS VECTOR

INTELIGENCIA · IA

La nueva velocidad del riesgo

Cómo la inteligencia artificial acorta el tiempo de reacción frente a las amenazas digitales — y qué significa para el mercado inmobiliario.

IA · CIBERSEGURIDAD · MERCADO INMOBILIARIO · AGOSTO 2026

www.vectorinmobiliario.cl

La nueva velocidad del riesgo

Cómo la inteligencia artificial acorta el tiempo de reacción frente a las amenazas digitales, y qué implica para el mercado inmobiliario

Centro de Estudios Vector · Research · Informe N°02 · Inteligencia IA · Edición Q3 2026 · Alcance: tesis global de ciberriesgo adaptada e interpretada para el mercado inmobiliario chileno.

FICHA TÉCNICA

TEMA	IA, ciberseguridad y rubro inmobiliario
ALCANCE	tesis global adaptada a Chile
FUENTE DE LA TESIS	J.P. Morgan · Eye on the Market (jul 2026)
MARCO LEGAL	Ley N°21.719 · vigente 1 dic 2026
EDICIÓN	Q3 2026
METODOLOGÍA	adaptación e interpretación Vector

01 RESUMEN EJECUTIVO

Durante décadas, el riesgo cibernético fue un problema lejano para la industria inmobiliaria: cosa de bancos, de gobiernos, de tecnológicas. Esa distancia se acabó, y la causa es la inteligencia artificial.

El cambio de fondo es simple de enunciar. Los modelos de IA de frontera ya no solo escriben o resumen: detectan vulnerabilidades de software que antes tomaba meses encontrar, y lo hacen en minutos. Esa misma capacidad, mal usada, acelera los ataques. El número que resume el problema es contundente: el tiempo promedio entre que una falla se hace pública y su primer ataque cayó a cerca de **un día**. Antes había semanas para reaccionar; hoy casi no hay ninguna.

El rubro inmobiliario importa porque tiene tres superficies expuestas al mismo tiempo: maneja datos personales sensibles (clientes, transacciones, financiamiento), opera cada vez más sobre plataformas digitales (CRM, portales, firma electrónica) y administra infraestructura física conectada (edificios inteligentes, control de acceso, climatización). Cada una es una puerta que hace cinco años casi no existía.

La conclusión no es que viene una catástrofe. Es que la ciberseguridad dejó de ser opcional y dejó de ser solo de las grandes empresas. Y que, como en todo lo demás, la ventaja no está en la herramienta —que se abarata—, sino en quién está preparado para enfrentarla. La ventana de anticipación está abierta hoy.

02 HALLAZGOS PRINCIPALES

01 **La ventana de reacción se cerró a un día.** El tiempo entre que una vulnerabilidad se divulga y se explota pasó de semanas a cerca de 24 horas.

02 **El problema no es la solución, es la reacción.** En cerca del 60% de las brechas, la corrección que la habría evitado ya existía: no se aplicó a tiempo.

03 **La IA es el multiplicador, para ambos lados.** La misma capacidad que permite atacar en minutos permite defender en minutos. No es IA contra humanos: es quién la usa primero y mejor.

04 **El rubro inmobiliario tiene tres superficies expuestas:** datos de clientes, operación digitalizada e infraestructura física conectada.

05 **En Chile ya es un riesgo legal, no solo técnico.** Con la Ley N°21.719 vigente desde diciembre de 2026, quien trata datos personales responde por su resguardo.

06 **El costo de prepararse es una fracción del costo de no hacerlo,** y se paga por adelantado. Esa asimetría es todo el argumento.

03 DESARROLLO DEL ANÁLISIS

La ventana que se cerró

Para entender por qué esto importa hay que ver cómo era antes, y en Chile hay una imagen que lo explica mejor que cualquier otra. Antes de que existieran los sistemas de alerta de tsunami, un gran terremoto en la costa no daba ningún aviso: la ola llegaba sin advertencia. Hoy, los minutos entre el sismo y la ola —a veces pocos— alcanzan para subir a zona segura, y han salvado incontables vidas. El aviso no detiene la ola; da tiempo para reaccionar. Toda la diferencia está en ese margen.

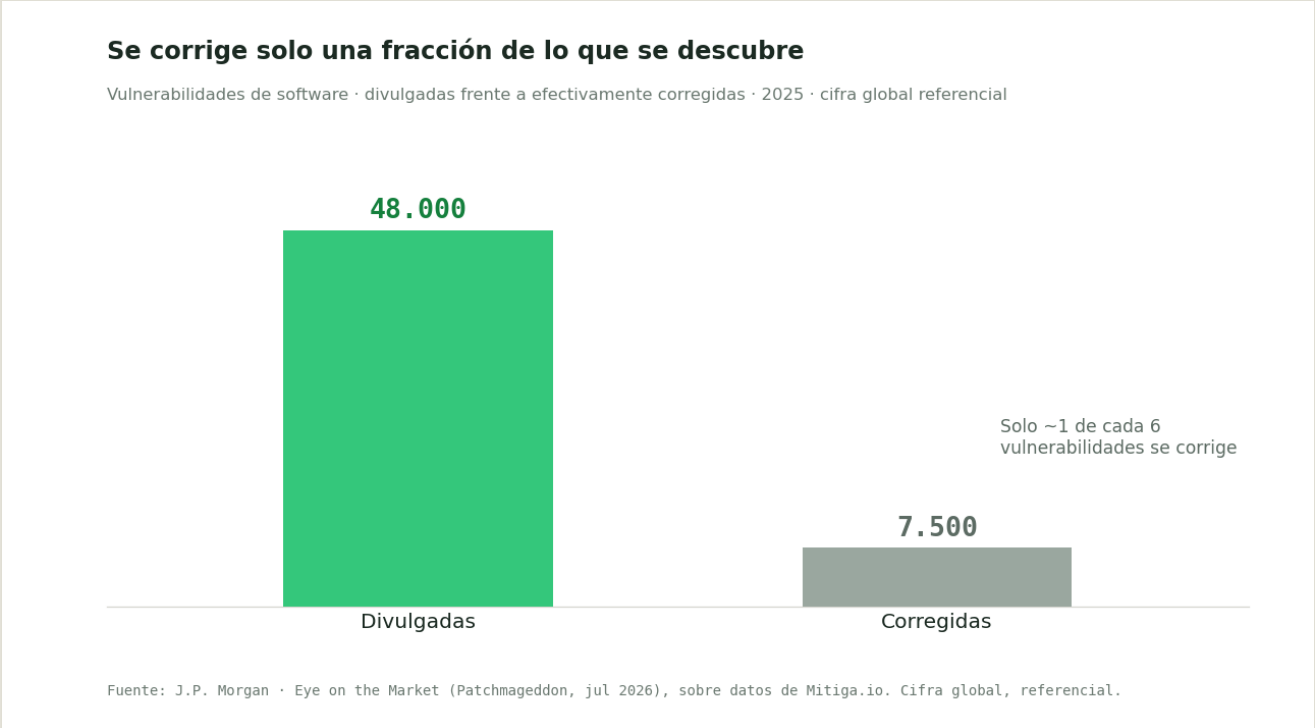
En ciberseguridad, ese aviso son las vulnerabilidades que se divulgan y las correcciones —las actualizaciones de seguridad que resuelven la falla— que se publican junto a ellas. Durante años el sistema funcionó con holgura: se descubría una falla, se publicaba junto a su corrección, y las organizaciones tenían semanas —a veces meses— para aplicarla antes de que alguien la explotara. Había tiempo.

Ese tiempo se está evaporando por tres movimientos simultáneos. El **volumen**: la cantidad de vulnerabilidades que se descubren cada año creció a un ritmo que ninguna organización puede seguir a mano. La **velocidad del atacante**: lo que antes requería semanas de trabajo especializado hoy se automatiza. Y la **accesibilidad**: capacidades que eran patrimonio de un puñado de actores estatales hoy están al alcance de grupos mucho más pequeños. La IA es el multiplicador de los tres, y actúa sobre una curva que ya venía inclinada: la tasa de

vulnerabilidades divulgadas crecía más rápido que la de corrección incluso antes de los modelos más capaces.

INDICADOR	SITUACIÓN	LECTURA
Tiempo del atacante para explotar una falla	~1 día tras su divulgación	La ventana de reacción casi desapareció
Vulnerabilidades divulgadas (2025)	~48.000	Crecen más rápido de lo que se corrigen
Vulnerabilidades efectivamente corregidas (2025)	~7.500	La brecha de corrección se expande
Brechas donde la corrección ya existía	~60%	El problema no es la solución, es la reacción

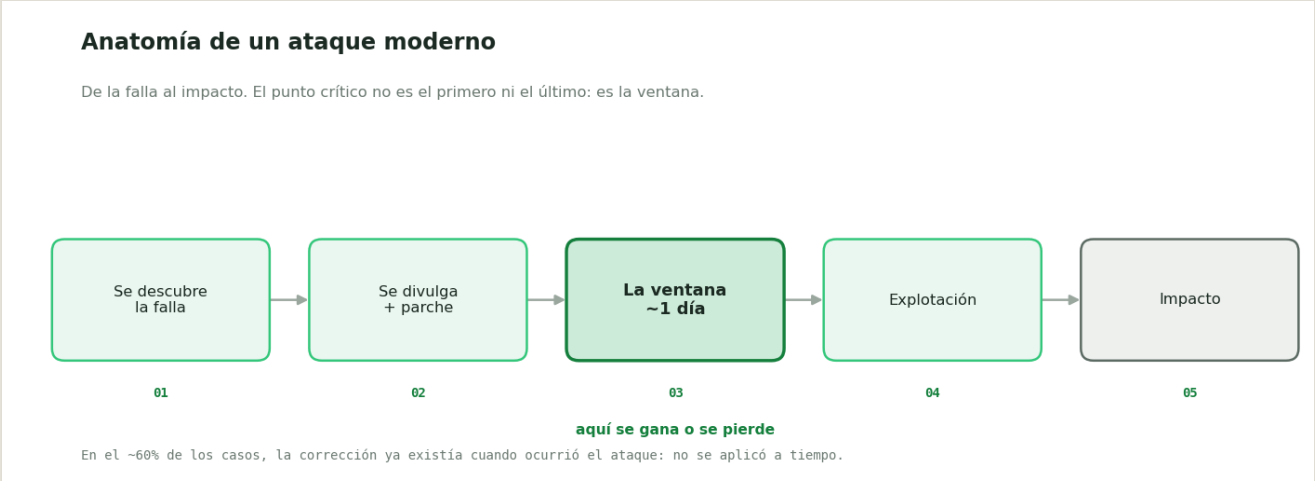
Las cifras son globales y referenciales, del análisis de J.P. Morgan (Eye on the Market, julio 2026); no representan mediciones del mercado chileno.



Vulnerabilidades divulgadas frente a corregidas · 2025

Cómo funciona un ataque hoy

La palabra "hackeo" evoca una imagen equivocada —un genio encapuchado tecleando en la oscuridad— que impide dimensionar el riesgo real. Un ataque moderno se parece más a una línea de producción que a una hazaña individual.



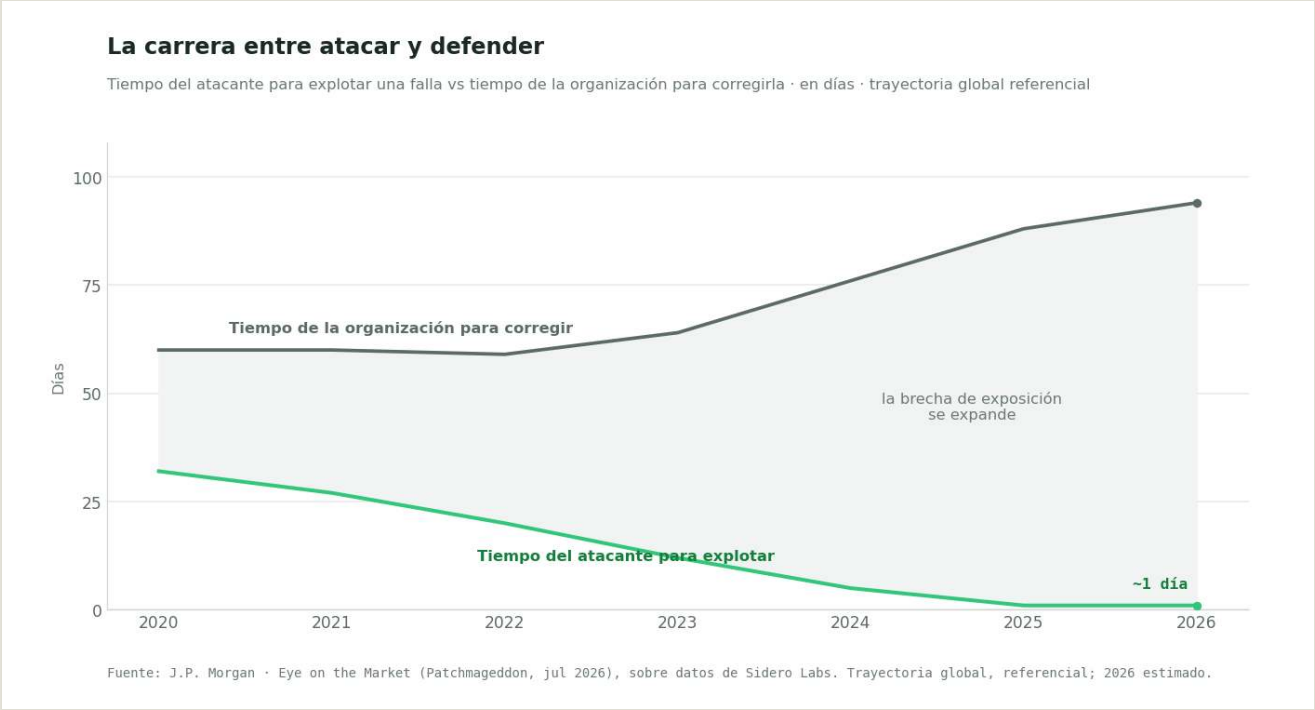
Anatomía de un ataque moderno · de la falla al impacto

Se descubre una falla en un software de uso común —un sistema de gestión, un plugin, una librería que miles de aplicaciones usan sin saberlo—. Se divulga públicamente, junto con la corrección que la resuelve: ese es el momento del aviso. A partir de ahí se abre la ventana, y cada organización que usa ese software debe aplicar la corrección antes de que alguien aproveche la falla. Antes, esa ventana era de semanas; hoy, de cerca de un día. Y cuando el ataque ocurre, en el 60% de los casos la corrección ya estaba disponible: simplemente no se aplicó a tiempo. El impacto final toma cualquiera de estas formas: robo de datos, secuestro de sistemas por ransomware, fraude o control de infraestructura física.

El punto crítico no es el primer paso ni el último. Es la ventana: ahí una organización gana o pierde, y ahí es donde la mayoría del rubro inmobiliario ni siquiera sabe que está jugando.

La carrera entre atacar y defender

Este es el gráfico que ordena todo el informe: dos líneas que se separan. El tiempo que tarda el atacante en explotar una falla cae hacia un día; el tiempo que tarda la organización en corregirla sube hacia los tres meses. La brecha entre ambos —la ventana en que el sistema queda expuesto pese a existir ya la corrección— se expande año a año. El defensor no pierde por falta de solución, sino por el tiempo que tarda en aplicarla.



La carrera entre atacar y defender · tiempos, en días

Hay una segunda lectura, menos pesimista. La misma IA que acelera al atacante está disponible para el defensor: herramientas de seguridad asistidas por IA ya detectan y proponen correcciones a un ritmo antes imposible. La carrera no está perdida; está redefinida. La consecuencia estratégica es una brecha que se expande: las organizaciones que adopten defensa asistida por IA se van a alejar de las que no. En un rubro donde la madurez digital es dispareja, la distancia entre una inmobiliaria preparada y una que no lo está va a ser cada vez mayor, y cada vez más costosa de cruzar.

Aplicación al mercado inmobiliario chileno

Acá está el trabajo que el análisis global no hace, y que es la razón de ser de este informe: por qué esto le importa, concretamente, a quien opera en el rubro inmobiliario chileno. Cuatro frentes.

Los datos del cliente son el activo más expuesto. Un broker o una inmobiliaria acumula exactamente lo que un atacante valora: identidad, capacidad de pago, datos de financiamiento, patrimonio, red de contactos. Esa base de datos, que es el activo comercial más importante de muchos actores del rubro, es también su mayor pasivo si no está protegida. En Chile esto deja de ser un riesgo reputacional para volverse legal y financiero: con la Ley N°21.719 sobre protección de datos personales, vigente desde diciembre de 2026, quien trata datos personales es responsable de su resguardo y responde por su filtración, con sanciones que escalan según la gravedad. La ciberseguridad pasó de ser un tema del que ve los computadores a ser un tema del directorio.

La operación se digitalizó más rápido que su seguridad. CRM, portales de propiedades, firma electrónica, cotizadores, plataformas de arriendo: la superficie digital del rubro creció en pocos años, integración sobre integración, y casi ninguna pieza fue elegida pensando en seguridad. La pregunta que casi nadie se hace, y que debería hacerse, es simple: sobre qué software corre lo que uso todos los días, y quién lo mantiene. La respuesta define buena parte de la exposición real de un negocio inmobiliario.

El edificio inteligente es un computador. El mismo sello de propiedad moderna que agrega valor comercial —accesos remotos, domótica, medición inteligente, cámaras conectadas— agrega superficie de ataque, y muchos de esos sistemas corren software antiguo que no se actualiza con facilidad. Para una administración o una desarrolladora, la seguridad digital de un edificio empieza a ser parte de su mantención, tan concreta como el ascensor o la red eléctrica, y un atributo que un comprador informado va a preguntar.

La transacción es el momento de máxima exposición. El fraude por desvío de transferencias —un correo falso que suplanta a una de las partes justo en el momento del pago — es de los ataques más rentables, y no requiere IA sofisticada: solo información y timing. La IA lo vuelve más creíble y más masivo: mensajes sin errores, contexto real, suplantación convincente. En un rubro donde una sola operación mueve montos altos, un desvío exitoso es catastrófico. La defensa no es tecnológica, es de proceso: verificar por un segundo canal cualquier cambio de datos bancarios. Barato, y casi nadie lo hace de forma sistemática.

---

04 ESCENARIOS

La mejor forma de dimensionar un riesgo abstracto es hacerlo concreto. Cinco situaciones, todas plausibles en el rubro chileno.

Escenario 1 · El correo que llegó justo a tiempo. Un broker cierra la venta de un departamento. El día del pago, el comprador recibe un correo —aparentemente del broker— con los datos bancarios "actualizados" para la transferencia: mismo tono, misma firma, referencia a la propiedad correcta. Transfiere. Un atacante había accedido a la cadena de correos y suplantó al broker en el momento exacto. La pérdida del monto es total y sin recuperación. Lo habría evitado una llamada de treinta segundos para confirmar la cuenta.

Escenario 2 · La base de datos que se fue. Una corredora descubre que su base de clientes —miles de contactos con capacidad de pago e historial— apareció a la venta en un foro. El ataque aprovechó una vulnerabilidad conocida de su CRM, con la corrección disponible hacía meses sin aplicarse. Al daño comercial se suma la responsabilidad legal bajo la Ley 21.719. Lo habría evitado mantener el sistema actualizado, o exigírselo al proveedor.

Escenario 3 · El edificio secuestrado. La administración de un edificio pierde el control del sistema de acceso: las puertas no responden y aparece una exigencia de pago para restablecerlo. El sistema de domótica corría software sin actualizar, expuesto a internet. El costo: residentes sin acceso, riesgo físico y un rescate. Lo habría evitado tratar la seguridad digital del edificio como parte de su mantención.

Escenario 4 · La desarrolladora paralizada. Una inmobiliaria mediana amanece con todos sus archivos cifrados —proyectos, contratos, planos, contabilidad— y una demanda de rescate. El ransomware entró por el computador de un colaborador que abrió un adjunto. Resultado: semanas de operación detenida en pleno lanzamiento de un proyecto. Lo habrían evitado respaldos aislados y doble factor de autenticación.

Escenario 5 · La ventaja silenciosa. Una inmobiliaria decide, antes de que le pase nada, ordenar dónde viven sus datos, exigir seguridad a sus proveedores y capacitar a su equipo contra el fraude de transferencia. No ocurrió nada. Pudo ocurrir cualquiera de los cuatro escenarios anteriores. La diferencia fue moverse dentro de la ventana, antes de la ola. Los cuatro primeros cuestan dinero, reputación o continuidad; el quinto cuesta una fracción, pagada por adelantado. Esa asimetría es todo el argumento.

05 CONCLUSIONES

La tesis global no admite mucho debate: la inteligencia artificial comprimió el tiempo entre el aviso y el impacto, y esa compresión llega a todas las industrias que dependen de software y de datos. La inmobiliaria es una de ellas, aunque todavía no se sienta así.

Lo que este informe agrega es la conexión con el rubro chileno. La evidencia muestra que la ventana de reacción se cerró a un día y que la mayoría de las brechas ocurren pese a existir la corrección. La lectura de fondo es que estamos ante otro caso del mismo patrón: la herramienta se democratiza y la ventaja se desplaza al que está preparado. Y la implicancia local es concreta: con la Ley 21.719 vigente, un negocio inmobiliario que no protege los datos de sus clientes no enfrenta solo un riesgo técnico, sino uno legal y financiero, y lo enfrenta ahora.

Los cinco escenarios muestran que el costo de no prepararse es alto y desigual —cae de golpe, cuando menos conviene—, mientras que el de prepararse es bajo y anticipado. Esa asimetría es la razón por la que la ciberseguridad dejó de ser un lujo de las grandes empresas para volverse higiene básica de cualquiera que maneje datos y dinero. En el rubro inmobiliario, todos manejan las dos cosas.

No hay que entrar en pánico; hay que entender el marco temporal. La ventana de anticipación está abierta hoy, como esos minutos entre el sismo y la ola. Alcanzan, si uno se mueve. El rubro que lo entienda a tiempo va a operar con una ventaja silenciosa; el que lo entienda tarde, lo va a hacer contra ella.

Qué mirar. No es una guía técnica —eso corresponde a un especialista—, sino los frentes que un actor inmobiliario debería tener en el radar: saber dónde viven los datos de sus clientes y quién los custodia (con la Ley 21.719, es obligación); preguntar por la seguridad de sus proveedores, no solo por su precio; tratar el fraude de transferencia como un riesgo operativo real, verificando por un segundo canal todo cambio de datos bancarios; incluir la seguridad digital en la mantención de edificios inteligentes; y mantener la higiene básica al día —actualizaciones, contraseñas robustas, doble factor, respaldos aislados—, con la que se evita el 60% de las brechas.

06 METODOLOGÍA

Este informe adapta e interpreta una tesis global de ciberseguridad y la conecta con la realidad de la industria inmobiliaria chilena. Las cifras de contexto provienen de la fuente citada, son globales y referenciales, y no constituyen mediciones propias del mercado chileno; los gráficos que las reproducen se rotulan como tales. La capa de interpretación y de aplicación local es análisis propio del Centro de Estudios Vector. Los diagramas son de elaboración propia. Edición Q3 2026.

07 FUENTES

- Michael Cembalest, Patchmageddon (Eye on the Market, J.P. Morgan Asset & Wealth Management, julio 2026): tesis y cifras globales de ciberriesgo, a su vez sobre datos de Sidero Labs y Mitiga.io.
- Ley N°21.719 sobre Protección de Datos Personales (Chile) · Ley N°19.628.
- Interpretación y aplicación al mercado inmobiliario chileno: Centro de Estudios Vector.

Análisis de industria con fines informativos. No constituye asesoría de ciberseguridad, legal ni de inversión. Las cifras globales citadas son referenciales y provienen de la fuente indicada. Edición Q3 2026.

NOTA DE CIERRE

El Centro de Estudios Vector publica investigación abierta sobre la industria inmobiliaria y la inteligencia artificial que la está reordenando. Compartimos estos análisis con un solo propósito: elevar la profundidad con que se lee, se analiza y se decide en el rubro. Entender antes —cuando la ventaja todavía está disponible— es la parte del trabajo que ninguna herramienta hace por uno.

José Ignacio Guzmán

FUNDADOR · VECTOR

Centro de Estudios Vector · Research


Vector
@vectorinmobiliario
Vector Inmobiliario
www.vectorinmobiliario.cl