Transformación digital y el riesgo cibernético

El reto de una gestión de riesgos ecosistémica

DOI: 10.29236/sistemas.n178a6

Resumen

La transformación digital visualiza en la actualidad como un imperativo estratégico que trasciende lo tecnológico para consolidar ecosistemas digitales de negocio basados en la co-creación de valor y la interconectividad. Esta dinámica de red expande la superficie de ataque, haciendo que la falla sea inevitable lo que implica una transición de la prevención a la ciberresiliencia. En este sentido, el modelo tradicional de gestión de riesgos (ERM) resulta insuficiente frente a entornos NAVI (No lineal, Acelerado, Volátil e Interconectado), por lo cual se introduce el concepto de Gestión de Riesgos Ecosistémica (GRECO). Este enfoque se fundamenta en la interdependencia propia de los ecosistemas, analizando las interacciones complejas y el acoplamiento estrecho de sus componentes. Para materializar esta gestión, se introduce el Índice de Exposición Sistémica Empresarial (IESEM), el cual integra tres elementos claves: la fragilidad estructural, la capacidad de absorción de shocks y la precisión en el mapeo de las dependencias. En conclusión, la GRECO integra al ERM para transformar la gestión de riesgos en una ventaja competitiva que permite a las organizaciones permanecer y prosperar ante la incertidumbre sistémica propia de acelerada transformación digital de las organizaciones modernas.

Palabras clave

Transformación digital, ecosistemas digitales, riesgo ecosistémico, ciberresiliencia, exposición sistémica

Introducción

La transformación digital se ha consolidado en la tercera década del siglo XXI no solo como una tendencia tecnológica, sino como un imperativo estratégico para las organizaciones que buscan innovar, mantenerse vigentes y generar valor sostenible para la sociedad. Para las empresas, este fenómeno representa un cambio fundamental en la forma en que operan, interactúan y generar valor, exigiendo una visión renovada que trasciende la implementación de herramientas tecnológicas para abrazar un cambio de mentalidad integral, generar nuevas experiencias en sus clientes y transformar la manera como se hacen las cosas (Pinzón & Bejarano, 2025).

En este nuevo contexto, los ecosistemas digitales de negocio se convierten en la base fundamental de cualquier transformación digital. Un ecosistema digital permite que redes de empresas, dispositivos y clientes creen valor conjunto, convirtiendo a la organización en un *hub* de capacidades dinámicas para alcanzar nuevas ventajas competitivas basadas en *contenido* (productos e información), *experiencia del cliente* e *infraestructura de plataformas*. La clave reside en la capacidad de diferenciarse ofreciendo algo nuevo y convincente, facilitado por el vehículo digital para crear experiencias distintas, basado en la información detallada de las necesidades y eventos de vida del cliente (Weill & Woerner, 2018).

La complejidad intrínseca de los ecosistemas desplaza el control tradicional que busca mitigar riesgos hacia una dinámica de redes menos predecibles, basado en un apetito de riesgo cibernético empresarial donde las capacidades cibernéticas ya no depende únicamente de sus perímetros internos, sino de la confiabilidad de su cadena de suministro, sus socios y la integridad de sus interfaces de programación de aplicaciones (APIs - *Application Program Interface*) expuestas (Valdez de León, 2019). Lo anterior implica que, en un ecosistema abierto y altamente conectado, algunos ataques serán inevitablemente exitosos; por ello, la capacidad organizacional para anticipar, absorber el impacto y recuperarse rápidamente se convierte en una ventaja competitiva clave no sólo para sobrevivir, sino permanecer.

En consecuencia con lo anterior, se detalla a continuación, desde la perspectiva de una transformación digital, una propuesta de gestión de riesgo cibernético ecosistémica que le permita a las empresas, no sólo crear entornos propicios para la innovación y generación de valor, sino crear portafolios de riesgos cibernéticos estratégicos que debe

gestionar desde su apetito de riesgo cibernético empresarial para concretar, apalancar y defender su promesa de valor, y evolucionar frente a los cambios del entorno y sus amenazas ahora y en el futuro.

Fundamentos de la transformación digital

Los fundamentos de una transformación digital se estructuran sobre siete factores esenciales identificados por la Asociación Nacional de Empresarios de Colombia (ANDI) en su más reciente estudio: liderazgo visionario, una cultura organizacional orientada al cambio, la tecnología como habilitador, la optimización constante de procesos, el desarrollo de talento digital, un marco regulatorio actualizado y una ciberseguridad robusta, elementos que debe funcionar de manera articula dentro de un ecosistema digital para concretar nuevas capacidades y ventajas competitivas (Pinzón & Bejarano, 2025). A continuación se detallan cada uno de estos factores.

Liderazgo visionario: El éxito depende del compromiso real de la alta dirección. El líder actual debe poseer capacidad de aprendizaje (aprender, desaprender y reaprender), curiosidad para entender cómo las tecnologías emergentes impactan los modelos de negocio y abrazar el incierto, como oportunidad dentro del "no saber". Según el MIT (Weill & Woerner, 2018), el reto es decidir si la empresa será un "*Ecosystem Driver*" (líder de ecosistema) o un proveedor modular, lo que requiere una visión que trascienda los silos tradicionales.

Cultura organizacional: La cultura es el punto de partida y de llegada. El reto principal es habilitar el cambio y la mentalidad digital. Se requiere una cultura de experimentación donde "fallar y aprender" sea parte del proceso. Aprender a "fallar bien" implica hacer simulaciones y prototipos en zonas inciertas donde todo resultado suma para crear nuevas oportunidades (Edmondson, 2023). Las organizaciones deben pasar de decisiones basadas en el instinto a una cultura de decisiones fundamentadas en la evidencia, como resultado de "rasgar" el velo de aquello que no se conocía.

Tecnología como habilitador: La tecnología (IA, Grandes datos y analítica, Nube) es el vehículo, no el fin. El reto es evitar la inversión en "maquillaje digital" sin cambiar la estructura subyacente. Esto es, dejarse llevar por la "fascinación" de la tecnología, y no por el cambio real de cómo se hacen las cosas y se cambia la experiencia del cliente. Las empresas deben integrar tecnologías transversales como IA y la analítica de datos para lograr una toma de decisiones en tiempo real.

Optimización de procesos: El objetivo es mejorar la productividad y reducir costos. El reto es evitar la automatización de procesos ineficientes o no digitales; primero se

define la promesa de valor y luego se transforma el proceso. La transición de cadenas de valor lineales a ecosistemas en red es crítica para la eficiencia. Es un ejercicio de construcción de capacidades dinámicas apalancadas en terceros de confianza para crear flexibilidad y adaptación frente a las cambiantes condiciones del entorno de negocios (Teece, 2018).

Talento digital: El capital humano es un centro de gravedad fundamental. El reto es la brecha de habilidades; se estima que el 40% de las competencias actuales serán obsoletas para 2030. Es imperativo invertir en programas de *upskilling* (nuevas habilidades) y *reskilling* (capacitación para nuevos roles) para mantener la competitividad y expandir la capacidad de aprendizaje e innovación que permite evolucionar y sorprender al cliente en un contexto cada vez más digital e interconectado (Pinzón & Bejarano).

Ciberseguridad robusta: Es un habilitador de crecimiento que defiende la promesa de valor de la empresa, para proteger y asegurar su reputación y confianza. El reto es que los ataques y los adversarios son cada vez más sofisticados, donde el paradigma no es "si la organización va a ser atacada", sino "cómo y cuándo se va a concretar el ataque". Por tanto, se debe transitar de una postura preventiva a una proactiva y vigilante basada en la ciberresiliencia, asumiendo que algunos ataques serán exitosos priorizando una limitación de los daños y una recuperación ágil.

Marco regulatorio: Los reguladores y empresas deben colaborar bajo el concepto de "conecta y colabora". El reto es lograr un trabajo conjunto entre los entes gubernamentales, las empresas privadas y los emprendedores para encontrar un equilibrio entre sus intereses y habilitar la innovación. La acción clave es participar en *sandboxes* regulatorios para probar modelos de negocio en entornos controlados y ver tanto las oportunidades como los riesgos, para crear espacios de construcción de regulaciones efectivas, no de las tecnologías en sí mismas, sino de sus aplicaciones (Pinzón & Bejarano, 2025).

Articular estos siete elementos demanda un vista ecosistémica digital que exige una gestión de riesgos que vaya más allá de la mitigación de los riesgos conocidos, de la aplicación de marcos de trabajo y buenas prácticas, y la disminución de la incertidumbre, y pase al reconocimiento del nivel de exposición sistémica de la organización para prepararse frente a efectos dominó, los cuales se convierten en el nuevo *(a)normal* de la dinámica de una organización interconectada.

Fundamentos de los ecosistemas digitales de negocio

Un ecosistema digital de negocios se define como una red dinámica

de organizaciones interactuantes que están conectadas digitalmente y habilitadas por la modularidad, donde cada actor afecta y es afectado por las ofertas de los demás. A diferencia de la era industrial tradicional, donde las empresas operaban en cadenas de valor lineales y cerradas para controlar cada paso del proceso, la transformación digital impulsa una transición hacia sistemas en red coordinados por múltiples plataformas (Skilton, 2016).

Los componentes fundamentales de este modelo son tres: primero, las *plataformas*, que es el bloque base que permite la apertura mediante APIs y asegura la calidad y seguridad del servicio; segundo, los *efectos de red*, que generan un ciclo virtuoso donde el aumento de participantes atrae a más usuarios finales, y viceversa; y tercero, *las expectativas de mercado*, que se refieren a la percepción de los usuarios sobre la viabilidad y permanencia del ecosistema a largo plazo. Para que estos componentes funcionen, se requieren habilitadores críticos como las comunidades de desarrolladores, productos novedosos que inicien la tracción, modelos de ingresos claros (como el "freemium" o ingresos compartidos) y *un modelo de gobernanza* transparente que establezca las reglas de participación y resolución de disputas (Valdez de León, 2019).

La dinámica de estos ecosistemas se basa en la co-creación de valor compartido, donde el éxito del líder de la plataforma depende del éxito de sus participantes. Este fenómeno, conocido como la "empresa invertida", desplaza el enfoque de "fabricar en casa" hacia el "orquestar recursos externos", reduciendo costos de transacción y acelerando la innovación (Valdez de León, 2019).

En este escenario, la ventaja competitiva no reside solo en el producto, sino en convertirse en el "destino" predilecto del cliente para resolver sus problemas y retos. Es concentrarse en responder al menos cuatro preguntas clave:

- ¿Quién son nuestros clientes o grupos de interés a quién servimos?
- ¿Qué problemas o retos ayudamos a resolver a nuestros clientes?
- ¿Qué experiencias distintas entregamos que el cliente no esperaba?
- ¿Qué activos tenemos que prueban que podemos cumplir la promesa?

Todo lo anterior, establece y expande la superficie de ataque disponible para un adversario, por tanto, la ciberseguridad y la ciberresiliencia se convierten en factores fundamentales para enmarcar las operaciones y defender a cada uno de los miembros del ecosistema.

Operar un ecosistema con múltiples terceros y conexiones, muchas veces no conocidas, genera una exposición sistémica para los participantes, donde una falla al proteger la infraestructura equivale a "construir sobre arena" (Pinzón & Bejarano, 2025), arriesgando la confianza digital del cliente, la cual se debe construir cuando las cosas no salen como estaban planeadas (responsabilidad) y no sobre la base de que el sistema no va a fallar (asegurar el cumplimiento).

Gestión de riesgos ecosistémica. El reto de permanecer, evolucionar y prosperar

La aproximación tradicional al riesgo, enfocada en la evaluación de amenazas discretas (y conocidas) y separadas (riesgo financiero, riesgo operativo o riesgo de cumplimiento en áreas), resulta insuficiente en la era actual. Esta visión fragmentada no logra capturar la dinámica esencial del riesgo: la interdependencia (interacción compleja - cuando las fallas de dos o más componentes interactúan de forma inesperada e incomprensible y acoplamiento estrecho - rapidez e inevitabilidad con la que las fallas se propagan) (Perrow, 1999). Un riesgo interdependiente describe una situación crítica en la que la materialización o el impacto de un evento adverso influye significativamente en la probabilidad o severidad de otro evento, incluso a través de dominios aparentemente separados.

En razón con lo anterior, el riesgo ecosistémico se refiere *a la amenaza que surge de la interdependencia compleja y sistémica de los componentes de un ecosistema, donde fallas inesperadas pueden propagarse a través de sus límites previamente definidos*.

Esto es, el resultado de la interacción de fallas que inicialmente eran vistas como aisladas, y que ahora se vinculan por una expansión inesperada del sistema.

A manera de ejemplo, un riesgo ecosistémico en el dominio cibernético se manifiesta cuando una vulnerabilidad tecnológica se combina (interactúa) inesperadamente con factores externos (geopolíticos, ambientales) que, debido al acoplamiento estrecho de la cadena de suministro digital, provoca una interrupción sistémica, que no sólo afecta a una organización sino que crea un efecto contagio que termina comprometiendo a los diferentes actores del ecosistema digital global con efectos inesperados.

En este sentido, en el contexto de la transformación digital la aplicación tradicional de la gestión de riesgos empresariales se queda corta frente a la perspectiva relacional de las organizaciones, que exige conocer que tan acoplada e interconectada está con su entorno, cómo se van a propagar los efectos de los riesgos y que nivel de preparación tiene para disminuir los efectos de la materialización de un evento adverso,

generalmente no esperado (Whitaker, 2016).

Por tanto, para adelantar una gestión de riesgos ecosistémica se proponen algunos elementos básicos para acompañar el proceso de la transformación digital de las empresas.

Fundamentos

- *La inevitabilidad de la falla* – En un malla de relaciones interdependientes en la que operan las organizaciones con terceros de confianza, las fallas son algo natural, por lo cual se hace necesario no sólo conocer y entender cómo es la relación con otros actores, sino prepararse para atender situaciones que se deriven de eventos inesperados.

- *Pedagogía del error* – Los eventos adversos tienen un origen en una decisión humana (alguien no configuró el doble factor de autenticación, alguien configuró un dispositivo sin notificar, alguien dejó de instalar un parche, etc). Por tanto, cuando esas decisiones se dan en medio del ecosistema, sin entender el nivel de interacción y acoplamiento de los diferentes componentes, se presentan situaciones que revelan un escenario de aprendizaje que debe capitalizarse a favor de todo el ecosistema.

- *La ilusión del control* – La aplicación y aseguramiento de los estándares y buenas prácticas establece el conjunto mínimo de acciones que las organizaciones requieren para asegurar sus operaciones de los riesgos conocidos, no son indicadores seguridad y control en un ecosistema donde la incertidumbre presente en las relaciones es dinámica en el tiempo.

Preguntas clave

- *¿Cómo se propaga el riesgo?* – Una inquietud que implica reconocer en el mapa de arquitectura los puntos de mayor acoplamiento e interacción para reconocer posibles efectos dominó en el ecosistema.

- *¿Cómo se contiene el riesgo?* – Una pregunta que invita a diseñar las iniciativas en el ecosistema con una postura de falla segura, que es aquella, que se construye para restringir la propagación del riesgo y el avance del adversario de forma de ganar tiempo y asegurar las condiciones básicas de la operación.

- ¿Cómo se limitan los daños? – Teniendo claras las respuestas a las dos preguntas anteriores, se dimensiona el alcance del evento, en términos de los efectos financieros, de reputación e infraestructura que permitan evaluar y asegurar que las capacidades cibernéticas disponibles mantienen a la organización dentro de su apetito de riesgo cibernético empresarial definido.

Estrategia de análisis

- *Interacciones complejas* - Fallos de múltiples componentes del sistema se vinculan de manera imprevista, no lineal y, frecuentemente, incomprensible para las personas durante un periodo crítico (P.e. Uso de librerías abiertas con posibles fallas de seguridad).

- *Acoplamiento estrecho* - Ausencia de holgura, flexibilidad o amortiguadores entre los componentes de un sistema, lo que resulta en procesos altamente dependientes del tiempo, secuencias de producción invariables y donde solo existe un camino exclusivo para alcanzar el objetivo deseado (P.e. Un punto único de falla en una infraestructura)

Métricas

- *Índice de exposición sistémica empresarial* - El Índice de Exposición Sistémica Empresarial (IESEM) es una métrica de gestión avanzada diseñada para cuantificar la vulnerabilidad inherente de una organización frente al riesgo ecosistémico, basado en:

  ° La fragilidad estructural del sistema (medida por la propensión a la interacción compleja y el acoplamiento estrecho)- *Riesgo inherente*.

  ° La capacidad o incapacidad organizacional para absorber shocks (medida por el balance entre potenciadores y reductores de resiliencia) – *Resiliencia*.

  ° La precisión en el mapeo de interdependencias (evaluando la capacidad de la organización para identificar las correlaciones/dependencias entre riesgos internos y amenazas externas) – *Anticipación*.

Para ejemplificar la aplicación del índice mencionado considere el siguiente caso: una plataforma global de logística automatizada (LogiGlobal). Esta organización opera un ecosistema digital donde convergen sistemas de TI (gestión de pedidos) y TO (tecnología de operaciones) (robots de almacén y grúas portuarias), con una dependencia crítica de APIs de terceros y servicios en la nube. El índice sería como se detalla en la tabla 1.

Conclusiones

La emergencia de la Cuarta Revolución Industrial (4RI), marcada por la convergencia de la Inteligencia Artificial (IA), la automatización y la hiperconectividad, ha reestructurado profundamente los sistemas económicos, políticos y sociales. Esta nueva era de transformación digital, si bien genera oportunidades significativas, introduce también riesgos novedosos y una aceleración de la volatilidad sistémica. En este contexto, la efectividad del *Enterprise Risk Management* (ERM) tradicional queda fuertemente cuestionada dadas las

Tabla 1. *Ejemplo de Aplicación del Índice de Exposición Sistémico Empresarial – IESEM*

Dimensión IESEM	Estado actual en LogiGlobal	Impacto sistémico potencial	Recomendación estratégica
Fragilidad Estructural	**ALTA.** Sistemas hiperconectados con secuencias invariantes y sin amortiguadores temporales.	Un error común puede causar un fallo masivo en cascada incomprensible para los operadores.	Introducir "holgura" y procesos que permitan retrasar pasos críticos sin detener la operación total.
Capacidad de absorción	**BAJA.** Dependencia total de software; carencia de aislamiento manuales o físicos.	Incapacidad de operar en "estado degradado" durante un ataque de ransomware.	Implementar barreras físicas y controles manuales para funciones vitales.
Mapeo de interdependencias	**MEDIO-BAJO.** Desconocimiento de vulnerabilidades en la cadena de suministro de software (SBOM).	Vulnerabilidad ante un "accidente en el ecosistema" por fallos en terceros no identificados.	Exigir transparencia total en la "lista de proveedores de software" a todos los socios tecnológicos.

Nota: Elaboración propia con ideas de Perrow, 1999.

condiciones dinámicas y cambiantes del entorno actual (Thompson et al., 2025).

Por lo tanto, se hace necesaria una transición en la gestión tradicional del riesgo corporativo hacia la gestión del riesgo ecosistémico (GRECO), un enfoque que equipara el marco de riesgos a un ecosistema que debe equilibrar las interdependencias complejas de sus riesgos y procesos mientras se adapta constantemente a un entorno externo, siempre cambiante y en constante evolución. Esto es, mantener un equilibrio dinámico que aprende, desaprende y reaprende de los riesgos emergentes del ecosistema de negocio donde opera, para avanzar en el logro de sus objetivos estratégicos a pesar de eventos inesperados que se materialicen de forma exitosa.

En este sentido, la fragilidad propia de las organizaciones al estar ubicadas en los nuevos ecosistemas digitales de negocio, las habilita, no sólo para reconocerse vulnerables frente a esta nueva realidad de la dinámica empresarial, sino para entender qué nivel exposición sistémica tiene y cómo se prepara para anticipar escenarios probables y posibles que le permitan tomar ventaja de posibles eventos adversos, aumentar su capacidad de amortiguamiento y respuesta, y sobremanera, permanecer y prosperar en entornos por definición hostiles, agrestes y con adversarios con capacidades cada vez más sofisticadas (McCowan et al., 2025).

En consecuencia con lo anterior, se requiere conocer y monitorear el nivel de exposición sistémica de la organización en sus tres variables

clave: fragilidad estructural, capacidad de absorción de shocks y mapeo de interdependencias, que entiende la GRECO como una manera en la cual la organización anticipa amenazas, asigna las inversiones de capital de manera efectiva y opera en un mundo NAVI: No lineal, Acelerado, Volátil e Interconectado. Esto es, refleja el riesgo inherente en el diseño del sistema, asegura el control operacional para su supervivencia y permanencia, y habilita la dirección estratégica y la capacidad de anticipación que le permite prosperar ahora y en el futuro.

La GRECO no compite con el ERM, sino que lo integra y extiende. Es un imperativo estratégico que identifica y gestiona una amenaza sistémica que surge cuando fallas inesperadas en los componentes del ecosistema, que antes se consideraban independientes, se propagan a través de los límites del sistema debido a su interconexión no anticipada, generando disrupciones compuestas y no lineales. Una palanca estratégica para crear valor y ventaja competitiva en medio de un escenario asimétrico y en constante movimiento.

Referencias

Edmondson, A. (2023). *Right kind of wrong: The science of failing well*. Simon & Schuster.

McCowan, S., Krumbmüller, F. & Jaggi, G. (2025). How can reimagining risk prepare you for an unpredictable world? *EY Insights*. https://www.ey.com/en_us/insights/consulting/how-can-reimagining-risk-prepare-you-for-an-unpredictable-world

Perrow, C. (1999). *Normal accidents: Living with high-risk technologies*. Princeton University Press.

Pinzón, S. & Bejarano, M. C. (2025). Guía de transformación digital. ANDI – Asociación Nacional de Empresarios de Colombia. https://www.andi.com.co/home/pagina/19-transformacion-digital

Skilton, M. (2016). *Building digital ecosystem architectures: A guide to enterprise architecting digital technologies in the digital enterprise*. Palgrave Macmillan.

Teece, D. J. (2018). Business models and dynamic capabilities. *Long Range Planning*, *51*(1), 40–49. https://doi.org/10.1016/j.lrp.2017.06.007

Thompson, D., Field, H., Glaser, G & Teixeira, T. (2025). The predictive resilience imperative. Embedding foresight & digital early warning into resilience strategy. *Arthur D'Little Insights*. https://www.adlittle.com/en/insights/viewpoints/predictive-resilience-imperative

Valdez de León, O. (2019). How to develop a digital ecosystem – a practical framework. *Technology Innovation Management Review*, *9*(8), 43–54. https://doi.org/10.22215/timreview/1260

Weill, P. & Woerner, S. (2018). *What's your digital business model?: Six questions to help you build the next-generation enterprise*. Harvard Business Review Press.

Whitaker, L. (2016). Enterprise Risk Management Framework as an Ecosystem. *2016 Enterprise Risk Management Symposium*. Arlington, VA. USA. Society of Actuaries and Casualty Actuarial Society. https://www.soa.org/globalassets/assets/files/resources/essays-monographs/2016-erm-symposium/mono-2016-erm-whitaker.pdf

***Jeimy J. Cano M., Ph.D, CFE, CICA**. Ingeniero y Magíster en Ingeniería de Sistemas y Computación, Universidad de los Andes. Especialista en Derecho Disciplinario, Universidad Externado de Colombia; Ph.D en Business Administration, Newport University, CA. USA. y Ph.D en Educación, Universidad Santo Tomás. Profesional certificado como Certified Fraud Examiner (CFE), por la Association of Certified Fraud Examiners y Certified Internal Control Auditor (CICA) por The Institute of Internal Controls. Profesor Distinguido de la Facultad de Derecho, Universidad de los Andes. Es director de la Revista SISTEMAS de la Asociación Colombiana de Ingenieros de Sistemas –ACIS–.*