



La junta directiva frente al riesgo tecnológico:

Gobernanza, responsabilidad fiduciaria y resiliencia digital

José Vega Gallardo

17 de septiembre de 2026

9:51 p. m.



IGCP

INSTITUTO DE GOBERNANZA CORPORATIVA - PANAMÁ

XI CONGRESO DE GOBIERNO CORPORATIVO

RETOS Y PORTUNIDADES DE LA GOBERNANZA DEL FUTURO: TECNOLOGÍA Y SOSTENIBILIDAD

Evolución del cumplimiento tecnológico a la supervisión estratégica del riesgo empresarial.

¿El día de mañana, qué podría destruir más valor en su organización?

¿Una mala decisión financiera?

Las pérdidas financieras suelen ser recuperables.
Los mercados fluctúan, los presupuestos se ajustan
y los errores se corrigen en el siguiente ciclo.

¿O la paralización total de operaciones por una semana?

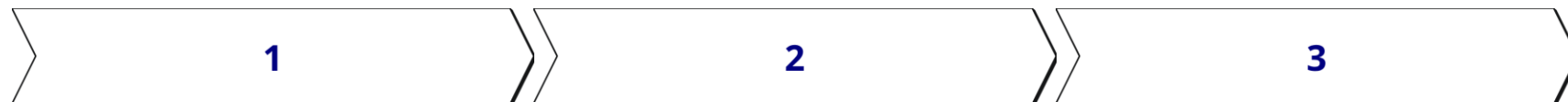
Un incidente tecnológico grave puede detener completamente la empresa: sin facturación, sin comunicaciones, sin acceso a datos críticos, con consecuencias reputacionales y legales irreversibles.

¿De qué aspecto creen que dependen sus organizaciones en mayor medida?

**La organización de hoy,
en cualquier sector,
depende de una capa
digital.**

El cambio de paradigma en la gobernanza

La agenda de la junta directiva ya no gira solo en torno a riesgos financieros, regulatorios y operacionales.



Modelo tradicional

Riesgos financieros, regulatorios, laborales y operativos gestionados por funciones especializadas

Transición digital

La tecnología pasa de ser un soporte a convertirse en el núcleo de la operación y la propuesta de valor

Era actual

El riesgo tecnológico es un riesgo corporativo que exige supervisión directa de la junta

Hoy, toda empresa es tecnológica

Las juntas directivas ya no gobiernan únicamente empresas. Gobiernan organizaciones digitales.

Datos

El activo más crítico de la empresa moderna

Software & IA

Decisiones operativas y estratégicas automatizadas

Nube

Infraestructura crítica tercerizada

Proveedores digitales

Terceros con acceso a activos esenciales

La nueva naturaleza del riesgo empresarial

A los riesgos clásicos se suman serias amenazas intangibles que pueden ocasionar pérdidas catastróficas en horas.

Ransomware

Paralización total de operaciones con extorsión económica

IA & algoritmos

Decisiones automatizadas con sesgos, errores o manipulación

Cadena de suministro

Ataques que ingresan a través de proveedores de confianza

Deepfakes

Fraude de identidad y desinformación corporativa a escala

Computación cuántica

Ruptura de cifrado y obsolescencia de seguridad actual

Dependencia tecnológica

Concentración en pocos proveedores críticos sin alternativas



Ciberataque a Ecopetrol (julio 2026)

- 3,300 cuentas de usuarios, ~1 TB (+327,000 archivos)
- Planilla, datos bancarios, datos biométricos, historiales médicos, credenciales de acceso, e información de miembros de la directiva
- Se logró impedir el cifrado por ransomware
- Afectó sistemas de almacenamiento de archivos en la nube de la compañía y 15 de sus subsidiarias.

Consecuencias

- *The Gentlemen* amenazó con publicar la información
- El 28 de julio Ecopetrol presentó Formulario 6-K ante la SEC
- impactos sobre el negocio, su reputación o sus resultados financieros.

El riesgo tecnológico ya no es asunto de TI

La percepción tradicional

- Asunto técnico, delegado al CTO o CISO.
- La junta aprobaba presupuestos de seguridad sin profundizar en la exposición real.
- Resultado: supervisión insuficiente de uno de los riesgos más destructivos del siglo XXI.

La realidad actual

- Riesgo corporativo de primer orden, con impacto directo en valor, reputación y continuidad.
- Los reguladores internacionales, los tribunales y los inversionistas no aceptan la ignorancia tecnológica como excusa.
- La SEC, la UE y otros organismos ya exigen que las juntas demuestren supervisión activa del riesgo cibernético y digital.

El deber fiduciario de los directores ha evolucionado. La supervisión del riesgo tecnológico ya no es opcional.

Responsabilidad fiduciaria en la era digital



Deber de diligencia

Supervisar activamente los riesgos tecnológicos, el uso de IA, la privacidad de datos y la continuidad del negocio con diligencia razonable



Deber de lealtad

Proteger la información estratégica, los datos personales, la propiedad intelectual y los secretos empresariales frente a amenazas internas y externas



Deber de supervisión

Asegurar la existencia y efectividad de programas de ciberseguridad, resiliencia, cumplimiento digital y gestión estructurada de incidentes



No se espera que un director sea informático.

La competencia tecnológica de la junta no se mide por la profundidad de su conocimiento técnico.

El checklist ejecutivo: IA

La IA opera hoy en procesos de crédito, recursos humanos, logística, atención al cliente y cumplimiento. La junta debe supervisar su uso con la misma rigurosidad que supervisa el riesgo financiero.

1 ¿Quién aprueba el despliegue de sistemas de IA?

Debe existir un proceso formal de aprobación con criterios de riesgo, ética y cumplimiento definidos.

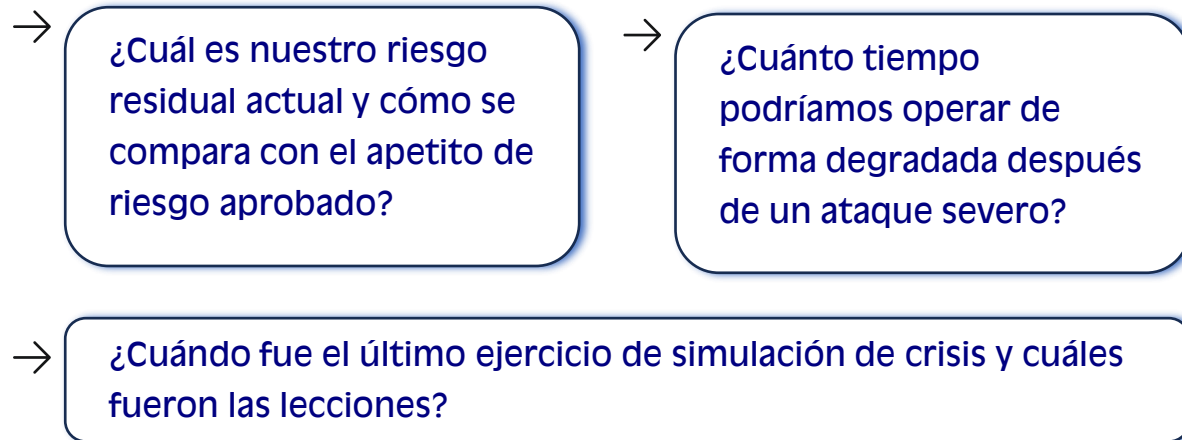
2 ¿Existe un inventario actualizado de sistemas de IA en operación?

Muchas organizaciones utilizan IA sin un registro centralizado ni responsable designado.

3 ¿Quién responde por una decisión automatizada errónea?

La ausencia de un marco de responsabilidad expone a la organización a litigios y sanciones regulatorias.

El checklist ejecutivo: Ciberseguridad



Estas preguntas deben ser respondidas con datos verificables, no con afirmaciones genéricas.

El checklist ejecutivo: Datos



¿Qué información es verdaderamente crítica, dónde está almacenada y quién tiene acceso?



¿Qué proveedor externo podría paralizar nuestra operación si falla o es comprometido?



¿Cuánto tiempo tardaríamos en recuperar operaciones críticas tras un incidente mayor?

Recordemos que estamos hablando de los activos intangibles más valiosos de la organización.

Los pilares de la gobernanza del riesgo tecnológico





Pilar 1: Gobernanza

La junta debe asegurar que existan roles claramente definidos:

- ¿Quién es responsable del riesgo tecnológico?
- ¿Existe un Comité de Riesgo o Comité de Tecnología con mandato formal?
- ¿El CISO reporta con independencia suficiente?



Pilar 2: Información

La junta necesita indicadores confiables, no reportes técnicos inaccesibles.

Los KPIs y KRIs de riesgo tecnológico deben ser comprensibles, comparables y vinculados a decisiones estratégicas.

Una junta bien informada es la primera línea de defensa

Pilar 3: Resiliencia operacional

¿Puede la organización mantener operaciones críticas durante un incidente?

La continuidad del negocio, los planes de respuesta y los tiempos de recuperación no solo deben ser diseñados por TI.

Estos elementos deben ser aprobados y probados regularmente por la junta directiva.

Pilar 4: Confianza digital

Privacidad, ética en el uso de IA, transparencia con clientes y reguladores.

La confianza es un activo estratégico.

Una brecha ética o de privacidad puede destruir en días lo que tomó años construir.

Pilar 5: Supervisión continua

Auditorías independientes,
evaluaciones de terceros,
ejercicios de simulación.

Revisión sistemática de
lecciones aprendidas.

La supervisión no es un
evento anual — es un
proceso permanente con
evidencia documentada.

Métricas que la junta debe conocer

72h

Tiempo máximo tolerable

Horas que la mayoría de empresas puede operar sin sistemas críticos antes de un daño irreversible

\$4.5M

Costo promedio de brecha

Costo global promedio de una violación de datos en 2024, según IBM Cost of a Data Breach Report

60%

Ataques vía terceros

Proporción de incidentes mayores que se originan en proveedores externos con acceso privilegiado

21 días

Tiempo promedio de detección

Tiempo que un atacante permanece dentro de una red antes de ser descubierto en América Latina

**El horizonte
tecnológico avanza
más rápido que los
ciclos de gobierno
corporativo**

Lo que redefinirá la gobernanza antes de 2030



IA agéntica y organizaciones autónomas

Sistemas que toman decisiones sin intervención humana, operando a velocidad y escala sin precedentes



La inminente computación cuántica

Capacidad de romper esquemas de cifrado actuales, haciendo obsoleta la seguridad digital existente



Identidad digital descentralizada

Nuevos modelos de autenticación y soberanía de datos que transformarán el cumplimiento regulatorio

Otras tendencias críticas hacia 2030

1

Regulación global de IA

La UE AI Act, marcos de la OCDE y regulaciones emergentes en LATAM impondrán obligaciones directas sobre las juntas respecto al uso de IA

2

Ciberataques asistidos por IA

Ataques más sofisticados, personalizados y rápidos, generados por IA adversarial, que superarán las defensas tradicionales

3

Soberanía de datos

Restricciones crecientes sobre dónde puede almacenarse y procesarse la información, con impacto directo en estrategias de nube y expansión internacional

4

Automatización de decisiones

Decisiones críticas de negocio delegadas a algoritmos, con implicaciones éticas, legales y reputacionales que la junta debe gobernar

La evolución del mandato de la junta directiva

Siglo XX

Las juntas protegían **activos físicos**: plantas, maquinaria, inventarios, propiedades y capital financiero

1

Presente

Las juntas gobiernan **riesgos algorítmicos**: IA, automatización de decisiones, identidad digital y resiliencia sistémica

2

3

4

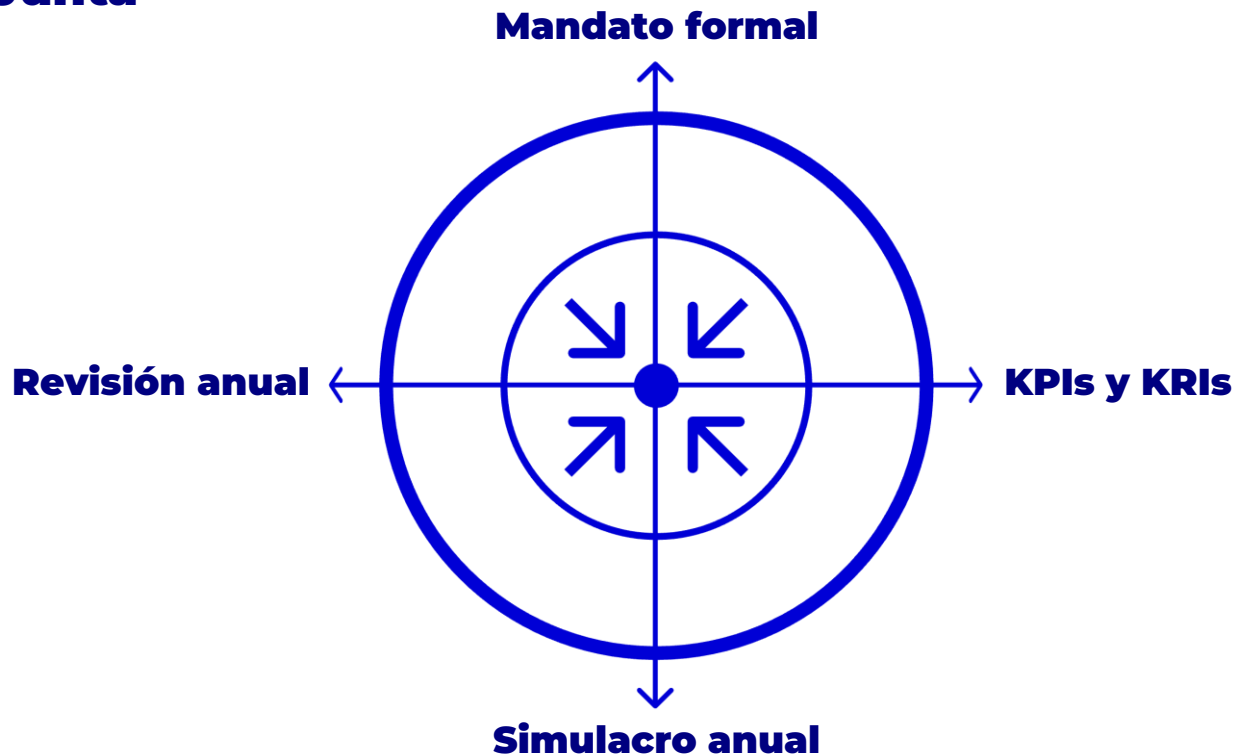
Comienzos del Siglo XXI

Las juntas integraron la supervisión de **activos digitales**: datos, sistemas, infraestructura tecnológica y reputación en línea

Mañana

Las juntas deberán proteger y gobernar las propias **decisiones digitales** — quién decide, cómo se decide y quién responde

Un marco de acción para la Junta



**Una junta efectiva no
necesita entender el código.
Necesita formular las
preguntas que ningún
ejecutivo pueda ignorar.**

:



Preguntas que transforman la supervisión

“

"Si sufrimos un ataque de ransomware mañana, ¿cuánto tiempo tardaríamos en recuperar el 80% de nuestras operaciones críticas?"

“

"¿Cuál es el proveedor externo cuya falla nos causaría mayor daño operacional y qué plan tenemos?"

“

"¿Qué decisiones de negocio están siendo tomadas hoy por algoritmos sin supervisión humana explícita?"



La ventaja competitiva del futuro

La ventaja competitiva del futuro dependerá no solo de quién adopte primero la inteligencia artificial, sino de **quién la gobierne mejor.**

Las juntas directivas que integren hoy la supervisión del riesgo tecnológico en su agenda estratégica no solo protegerán a sus organizaciones — las posicionarán para liderar con confianza en la economía digital.

¡Gracias!

How can I help you today?

¿Cuáles son los datos de contacto de José Vega Gallardo?



Chat

Cowork

Sonnet 5 Medium



José Vega Gallardo



jvega@encrptalaw.com



@panamajoeey



linkedin.com/in/ipjoeey



Si lo deseas, te los doy en un código QR

¡Buena idea! Dame el QR, por favor