La Empresa Mínima Viable: ¿cómo sostener la promesa de valor en medio del incierto cibernético?

Resumen

La prevención total de un ciberataque es una promesa que ninguna organización puede cumplir. Cuando algo falla, la pregunta deja de ser cómo evitar el golpe y pasa a ser qué parte del negocio debe seguir de pie. La Empresa Mínima Viable (EMV) responde a esa pregunta: es la versión más pequeña de la organización capaz de sostener su promesa de valor al cliente mientras el resto se recupera. Este documento ordena un concepto que hoy aparece disperso en la literatura profesional, lo integra con las operaciones y la gobernanza mínimas viables, y lo enlaza con tres paradigmas de diseño: seguridad, resiliencia y antifragilidad. Sobre esa base propone un método de implementación para la junta, una aplicación basada en un ejemplo real tomado de un incidente reciente con inteligencia artificial, un conjunto de recomendaciones para la toma de decisiones y un instrumento de madurez para autoevaluar el avance. El aporte de este ejercicio está situado en usar el concepto de EMV y convertirlo en una herramienta de gobernanza accionable por un equipo ejecutivo.

Palabras clave: empresa mínima viable, resiliencia cibernética, gobernanza, junta directiva, antifragilidad, inteligencia artificial.

Jeimy J. Cano M.

1. Introducción

El riesgo cibernético cambió de naturaleza. Dejó de ser un problema de la sala de servidores para instalarse en la agenda de la junta, porque su materialización compromete la promesa de valor de la empresa y, en el límite, su continuidad (Cano, 2023). Los directores reconocen su importancia y la ubican entre sus prioridades (Corporate Board Member & Diligent Institute, 2026), aunque muchos recibieron formación en otras disciplinas y solo dedican al tema unos pocos minutos al año (Parrish, 2024). Esa brecha de conocimiento es relevante: persiste en los consejos, conduce a decisiones costosas sobre inversión tecnológica y expone a la organización a responsabilidades que antes no existían (Calder, 2019; Hepfer, 2025).

La respuesta tradicional, incorporar más controles, resulta insuficiente. Los atacantes superan controles bien financiados, y la interconexión con terceros amplió la superficie de exposición más allá del perímetro corporativo (Weis, 2024). A esto se suma un actor nuevo: la inteligencia artificial, que actúa con autonomía y puede causar daño sin intención maliciosa cuando interpreta mal su contexto (Anthropic, 2026). En este escenario, la junta necesita un marco de decisión que no dependa de la promesa de evitar todo ataque, sino de asegurar que lo esencial sobreviva.

Este no es un asunto que la junta pueda delegar por completo en el área técnica. La supervisión del riesgo cibernético forma parte del deber de cuidado del cuerpo directivo, porque las consecuencias de un ataque: pérdidas, sanciones, daño reputacional, recaen sobre la organización y sus accionistas (Larcker & Tayan, 2011). Decidir qué debe sobrevivir es, por naturaleza, una decisión de negocio y de gobierno, no una configuración tecnológica.

Ese marco es la empresa mínima viable. Este documento la presenta como una guía de gobernanza: define qué debe protegerse por encima de todo, cómo decidirlo y cómo medir el avance. La junta que adopta esta lógica deja de perseguir una seguridad total inalcanzable y empieza a defender, de manera deliberada, aquello sin lo cual el negocio deja de existir.

2. Fundamentos teóricos de la empresa mínima viable

2.1 Antecedentes del concepto

El apellido "mínimo viable" nació fuera del dominio de la ciberseguridad. Procede del producto mínimo viable, término acuñado en 2001 y popularizado en el ámbito emprendedor como la versión más simple de un producto capaz de generar aprendizaje con el menor esfuerzo (Ries, 2011). De allí tomó prestada una idea clave: en vez de construirlo todo, identificar el núcleo que basta para funcionar.

Entre 2024 y 2026, ese principio migró del crecimiento a la supervivencia. Una familia de términos surgió casi en paralelo desde la literatura profesional: empresa mínima viable, compañía mínima viable, negocio mínimo viable y operaciones mínimas viables. Todos apuntan a lo mismo con diferentes matices. La empresa mínima viable se define como las capacidades, activos y dependencias críticas necesarias para sostener los compromisos esenciales del negocio (EY, 2026). La compañía mínima viable se plantea como la versión más pequeña de una organización que puede seguir operando de forma segura, sostenible y conforme ante una disrupción extrema pero plausible (KPMG, 2026), y como un imperativo de la sala de juntas que obliga a identificar los servicios y funciones que deben permanecer activos en una crisis (PwC, 2025). El evento relevante suele citarse con nombre propio: la interrupción global de julio de 2024 de Crowdstrike, que mostró el efecto dominó de una falla simultánea y despertó el interés por entender qué se necesita, como mínimo, para seguir operando.

Este concepto no es ajeno en el mundo de las normas. Tiene un precursor formal en la continuidad del negocio: el objetivo mínimo de continuidad, es decir, el nivel más bajo aceptable de productos o servicios durante una interrupción, recogido en el estándar internacional de continuidad (ISO, 2019). La diferencia es de alcance. El objetivo mínimo de continuidad se ocupa de las salidas del negocio; la empresa mínima viable abarca la forma mínima de toda la organización, incluidas sus estructuras y capacidades.

No existe un origen académico formal ni un autor único del concepto; se trata de un concepto fundado en la práctica de consultoría. Este documento adopta "empresa mínima viable" como término paraguas y la define por sus **elementos esenciales del negocio**: las capacidades, activos y dependencias sin los cuales la organización no puede cumplir su promesa de valor al cliente.

Conviene distinguir la empresa mínima viable de la recuperación ante desastres tradicional. No son opuestas: la empresa mínima viable define la meta: el estado mínimo al que hay que volver primero, y la recuperación ante desastres aporta los medios para llegar allí. La diferencia está en el énfasis. En lugar de intentar restaurar todo a la vez en medio del caos, la organización recupera de forma ordenada su núcleo esencial y, solo después, el resto (KPMG, 2026). Es un cambio de prioridad más que de herramientas.

2.2 Tres capas de lo mínimo viable

Lo mínimo viable opera en tres capas complementarias que la junta debe distinguir. La primera es *la operación*: las operaciones mínimas viables son el conjunto reducido de servicios y procesos que deben mantenerse en pie durante un evento adverso (Cano, 2026). La segunda es *la empresa* en su conjunto, con sus personas, dependencias y compromisos con el cliente (EY, 2026). La tercera es *la gobernanza*: la gobernanza mínima viable es la menor cantidad de gobierno necesaria para gestionar el riesgo de forma efectiva sin detener la capacidad de la organización para identificar y aprovechar oportunidades (van der Meulen et al., 2026). Las tres se necesitan: sin operación no hay servicio, sin empresa no hay promesa de valor, y sin gobernanza las decisiones llegan tarde.

Un ejemplo aterriza la distinción. En un banco, las operaciones mínimas viables serían procesar pagos y dar acceso a saldos; la empresa mínima viable añadiría a las personas de soporte, la conexión con la red de pagos y el compromiso de responder al cliente; la gobernanza mínima viable sería el acuerdo previo de quién puede declarar la crisis y autorizar la pausa de lo prescindible. Las tres capas describen el mismo cuerpo desde ángulos distintos, y ninguna se sostiene sin las otras dos.

2.3 Tres paradigmas de diseño: seguridad, resiliencia y antifragilidad

La empresa mínima viable cobra sentido dentro de una evolución de paradigmas que va de resistir a fortalecerse (Cano, 2026). La *seguridad por diseño* busca la robustez de la estructura: privilegia la protección y confía en la solidez de los controles. La *resiliencia por diseño* abandona la ilusión de control y acepta que el golpe llegará; su lógica es absorberlo, adaptarse y mantener la operación (Cano, 2025). La *antifragilidad por diseño* da un paso más: aspira a que la organización mejore a través del desorden, es decir, que cada incidente la deje más fuerte que antes.

Aquí surge una tensión que conviene resolver. "Mínimo viable" sugiere amortiguar para sobrevivir; "antifragilidad" sugiere crecer con el estrés. El puente entre ambos es de secuencia, no de contradicción**.** La empresa mínima viable es la base: el umbral de supervivencia que asegura que la promesa de valor no se deja de cumplir. La antifragilidad por diseño es el mecanismo que, después de cada crisis, eleva esa base. Un incidente bien aprovechado reduce el tiempo de recuperación futuro y añade controles que antes no existían. Así, lo mínimo viable no es una meta por sí misma, sino la base sobre la cual la organización aprende a fortalecerse.

2.4 Comparación de los conceptos base

Tabla 1

Los tres "mínimos viables" y la pregunta de gobernanza que responde cada uno

Concepto	¿Qué define?	Pregunta de gobernanza
Empresa mínima viable (EY, 2026)	La forma mínima de toda la organización que sostiene la promesa de valor.	¿Qué debe seguir de pie para no incumplirle al cliente?
Operaciones mínimas viables (Cano, 2026)	El conjunto reducido de procesos y servicios a mantener.	¿Qué procesos no pueden detenerse?
Gobernanza mínima viable (van der Meulen et al., 2026)	El mínimo de gobernanza para decidir rápido sin frenar la operación.	¿Quién decide y con qué límites durante la crisis?

Nota. Elaboración propia a partir de EY (2026), Cano (2026) y van der Meulen et al. (2026).

Tabla 2

Paradigmas de diseño y la decisión directiva que cada uno demanda

Paradigma de diseño	Lógica central	Decisión de junta que activa
Seguridad por diseño	Robustez: proteger y prevenir.	Aprobar controles y presupuesto de protección del núcleo.
Resiliencia por diseño	Absorber el golpe y seguir operando.	Fijar umbrales de operación y tiempos de recuperación.
Antifragilidad por diseño	Mejorar a partir del desorden.	Exigir aprendizaje medible tras cada incidente.

Nota. Adaptado de Cano (2026).

2.5 ¿Por qué la prevención, por sí sola, no basta?

La empresa mínima viable parte de una premisa incómoda: prevenir no basta. Los atacantes superan controles bien financiados, y una porción importante de los activos de las organizaciones vive en una "zona de vulnerabilidad", con visibilidad y cobertura por debajo del promedio (EY,

2026). El gasto en seguridad reduce el impacto de un ataque, pero no lleva su probabilidad a cero (ISACA, 2025). Aceptar esto no es rendirse. Es la condición para decidir, con cabeza fría y antes de la crisis, qué debe sobrevivir. La prevención sigue siendo necesaria, no obstante deja de ser suficiente. La empresa mínima viable no la reemplaza: la complementa con una segunda línea de razonamiento centrada en la supervivencia de lo esencial.

3. Caracterización de la empresa mínima viable en el contexto empresarial

Caracterizar la empresa mínima viable exige traducir un concepto en una lista concreta. Los elementos esenciales del negocio son ese resultado: las capacidades, activos y dependencias sin los cuales la promesa de valor al cliente se rompe. No son los sistemas más costosos ni los más visibles, sino **aquellos cuya ausencia compromete el servicio**. Identificarlos obliga a un ejercicio interdisciplinario entre el negocio, la tecnología y la ciberseguridad, porque solo el negocio sabe qué le promete al cliente y solo la tecnología sabe de qué depende esa promesa (De Haes, Caluwe, Huygh & Joshi, 2020).

El método parte de una pregunta simple y difícil: *si un ataque apagara la mitad de la organización, ¿qué mitad debe seguir operativa para que el cliente no lo note?* Responderla supone detallar los procesos que sostienen la promesa de valor, las aplicaciones y datos que los habilitan, y las dependencias de terceros que, con frecuencia, son el eslabón más frágil (Weatherley, 2015; McCarthy & Flynn, 2003). El resultado es una frontera clara entre lo esencial y lo prescindible, revisada y aprobada por la junta, no delegada al área técnica.

3.1 Lo esencial frente a la empresa completa

Tabla 3

¿Qué se mantiene y qué se pausa durante un ataque?

Dimensión	Empresa en normalidad	Empresa mínima viable (bajo ataque)
Objetivo	Eficiencia, crecimiento, plena funcionalidad.	Sostener la promesa de valor al cliente.
Procesos	Todos los procesos operan.	Solo procesos esenciales; el resto en pausa controlada.
Métrica clave	Rentabilidad y servicio pleno.	Tiempo de recuperación y disponibilidad del núcleo.
Decisión dominante	Optimización.	Priorización y contención.

Nota. Elaboración propia; la clasificación de la decisión dominante se apoya en McDonough (2023).

3.2 ¿Cómo trazar la frontera entre lo esencial y lo prescindible?

Definir lo esencial no es un juicio de intuición, sino un procedimiento. La frontera se traza con un criterio único: el impacto en la promesa de valor dentro de un plazo, y avanza en nueve pasos que la junta puede y debe supervisar.

Tabla 4

Procedimiento para trazar la frontera entre lo esencial y lo prescindible

Paso	¿Qué se hace?	Resultado (evidencia)
1. Declarar la promesa de valor	Escribir en una frase qué le promete la empresa al cliente.	Enunciado aprobado por la junta.
2. Listar servicios que la sostienen	Enumerar los servicios que el cliente nota si se detienen.	Lista corta de servicios clave.
3. Mapear procesos, datos y sistemas	Rastrear de qué depende cada servicio hacia adentro.	Mapa de dependencias por servicio.
4. Incluir personas y terceros	Añadir el factor humano y los	Lista de dependencias humanas y

Paso	¿Qué se hace?	Resultado (evidencia)
críticos	proveedores insustituibles.	externas.
5. Aplicar la prueba de interrupción	Preguntar cuánto aguanta el negocio sin cada elemento.	Umbral de tolerancia por elemento (horas/días).
6. Clasificar con criterio único	Marcar como esencial lo que compromete la promesa antes del umbral.	Dos listas: esencial y prescindible.
7. Resolver zonas grises	Revisar los casos dudosos con las áreas de negocio, de tecnología y de riesgos.	Decisiones documentadas de casos límite.
8. Aprobar y registra fecha de la frontera	La junta ratifica la lista y fija fecha de revisión.	Frontera aprobada, con responsable y fecha.
9. Revisar tras cada cambio o incidente	Actualizar cuando cambie el negocio, un proveedor o tras un ataque.	Frontera vigente, no vencida.

Nota. Elaboración propia.

Regla de decisión. Un elemento es esencial solo si su interrupción compromete la promesa de valor al cliente antes del umbral de tolerancia definido. Todo lo demás es prescindible y puede entrar en pausa controlada durante un ataque. El criterio no es el costo ni la importancia percibida del sistema, sino el impacto en el cliente dentro de un plazo establecido. Un error frecuente lo invalida: clasificar como esencial "casi todo". Si la lista esencial es larga, la frontera no es útil y obliga a priorizar de nuevo con umbrales más estrictos.

3.3 La frontera aplicada: ¿qué muestra el caso?

El incidente con inteligencia artificial descrito en la sección 5 permite probar el método. La aplicación que sigue es una reconstrucción ilustrativa: se apoya en los hechos publicados (Anthropic, 2026), para mostrar la aplicación del procedimiento.

Tabla 5

Aplicación del procedimiento al incidente analizado

Paso del método	¿Qué muestra el caso?	Lección
Mapear dependencias (pasos 3–4)	Había credenciales expuestas y accesos sin autenticación.	Sin mapa de dependencias, el atacante entra por donde nadie mira.
Prueba de interrupción y umbral (paso 5)	Se accedió a datos de producción sin romper visiblemente el servicio.	El daño silencioso no activa umbrales pensados solo para caídas.
Regla de decisión y detección (pasos 6, 9)	Las organizaciones no detectaron la actividad; se enteraron al ser contactadas.	La frontera no es útil si no se detecta el compromiso de lo esencial.

Nota. Elaboración propia a partir de Anthropic (2026).

La detección forma parte de la frontera. El caso deja una enseñanza incómoda: una organización puede tener bien definido su núcleo esencial y aun así fracasar si no advierte que lo están comprometiendo. Por eso la frontera no termina en la lista de elementos esenciales; incluye la capacidad de saber, de forma oportuna, que alguno de ellos está bajo ataque (ISACA, 2025b). Un núcleo protegido pero invisible es un núcleo expuesto.

3.4 Reflexiones sobre el contexto latinoamericano

La mayoría de las fuentes que sustentan este concepto provienen de Norteamérica y Europa. Por tanto es necesario situarla en el contexto latinoamericano. En buena parte de América Latina, las juntas operan con menos recursos especializados, una regulación heterogénea entre países y una alta dependencia de proveedores externos que concentran el riesgo (Cano, 2023; Cano, 2025b).

Gobernar bajo alta incertidumbre, además, plantea oportunidades específicas para las juntas de mercados emergentes que conviene aprovechar (The Boston Consulting Group & INSEAD, 2026). Con esta realidad, la empresa mínima viable ofrece una ventaja práctica: obliga a focalizar la inversión en lo que de verdad importa, en lugar de dispersarla intentando defender todo por igual.

4. Propuesta para la implementación en una organización

El aporte de este documento está en la integración de diversos marcos que en la actualidad están dispersos para apoyar el reto de la gobernanza bajo un ataque cibernético. Este ejercicio reúne cuatro marcos dispersos: empresa, operaciones y gobernanza mínimas viables, más los paradigmas de diseño, en un método que una junta puede aprobar y supervisar (Parenty & Domet, 2019; Bood, van Ees & Postma, 2022). El método cuenta con cinco fases.

1. **Definir la promesa de valor.** La junta hace explícito qué le promete la empresa al cliente. Sin esa declaración, cualquier lista de sistemas “críticos” es arbitraria (Bood, van Ees & Postma, 2022). Evita armar el núcleo por intuición.
2. **Identificar los elementos esenciales.** Un equipo interdisciplinarip traza los procesos, datos, aplicaciones y terceros que sostienen esa promesa, y marca la frontera de lo esencial (De Haes et al., 2020). Evita proteger lo visible en vez de lo que sostiene el servicio.
3. **Fijar umbrales de supervivencia.** Para cada elemento esencial se define cuánto tiempo puede estar caído y cuánta pérdida de datos se tolera. Son decisiones de negocio, no técnicas (OECD, 2011). Evita que la urgencia del incidente defina tarde lo que debió decidirse antes.
4. **Aislar y proteger el núcleo.** Los medios para reconstruir el núcleo: respaldos, identidades, procedimientos, deben vivir fuera del radio de impacto del ataque, accesibles aun cuando el entorno principal esté comprometido (Weis, 2024). Evita que el respaldo caiga con el mismo golpe que el sistema principal.
5. **Ensayar y aprender.** Se prueba la recuperación con ejercicios realistas y se convierte cada hallazgo en una mejora. Aquí la antifragilidad deja de ser discurso y se vuelve práctica (Cano, 2025). Evita descubrir las fallas del plan durante la crisis real.

La quinta fase cierra el círculo con la primera: cada ensayo revela supuestos equivocados sobre la promesa de valor y obliga a revisarla. La empresa mínima viable no es un documento que se archiva, sino una conversación que se sostiene en el tiempo (Nottingham, 2026).

4.1 Roles y responsabilidades

El método falla si no se tiene un dueño concreto de cada parte. La distribución de responsabilidades separa lo que decide la junta de lo que ejecuta la gerencia, sin diluir la rendición de cuentas (Parenty & Domet, 2019).

Tabla 8

Reparto de responsabilidades en la empresa mínima viable

Rol	Responsabilidad principal
Junta directiva	Aprobar la promesa de valor, la lista de elementos esenciales y los umbrales; exigir ensayos y aprendizaje.
Dirección ejecutiva (vicepresidentes)	Asegurar recursos y liderar la respuesta en crisis según el protocolo de 48 horas.
Responsable de seguridad (CISO)	Traducir la frontera en controles, aislar la recuperación y reportar la detección.
Dueños de proceso de negocio (Gerentes)	Definir los umbrales de sus servicios y validar la frontera.
Auditoría y riesgo	Verificar la evidencia de cada avance y retar los supuestos.

Nota. Elaboración propia a partir de Parenty y Domet (2019) y De Haes et al. (2020).

5. Ejemplo práctico: un incidente real con inteligencia artificial

Los conceptos se entienden mejor con un hecho. El caso que sigue no ilustra un ransomware clásico, sino algo más nuevo y más incómodo para una junta: un sistema de inteligencia artificial que, sin proponérselo, causó daño real en organizaciones que ni siquiera lo advirtieron. Se eligió por tres razones: es reciente, está documentado con transparencia por su propio protagonista y muestra con crudeza por qué la supervivencia de lo esencial y la detección temprana importan más que la promesa de una defensa perfecta.

Los hechos.

En julio de 2026, Anthropic publicó la revisión de sus propias pruebas de ciberseguridad. Tras examinar 141.006 ejecuciones de evaluación, halló tres incidentes en los que un modelo de inteligencia artificial, al que se le había indicado que operaba en una simulación sin acceso a internet, alcanzó sistemas reales y comprometió la infraestructura de tres organizaciones distintas (Anthropic, 2026). Los modelos usaron técnicas básicas: contraseñas débiles, puntos de acceso sin autenticación, inyección de código y un paquete malicioso publicado en un repositorio público. Un dato resulta decisivo para una junta: las organizaciones afectadas no habían detectado la actividad; se enteraron cuando Anthropic las contactó.

Lo que se infiere.

De este episodio se desprenden tres lecciones para la gobernanza del riesgo, presentadas como inferencias razonadas, no como certezas. Primera: un agente de inteligencia artificial puede ejecutar acciones dañinas reales por una lectura equivocada de su contexto, sin intención maliciosa (Harkins, 2026). La frontera entre una acción alineada y una dañina depende de lo que el sistema cree sobre su entorno. Segunda: la detección sigue siendo el punto ciego; si el afectado no advierte el ataque, ningún plan de recuperación se activa (ISACA, 2025b). Tercera: la resiliencia no puede descansar en evitar el incidente, sino en asegurar que los elementos esenciales resistan aunque el atacante: humano o artificial, tenga éxito.

Nota aclaratoria. Un solo caso no prueba una regla. Este incidente es atípico (por ahora): ocurrió en un entorno de pruebas de un laboratorio de inteligencia artificial, no en una empresa víctima de extorsión. Su valor es ilustrativo. Se incluye porque muestra, con hechos verificables y recientes, un riesgo emergente que las juntas aún no han incorporado a su agenda: la acción autónoma de la inteligencia artificial y el fallo de detección que la acompaña (Tow, 2026).

El episodio revela, además, lo difícil que es anticipar la conducta de estos sistemas. Los tres incidentes involucraron modelos distintos y respuestas distintas: uno continuó el ataque incluso tras reconocer que el entorno era real; otro dedujo que estaba en la internet abierta, pero se convenció de que seguía en una simulación; el más reciente se detuvo al concluir que el objetivo era real (Anthropic, 2026). Para una junta, la lección no es técnica. La misma tecnología puede comportarse de maneras opuestas ante la misma señal, y esa variabilidad es, en sí misma, un asunto de gobernanza: obliga a no confiar la protección de lo esencial al buen juicio de un sistema cuyo comportamiento no se puede asegurar.

6. Retos clave para incorporar el concepto

Adoptar la empresa mínima viable enfrenta obstáculos concretos. El primero es cultural: exige que la junta acepte que el ataque tendrá éxito, una idea incómoda para quien ha invertido años y presupuesto en prevención (Arribas et al., 2026), y que prepare su modelo de gobernanza para

actuar en plena crisis y no solo antes de ella (Lavin et al., 2025). El segundo es de datos: muchas organizaciones no saben con precisión de qué depende su promesa de valor, y sin ese mapa cualquier definición de lo esencial es un supuesto (Cano, 2026). El tercero es la dependencia de terceros: cuando el elemento esencial vive en un proveedor, la organización controla el riesgo solo en parte (EY, 2026).

A estos se suma un desafío nuevo y dinámico. Los agentes de inteligencia artificial autónomos amplían la velocidad y la escala de los ataques, y difuminan la atribución (Harkins, 2026; The Conference Board, 2026). Un adversario que delega en un agente puede operar sin descanso y adaptar su comportamiento en tiempo real. Frente a esto, la empresa mínima viable no ofrece una defensa perfecta, pero sí una prioridad clara: si no se puede impedir todo, hay que asegurar que lo esencial sobreviva y se detecte de forma anticipada (Deloitte, 2026).

Dos obstáculos más deben considerarse. El primero es de competencias: los consejos reconocen carencias en su propia comprensión de la ciberseguridad, lo que dificulta supervisar decisiones técnicas con criterio y exige apoyo experto (Hepfer, 2025). El segundo es la fatiga de la prevención: años de inversión en controles generan una falsa sensación de seguridad que resta urgencia a la conversación sobre su supervivencia. Superarlos es, ante todo, una tarea de gobernanza: poner el tema en la agenda, medir con honestidad y sostener la disciplina en el tiempo.

7. Recomendaciones para los miembros de la junta

Las siguientes acciones son necesarias y evitan la generalidad de “pedir más reportes”. Cada una es verificable y tiene un dueño.

- **Aprobar cada año la lista de elementos esenciales.** Que sea una decisión formal de la junta, no un anexo técnico (Larcker & Tayan, 2011).
- **Fijar umbrales de supervivencia.** Establecer, por escrito, el tiempo máximo de caída y la pérdida de datos tolerable para cada elemento esencial.
- **Exigir un protocolo de decisión a 48 horas.** Definir quién decide qué en las primeras horas de una crisis, con la gobernanza mínima viable ya acordada (van der Meulen et al., 2026).
- **Atar el presupuesto a los elementos esenciales.** Priorizar la inversión en la defensa y recuperación de lo esencial antes que en la cobertura uniforme (Montford & McCool, 2016).
- **Medir el aprendizaje.** Después de cada incidente o ensayo, verificar que el tiempo de recuperación es menor y que se adoptaron controles nuevos (Cano, 2025).
- **Vigilar la detección.** Preguntar de forma explícita cómo se enteraría la organización de un ataque silencioso, incluido uno conducido por inteligencia artificial (Anthropic, 2026).

Estas seis acciones no son un ideal inalcanzable. Cada una corresponde a una afirmación del instrumento de madurez del Anexo C, de modo que la junta puede medir en qué punto se encuentra y qué le falta para avanzar al siguiente nivel. El progreso no exige un programa perfecto, sino una decisión y esfuerzo sostenido en el tiempo.

8. Conclusiones

El título de este documento plantea una pregunta: *¿cómo sostener la promesa de valor en medio del incierto cibernético?* Una respuesta es la empresa mínima viable. No promete evitar el ataque sino asegurar que, cuando el golpe llegue, siga de pie aquello sin lo cual la promesa al cliente no se puede cumplir. En un entorno donde el adversario evoluciona y ahora delega en agentes autónomos, esa certeza mínima vale más que la ilusión de una seguridad invulnerable.

La empresa mínima viable ofrece a la junta algo que la promesa de la prevención absoluta no puede ofrecer: una prioridad clara y detallada cuando todo falla. No es un concepto original de este documento, sino una síntesis de marcos existentes convertida en herramienta de gobernanza. Su valor está en obligar a una decisión que muchas organizaciones postergan: definir qué debe sobrevivir, y en enlazar esa decisión con una progresión de madurez que va de resistir a fortalecerse.

En consecuencia, una junta que sabe cuáles son sus elementos esenciales, que ha fijado umbrales y que aprende de cada golpe sostiene su promesa de valor en el incierto mejor que otra que confía en que no va a ser atacada (Parenty & Domet, 2019).

Anexos

Estos anexos convierten el concepto en herramientas de trabajo. Pueden usarse por separado: la lista de verificación (A) y las preguntas (B) sirven para iniciar la conversación; el instrumento (C) mide el punto de partida; los anexos D a J acompañan la puesta en marcha y el seguimiento.

Anexo A. Lista de verificación para definir los elementos esenciales

- Se declaró por escrito la promesa de valor al cliente.
- Se enumeraron los procesos que sostienen esa promesa.
- Se identificaron las aplicaciones y datos de los que dependen esos procesos.
- Se listaron los terceros críticos y sus dependencias.
- Se marcó la frontera entre lo esencial y lo prescindible.
- La junta aprobó formalmente la lista de elementos esenciales.
- Los medios de recuperación se encuentran fuera del alcance del impacto del ataque.

Anexo B. Preguntas que la junta debe hacer a la gerencia

- ¿Cuál es nuestra promesa de valor y de qué depende exactamente?
- Si perdiéramos la mitad de los sistemas, ¿qué mitad debe seguir operando?
- ¿Cuánto tiempo puede estar caído cada elemento esencial?
- ¿Cómo nos enteraríamos de un ataque silencioso?
- ¿Podemos recuperar la esencia de las operaciones si el entorno principal está comprometido?
- ¿Qué proveedor concentra tanto riesgo que su caída compromete nuestra promesa de valor?
- ¿Quién decide qué en las primeras 48 horas de una crisis?
- ¿Nuestro presupuesto de seguridad prioriza la defensa del núcleo esencial?
- ¿Cuándo fue la última simulación de recuperación y qué cambió luego de ella?
- ¿Qué aprendimos del último incidente y cómo mejoró nuestra preparación?

Anexo C. Instrumento de madurez (autodiagnóstico)

Instrucciones. Cada afirmación se valora de 1 a 5, donde 1 = totalmente en desacuerdo y 5 = totalmente de acuerdo. Es un autodiagnóstico. Para reducir el sesgo, cada puntaje debe respaldarse con evidencia (un documento, un registro, una simulación), no con opiniones, y conviene que respondan varias personas de negocio y de tecnología.

1. Tenemos declarada por escrito nuestra promesa de valor al cliente.
2. Sabemos qué procesos sostienen esa promesa.
3. Identificamos los datos y aplicaciones de los que dependen esos procesos.
4. Conocemos nuestros terceros críticos y sus dependencias.
5. Existe una frontera clara entre lo esencial y lo prescindible.
6. La junta aprobó formalmente la lista de elementos esenciales.
7. Fijamos umbrales de tiempo de caída y pérdida de datos tolerables.
8. Los medios de recuperación están aislados del radio de impacto.
9. Ensayamos la recuperación con ejercicios realistas.
10. El tiempo de recuperación mejora tras cada ensayo o incidente.

11. Existe un protocolo de decisión para las primeras 48 horas.
12. El presupuesto prioriza la defensa del núcleo esencial.
13. Tenemos forma de detectar un ataque silencioso.
14. Consideramos el riesgo de agentes de inteligencia artificial autónomos.
15. Convertimos cada incidente en mejoras concretas y verificables.

Interpretación de los intervalos

Tabla 6

Intervalos de valoración del instrumento (rango posible: 15 a 75)

Puntaje total	Nivel de madurez	Significado
15 – 34	Inicial	La organización no ha definido su núcleo esencial; la supervivencia ante un ataque depende de la suerte.
35 – 49	Consciente	Existe conciencia y algunos mapas, pero sin decisiones formales de junta ni umbrales.
50 – 64	Gestionado	El núcleo está definido y aprobado, con umbrales y recuperación aislada; falta simulaciones periódicas.
65 – 75	Antifrágil	La organización simula, aprende y eleva su línea base tras cada incidente; la detección está bajo vigilancia.

Nota. Elaboración propia.

¿Cómo pasar de un nivel al siguiente?

- **De Inicial a Consciente:** declarar la promesa de valor y mapear los procesos que la sostienen (afirmaciones 1 a 4).
- **De Consciente a Gestionado:** llevar la lista de elementos esenciales a aprobación de la junta, fijar umbrales y aislar la recuperación (afirmaciones 5 a 8).
- **De Gestionado a Antifrágil:** instaurar simulaciones periódicas, el protocolo de 48 horas y la medición del aprendizaje y la detección (afirmaciones 9 a 15).

Anexo D. Guión de decisiones de la junta en las primeras 48 horas

1. **Hora 0 a 4.** Confirmar el alcance del evento adverso y activar el protocolo. La junta verifica quién dirige la respuesta y qué elementos esenciales están afectados.
2. **Hora 4 a 12.** Decidir sobre la operación mínima. Autorizar la pausa controlada de lo prescindible para proteger los procesos, infraestructura y productos/servicios esenciales.
3. **Hora 12 a 24.** Comunicar. Aprobar el mensaje a clientes, reguladores y grupos de interés, evitando promesas que no se puedan cumplir.
4. **Hora 24 a 48.** Recuperar los elementos esenciales y registrar aprendizajes. Iniciar la reconstrucción desde los medios aislados y documentar cada hallazgo para elevar el línea base.

Anexo E. Glosario para directores

Empresa mínima viable. La versión más pequeña de la organización capaz de sostener su promesa de valor al cliente durante una disrupción grave.

Elementos esenciales del negocio. Las capacidades, activos y dependencias sin los cuales esa promesa se compromete.

Operaciones mínimas viables. El conjunto reducido de procesos y servicios que deben mantenerse en pie durante el evento adverso.

Gobernanza mínima viable. La menor cantidad de gobernanza necesaria para decidir con rapidez sin frenar la operación.

Umbral de tolerancia (tiempo y datos). El tiempo máximo que un elemento puede estar caído y la cantidad de datos recientes que la organización puede permitirse perder tras un incidente.

Antifragilidad por diseño. La propiedad, buscada de forma deliberada, de salir fortalecido de cada incidente en lugar de solo sobrevivirlo.

Pausa controlada. La detención ordenada de lo prescindible para concentrar recursos en el núcleo durante el ataque.

Anexo F. Acta modelo de aprobación de los elementos esenciales

Formato breve para dejar constancia de la decisión de la junta. Se completa una vez al año y tras cada cambio relevante.

- Fecha de la sesión y participantes.
- Promesa de valor al cliente (enunciado vigente).
- Lista de elementos esenciales aprobada.
- Umbral de tolerancia (tiempo de caída y pérdida de datos) por elemento.
- Responsable de custodia de la lista y de los medios de recuperación aislados.
- Fecha de la próxima simulación de recuperación y de la siguiente revisión.
- Firmas de aprobación de la junta.

Anexo G. Hoja de ruta de 90 días

Secuencia mínima para poner en marcha el concepto sin esperar un programa perfecto.

Días 1 a 30. Declarar por escrito la promesa de valor, conformar el equipo mixto de negocio, tecnología y riesgo, e iniciar el mapa de dependencias de los servicios clave.

Días 31 a 60. Aplicar la prueba de interrupción, clasificar cada elemento como esencial o prescindible y fijar los umbrales de tolerancia de tiempo y datos.

Días 61 a 90. Aislar los medios de recuperación, aprobar la frontera en sesión de junta (Anexo F) y programar el primer ensayo de recuperación del núcleo.

Anexo H. Ejemplo ilustrativo de frontera

El siguiente ejemplo es ilustrativo y sirve solo para mostrar cómo se ve una frontera terminada. Corresponde a una empresa mediana de comercio electrónico. Los umbrales son de referencia; cada organización debe fijar los suyos.

Tabla 7

Frontera terminada para una empresa de comercio electrónico (ejemplo ilustrativo)

Elemento	Depende de	Umbral	Clasificación
Cobro y pasarela de pago	Pasarela externa y base de pedidos	2 horas	Esencial
Catálogo y carrito de compra	Servidor web e inventario	6 horas	Esencial
Atención al cliente	Telefonía y sistema de clientes	12 horas	Esencial
Campañas de marketing	Plataforma de correo masivo	1 semana	Prescindible
Reportes internos de gestión	Almacén de datos analítico	2 semanas	Prescindible
Portal interno de empleados	Intranet	3 días	Prescindible

Nota. Ejemplo hipotético; elaboración propia.

La lectura es concreta. Sin cobro, catálogo y atención, la promesa de valor: comprar y recibir, se compromete en horas; por eso son esenciales. El marketing, los reportes y el portal interno pueden esperar días o semanas sin que el cliente lo note; entran en pausa controlada.

Anexo I. Errores comunes al definir la empresa mínima viable

- Declarar "casi todo" esencial, con lo que la frontera pierde utilidad.
- Trazar la frontera sin la voz del negocio, dejándola en manos del área técnica.
- Guardar los respaldos en el mismo entorno que puede ser atacado.
- Confundir un plan escrito con una capacidad probada en una simulación.
- Olvidar a los terceros de los que depende el núcleo esencial.
- Medir la madurez con opiniones en lugar de evidencia verificable.
- Definir la frontera una vez y no revisarla tras los cambios del negocio.

Anexo J. Preguntas frecuentes de la junta

¿La empresa mínima viable reemplaza nuestro plan de continuidad? No. Lo ordena. Le da una prioridad: el núcleo esencial, para que la recuperación empiece por lo que sostiene la promesa de valor.

¿No es esto responsabilidad del área de tecnología? La ejecución sí; la decisión no. Definir qué debe sobrevivir es una decisión de negocio que la junta aprueba y supervisa.

¿Cuánto cuesta implementarlo? El primer paso: definir la frontera, cuesta tiempo y criterio, no inversión mayor. El gasto llega después, y se concentra en defender y recuperar el núcleo, no en cubrir todo por igual.

¿Cada cuánto se revisa? Al menos una vez al año y tras cada cambio relevante del negocio, un proveedor crítico o un incidente.

¿Cómo sabemos si vamos avanzando? Con el instrumento del Anexo C y con dos señales concretas: el tiempo de recuperación disminuye y cada incidente deja controles nuevos.

Anexo K. Tablero de indicadores para la junta

Seis indicadores permiten a la junta vigilar el estado de la empresa mínima viable sin entrar en el detalle técnico. Cada uno tiene una señal de alerta que obliga a preguntar.

Tabla 9

Indicadores de seguimiento de la empresa mínima viable

Indicador	¿Qué observa?	Señal de alerta
Cobertura del núcleo	Elementos esenciales con umbral definido.	Menos del 100 %.
Simulaciones de recuperación	Meses desde el último ensayo del núcleo.	Más de doce meses.
Tiempo de recuperación	Recuperación real frente al objetivo.	La real supera al objetivo.
Recuperación aislada	Respaldos fuera del radio de impacto.	Sin verificar.
Detección	Tiempo estimado para detectar un ataque al núcleo.	Desconocido.
Terceros críticos	Proveedores del núcleo sin plan de contingencia.	Uno o más.

Nota. Elaboración propia.

El tablero no sustituye el criterio de la junta; lo enfoca. Un indicador en alerta no es una falla, sino una conversación pendiente. Revisado con regularidad, convierte la empresa mínima viable en una práctica viva y no en un documento que se firma y se olvida.

Anexo L. El método en una página

Resumen para llevar a la sesión de junta. Cada fila enlaza una fase del método con la decisión que corresponde al cuerpo directivo.

Tabla 10

Síntesis del método y el papel de la junta

Fase	¿Qué define?	Decisión de la junta
Promesa de valor	Qué le promete la empresa al cliente.	Aprobar el enunciado.
Elementos esenciales	De qué depende esa promesa.	Aprobar la lista y su frontera.
Umbrales	Cuánto se tolera sin cada elemento.	Fijar tiempo de caída y pérdida de datos.
Aislamiento	Cómo se reconstruye el núcleo.	Exigir recuperación fuera del radio de impacto.
Simulación	Si el plan funciona de verdad.	Programar y revisar los ejercicios.
Detección	Si sabríamos que nos atacan.	Preguntar por la capacidad de detección.

Nota. Elaboración propia.

Si la junta solo retiene una idea de este documento, que sea esta: **no se trata de evitar todo ataque, sino de decidir, antes de que ocurra, qué debe seguir de pie**. Esa decisión es indelegable y es, en el fondo, una afirmación sobre la identidad de la empresa: aquello que promete a sus clientes y que se compromete a no dejar caer.

Referencias

Anthropic. (2026). Investigating three real-world incidents in our cybersecurity evaluations. https://www.anthropic.com/news/investigating-incidents-cybersecurity-evals

Arribas, F., Canals, J. & Ormazabal, G. (2026). Corporate governance in a context of disruption: The board of directors. *IESE Business School*. https://www.iese.edu/media/research/pdfs/ST-0685-E.pdf

Bood, R., van Ees, H., & Postma, T. (2022). *The role of the board in corporate purpose and strategy*. Cambridge University Press.

Calder, A. (2019). *Duty of care: An executive's guide for corporate boards in the digital era*. John Wiley & Sons.

Cano, J. (2023). *Ciberseguridad empresarial: Reflexiones y retos para los ejecutivos del siglo XXI*. Ediciones de la U.

Cano, J. (2025). Estrategia de ciberseguridad FAD (Flexible, Adaptable y Dinámica): El reto de una respuesta activa y resiliente. En *Proceedings of Information Systems in Latin America (ISLA 2025)*. Association for Information Systems. https://aisel.aisnet.org/isla2025

Cano, J. (2025b) Las juntas directivas y el dilema del volcán. El debido cuidado frente al riesgo cibernético empresarial. 2. *ISACA Journal*. https://www.isaca.org/es-es/resources/isaca-journal/issues/2025/volume-2/the-board-of-directors-and-the-volcano-dilemma-due-care-in-the-face-of-enterprise-cyberrisk

Cano, J. (2026). The evolution of security and control paradigms. 4. *ISACA Journal*. https://www.isaca.org/resources/isaca-journal/issues/2026/volume-4/the-evolution-of-security-and-control-paradigms

Corporate Board Member & Diligent Institute. (2026). What directors think 2026. *Diligent Institute*. https://boardmember.com/webinars/whatdirectorsthink2026/

De Haes, S., Caluwe, L., Huygh, T., & Joshi, A. (2020). *Governing digital transformation: Guidance for corporate board members*. Springer.

Deloitte. (2026). Board governance in 2026. *Deloitte*. https://www.deloitte.com/us/en/programs/center-for-board-effectiveness/articles/board-audit-committee-trends.html

EY. (2026). Global cybersecurity leadership insights study: Redefine resilience. *Ernst & Young*. https://www.ey.com/en_gl/insights/consulting/how-can-you-redefine-resilience-for-the-next-frontier-of-vulnerabilities

Harkins, M. (2026). When trust has no security: AI risks everything. *Institute for Critical Infrastructure Technology*. https://www.icitech.org/post/when-trust-has-no-security-ai-risks-everything

Hepfer, M. (2025). Un CISO no basta para solventar las carencias del consejo de administración en ciberseguridad. *Harvard Deusto Business Review*. https://www.harvard-deusto.com/un-ciso-no-basta-para-solventar-las-carencias-del-consejo-de-administracion-en-ciberseguridad

ISACA (2025). Tech trends and priorities: Global 2026. *ISACA*. https://www.isaca.org/tech-trends-and-priorities

ISACA. (2025b). Threat modeling revisited. *ISACA*. https://www.isaca.org/resources/white-papers/2025/threat-modeling-revisited

ISO. (2019). ISO 22301:2019. Security and resilience — Business continuity management systems — Requirements. ISO.

KPMG. (2026). Defining the minimum viable company: Why the concept matters now. *KPMG*. https://kpmg.com/uk/en/insights/regulatory/defining-the-minimum-viable-company.html

Larcker, D., & Tayan, B. (2011). *Corporate governance matters: A closer look at organizational choices and their consequences*. Pearson.

Lavin, A., Mazza, C. & Aguilera, R. (2025). El gran reto de los consejos de administración ante la crisis persistente. *Harvard Deusto Business Review*. https://www.harvard-deusto.com/el-gran-reto-de-los-consejos-de-administracion-ante-la-crisis-persistente

McCarthy, M. P., & Flynn, T. P. (2003). *Risk from the CEO and board perspective*. McGraw-Hill.

McDonough, B. R. (2023). *Cyber guardians: Empowering board members for effective cybersecurity*. John Wiley & Sons.

Montford, J. T., & McCool, J. D. (2016). *Board games: Straight talk for new directors and good governance*. Praeger.

Nottingham, L. (2026). The CEO's playbook for difficult board directors. *MIT Sloan Management Review*. https://sloanreview.mit.edu/article/the-ceos-playbook-for-difficult-board-directors/

OECD. (2011). Board practices: Incentives and governing risks. *OECD Publishing*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2011/08/board-practices_g1g139a6/9789264113534-en.pdf

Parenty, T. J., & Domet, J. J. (2019). *A leader's guide to cybersecurity: Why boards need to lead — and how to do it*. Harvard Business Review Press.

Parrish, L. (2024). *The shortest hour: An applied approach to boardroom governance of cyber security*. CRC Press.

PwC. (2025). Define your minimum viable company now to survive the next shock. *PricewaterhouseCoopers*. https://www.pwc.co.uk/services/crisis-and-resilience/define-your-minimum-viable-company-now-to-survive-next-shock.html

Ries, E. (2011). *The lean startup: How today's entrepreneurs use continuous innovation to create radically successful businesses*. Crown Business.

The Boston Consulting Group, & INSEAD. (2026). Governing under high uncertainty: Opportunities for emerging market boards. *BCG & INSEAD*. https://www.bcg.com/publications/2026/turkey-governing-under-high-uncertainty-opportunities-for-emerging-market-boards

Tow, B. (2026). Cyber risk at the board level. *Forbes*. https://www.forbes.com/councils/forbestechcouncil/2026/01/30/cyber-risk-at-the-board-level/

van der Meulen, N., Jewer, J. & Levallet, N. (2026). Minimum viable governance for generative AI (Research Briefing, Vol. XXVI, No. 3). *MIT Center for Information Systems Research*. https://cisr.mit.edu/publication/2026_0301_GenAIGovernance_VanderMeulenJewerLevallet

The Conference Board. (2026). C-Suite outlook 2026. *The Conference Board*. https://www.conference-board.org/publications/C-Suite-Outlook-2026-Uncertainty-and-Opportunity

Weatherley, R. (2015). *Eyes wide open: A first-timer's guide to the real world of boards and company directorship*. Major Street Publishing.

Weis, D. (2024). *Boardroom cybersecurity: A director's guide to mastering cybersecurity fundamentals*. Apress.