# Transformación de la postura

*Sobre ciberseguridad ejecutiva en las juntas directivas: de "a prueba de fallas" a "resistente ante las fallas"*

DOI: 10.29236/sistemas.n179a6

**Resumen**
Las juntas directivas enfrentan una brecha estructural entre la manera en que conciben el riesgo cibernético y la naturaleza real de los sistemas sociotécnicos modernos. La perspectiva dominante, denominada "*fail-safe*" ("a prueba de fallas"), busca prevenir todo falla mediante la implementación de controles formales, generando una falsa sensación de seguridad que expone a las organizaciones a efectos en cascada cuando se materializa la inevitabilidad de la falla. Este artículo propone una transformación conceptual y práctica hacia una postura "*safe-to-fail*" ("resistente ante la falla"), fundamentada en los principios de la ingeniería del caos en seguridad (*Security Chaos Engineering*, SCE) y la resiliencia de sistemas complejos, que permita a los equipos directivos aprender, desaprender y reaprender de las brechas y los incidentes de seguridad, para innovar y moverse rápidamente a pesar de la presencia de eventos cibernéticos adversos pasados, presentes y futuros.

**Palabras clave**
Ciberseguridad ejecutiva, junta directiva, resiliencia sistémica, a prueba de fallas, ingeniería del caos en seguridad,

## Introducción

La digitalización acelerada de las organizaciones ha transformado el riesgo cibernético en uno de los riesgos empresariales más críticos de la década. Sin embargo, la manera en que las juntas directivas comprenden, gobiernan y responden frente a esta realidad permanece inmersa en paradigmas diseñados para un mundo lineal y predecible, que resulta disonante para la complejidad creciente de los sistemas de información modernos.

Según el Informe Global de Riesgos 2024 del Foro Económico Mundial, los ataques cibernéticos y la inseguridad de la información figuran entre los diez riesgos globales más importantes para los próximos dos años, siendo el segundo riesgo corporativo con mayor consenso entre líderes empresariales a nivel global (World Economic Forum, 2024). IBM reporta que el costo promedio global de una violación de datos en 2023 alcanzó los USD 4.45 millones, el valor más alto registrado en los 18 años de historia del informe, con un incremento del 15% respecto a 2020 (IBM, 2023). En América Latina, la región experimentó más de 137.000 millones de intentos de ciberataques en 2022, según Fortinet (2023), lo que representa un aumento significativo frente a años anteriores.

A pesar de estas cifras, la Encuesta Global de Directores 2023 de PwC reveló que solo el 39% de los miembros de juntas directivas encuestados declararon tener alta confianza en la capacidad de su organización para recuperarse de un ciberataque significativo, y sólo el 23% afirmó recibir información suficiente sobre los riesgos cibernétios para ejercer una supervisión efectiva (PwC, 2023). Gartner proyecta que para 2026, el 70% de las juntas directivas incluirán un miembro con experiencia en ciberseguridad, reconociendo la brecha de competencia actual (Gartner, 2023).

Esta asimetría entre la magnitud del riesgo y la capacidad de gobernanza directiva; es el resultado de un paradigma conceptual basado exclusivamente en la aplicación exclusiva de estándares y buenas prácticas que busca lograr una organización “a prueba de fallas”.

Esta perspectiva “a prueba de fallas”, se centra en prevenir todo incidente mediante controles acumulativos, lo que Shortridge y Rinehart (2023) lleva a un “teatro de la seguridad”: contexto que crea la percepción de protección sin lograr una resiliencia real. Cuando la falla, inevitable en sistemas complejos, finalmente ocurre, las organizaciones presentan limitaciones en su capacidad adaptativa para

responder con agilidad a estos eventos.

La propuesta que se detalla en este artículo no recaba en aspectos técnicos de implementación, sino en una reconfiguración de los marcos mentales con los que los miembros de junta conciben el riesgo, la responsabilidad y el éxito en materia de la gestión del riesgo cibernético.

Adoptando los principios de la ingeniería del caos en seguridad, se argumenta que las juntas directivas deben transitar de la búsqueda de la prevención hacia la construcción de capacidades organizacionales y cibernéticas que permitan absorber, adaptarse y aprender de la inevitabilidad de la falla.

## La junta directiva y riesgo cibernético: cuatro tensiones para analizar

Las juntas directivas operan sobre la base de marcos de gobernanza diseñados históricamente para riesgos financieros, operacionales y regulatorios de naturaleza relativamente lineal. El riesgo cibernético, por su naturaleza sistémica, interdependiente y adaptativa, desafía estos marcos en sus fundamentos. Cuatro tensiones estructurales caracterizan esta problemática, que incomodan el saber previo de los miembros de junta sobre la gestión de riesgos empresariales.

*Tensión No.1*: *Complejidad técnica y la capacidad de comprensión directiva*. La mayoría de los miembros de juntas cuentan con limitada formación técnica en ciberseguridad, lo que los hace dependientes de representaciones simplificadas que a menudo distorsionan la naturaleza real del riesgo. Como señala el *National Association of Corporate Directors* (NACD, 2023), el 65% de los directores encuestados indicaron sentirse poco preparados para supervisar el riesgo cibernético de manera efectiva. Esta brecha conduce a la aceptación ciega de métricas basadas en volúmenes, número de vulnerabilidades detectadas, porcentaje de cobertura de controles; en lugar de métricas de desempeño y capacidad orientadas a la resiliencia efectiva, que muestre qué tanto aprende la empresa de sus eventos adversos y cómo se preparar no sólo para sobrevivir, sino para permanecer.

*Tensión No.2*: *Demanda de certezas y la naturaleza incierta del riesgo cibernético*. Los directivos, formados en culturas de toma de decisiones que privilegian las certezas y el control, demandan garantías de seguridad que el entorno de sistemas complejos no puede ofrecer. Shortridge y Rinehart (2023) señalan que las metodologías cuantitativas (como FAIR - *Factor Analysis of Information Risk*), ampliamente utilizadas en programas de seguridad de la información, requieren el conocimiento sobre la frecuencia y magnitud de los eventos cibernéticos adversos que son prácticamen-

te imposibles de calcular con precisión en sistemas complejos y con efectos en cascada, generando una ilusión cuantitativa de control.

*Tensión No.3: Presión productiva y la inversión en resiliencia*. En el ámbito del riesgo cibernético, existe una tensión fundamental: la presión por salir primero en mercados competitivos prioriza la eficiencia inmediata, limitando la inversión en resiliencia y resistencia a los ataques (Rasmussen, 1997). Esta presión lleva al debilitamiento de las defensas cibernéticas, aumentando el apetito de riesgo cibernético empresarial, fuera de la zona definida inicialmente, generando variaciones menores que desencadenan fallos inesperados, erosionando progresivamente la resiliencia incluso cuando los indicadores financieros son positivos.

*Tensión No.4: Respuesta reactiva y la capacidad adaptativa proactiva*. Durante una crisis, el impulso de actuar para retomar el control suele derivar en decisiones impulsivas que ignoran los costos de oportunidad, sacrificando a menudo evidencia forense crucial o la continuidad operativa. Frente a esta reacción, la proactividad exige una preparación deliberada mediante planes probados y el fomento del pensamiento lógico, permitiendo alternativas estratégicas como la "espera vigilante". Equilibrar esta tensión es vital para evitar que la urgencia emocional comprometa la resiliencia organizacional (Dykstra et al., 2022).

Estas cuatro tensiones generan consecuencias institucionales relevantes. Las juntas directivas tienden a aprobar presupuestos de seguridad estructurados alrededor de inversiones en herramientas preventivas y detectivas, sin asignar recursos equivalentes al desarrollo de capacidades de respuesta, recuperación y aprendizaje.

Los modelos de reporte sobre el riesgo de ciberseguridad al directorio hacen énfasis en métricas de estado que no capturan la dimensión dinámica de la resiliencia. Y los marcos de responsabilidad ejecutiva sancionan la falla mediante investigaciones de "causa raíz" que inevitablemente terminan atribuyendo responsabilidad a individuos, en lugar de identificar los factores sistémicos que Reason (1990) denomina "condiciones latentes", aquellas debilidades ocultas, fallas de diseño o decisiones organizacionales deficientes que permanecen inactivas en un sistema durante mucho tiempo. No causan accidentes inmediatos, pero crean brechas en las defensas, facilitando que errores humanos (fallas activas) desencadenen eventos desafortunados.

En síntesis, se presenta en la tabla 1 el resumen de las tensiones entre la junta directiva y el riesgo cibernético.

**Tabla 1.** *Síntesis de la problemática: Junta directiva y riesgo cibernético*

| | Manifestación en la junta directiva | Consecuencia organizacional |
|---|---|---|
| **Competencia técnica** | Dependencia de representaciones simplificadas del riesgo. | Métricas de volumen en lugar de métricas de desempeño. |
| **Marco conceptual** | Paradigma dominante: "a prueba de fallas" | Falsa sensación de seguridad |
| **Estructura de reporte** | Indicadores de estado, no de capacidad adaptativa. | Bajo niveles de inversión en resiliencia. |
| **Cultura de responsabilidad** | Búsqueda de causa raíz individual. | Limitación del aprendizaje organizacional. |
| **Presiones productivas** | Eficiencia sobre resiliencia. | Erosión progresiva de las defensas cibernéticas |
| **Respuesta al incidente** | Sesgo hacia la acción inmediata. | Decisiones emocionales y aumento de costos. |

Nota: Elaboración propia.

## El paradigma "resistente ante fallas" y la ingeniería del caos de la seguridad

Ahern (2011) introduce el concepto "*safe-to-fail*" ("resistente ante fallas") en el contexto del diseño urbano resiliente, argumentando que las estrategias efectivas de gestión del riesgo no buscan eliminar la falla, sino diseñar sistemas donde ésta sea controlable, observable y recuperable. Kim et al. (2017) extienden este marco al dominio de sistemas complejos bajo incertidumbre, identificando que la transición de "*fail-safe"* ("a prueba de fallas") a "safe-to-fail" requiere un cambio en el foco: de prevenir la falla de componentes individuales a mantener las funciones críticas del sistema bajo condiciones adversas.

El paradigma "*safe-to-fail*" representa una transformación conceptual y filosófica en la gestión del riesgo cibernético, desplazando el enfoque de la prevención hacia la resiliencia operativa. A diferencia del modelo tradicional "*fail-safe*", que intenta cerrar toda vulnerabilidad bajo una falsa sensación de seguridad, este enfoque acepta la inevitabilidad de la falla en sistemas sociotécnicos complejos. En lugar de considerar las sorpresas como inaceptables, el diseño "*safe-to-fail*" prioriza la continuidad de las funciones críticas y la reducción de las consecuencias del impacto por encima de la reducción de la probabilidad de daño (Shortridge & Rinehart, 2023).

Este paradigma fomenta una cultura de aprendizaje y flexibilidad mediante la experimentación continua y el uso de la ingeniería del caos, habilitando que el sistema se adapte y recupere su estado operativo con agilidad. Esto es, reemplazar el control administrativo tradicional, propio de la vista exclusiva de las listas de chequeo y verifica-

ción centralizadas, por agentes autónomos y descentralizados, donde las decisiones se toman a nivel local por quienes realizan el trabajo, permitiendo al sistema que se adapte rápidamente a contextos específicos sin esperar una aprobación centralizada. De esta forma, las organizaciones fortalecen su resistencia frente a los ataques, asegurando que el sistema evolucione de forma rápida ante la adversidad (Shortridge & Rinehart, 2023).

La ingeniería de caos en seguridad (SCE – *Security Chaos Engineering*) es una disciplina sociotécnica diseñada para fortalecer la resiliencia mediante la experimentación continua y empírica. Este paradigma aplica el método científico introduciendo proactivamente fallos controlados y condiciones adversas, como errores de configuración o escenarios de ataque, para observar cómo el sistema responde y se adapta en la realidad. Utilizando el enfoque de Evaluación y Experimentación (E&E), la SCE permite descubrir debilidades sistémicas y refinar modelos mentales antes de que ocurran incidentes reales. Su uso sistemático optimiza la capacidad adaptativa, asegurando la continuidad de las funciones críticas frente a entornos digitales complejos (Shortridge & Rinehart, 2023).

En resumen, mientras que el diseño "*safe-to-fail*" busca expandir los umbrales de operación de la seguridad para otorgar un margen de maniobra al sistema frente a eventos inciertos, la SCE utiliza el enfoque de Evaluación y Experimentación (E&E) para demarcar o mapear esos límites y asegurar que las interacciones complejas a través del espacio-tiempo no resulten en fallos en cascada incontrolables. En conjunto, estos dos conceptos permiten que la seguridad/ciberseguridad sea algo que el sistema "hace" activamente (y no sólo "tiene") (Shortridge & Rinehart, 2023), permitiendo que la organización prospere incluso bajo escenarios de ataques continuos.

## Transformación de la perspectiva de la junta directiva: de "a prueba de fallas" a "resistente ante las fallas"

La transformación de la perspectiva directiva en ciberseguridad requiere intervenir tres dimensiones simultáneas: conceptual (cómo los directivos entienden el riesgo cibernético), estructural (cómo se organiza la gobernanza y el reporte), y conductual (cómo actúan los directivos ante un incidente o una decisión de inversión).

El principio rector de esta transformación es que "la resiliencia es algo que un sistema hace, no algo que un sistema tiene" (Shortridge & Rinehart, 2023, p. 20). Para las juntas directivas, esto significa transitar de la pregunta "¿Estamos seguros?" hacia la pregunta "¿Qué tan capaces somos de absorber, adap-

tarnos y aprender cuando algo falla?".

En este contexto, se detallan a continuación cinco (5) estrategias básicas que habiliten la transformación de la mentalidad o perspectiva de la junta directiva de "a prueba de fallas" a "resistente ante las fallas" frente la gestión y gobernanza del riesgo cibernético, con algunas recomendaciones para la aplicación de las mismas.

*Estrategia No.1 Reencuadre del lenguaje y los modelos mentales*. El primer paso de la transformación es modificar el vocabulario directivo sobre ciberseguridad. Los términos "prevención" y "protección" evocan una lógica de fortaleza estática que es conceptualmente incompatible con la naturaleza sistémica de los ecosistemas digitales actuales. Deben introducirse progresivamente términos como "resiliencia", "capacidad adaptativa", "tiempo de recuperación" y "aprendizaje de las fallas", "pedagogía del error".

Esta estrategia debe implementarse mediante sesiones educativas periódicas, en las que el CISO (*Chief Information Security Officer*) ilustre las diferencias entre robustez y resiliencia con ejemplos concretos en el contexto de su sector de negocio. Esto es, entender que la robustez constituye la capacidad estática de resistir perturbaciones para retornar al estado original, mientras la resiliencia representa una capacidad adaptativa dinámica para anticipar, responder y aprender de fallos inevitables.

Recomendación: El reencuadre conceptual puede generar resistencia si los directivos perciben que se está minimizando la gravedad del riesgo. La comunicación debe ser gradual y consistente, enfatizando que el paradigma "*safe-to-fail*" no reduce la urgencia de la inversión, sino que la orienta de manera más efectiva.

*Estrategia No.2 Rediseño del marco de reporte directivo*. El marco de reporte del CISO a la Junta Directiva debe ser rediseñado para capturar capacidades de resiliencia en lugar de estados de control. Forsgren et al. (2018) ofrece las métricas DORA[1] (*Digital Operational Resilience Act*) como punto de partida: frecuencia de despliegue (velocidad de respuesta adaptativa), tiempo de entrega de cambios (agilidad organizacional), tasa de fallas luego de cambios (calidad del proceso), y tiempo de restauración del servicio (capacidad de recuperación).

1 Digital Operational Resilience Act (DORA) - La Ley de Resiliencia Operativa Digital (DORA) es una normativa introducida por la Unión Europea para reforzar la resiliencia digital de las entidades financieras. Entró en vigor el 17 de enero de 2025 y asegura que los bancos, las compañías de seguros, las empresas de inversión y otras entidades financieras puedan resistir, responder y recuperarse de las interrupciones de las TIC (tecnologías de la información y la comunicación), como los ciberataques o los fallos del sistema. Fuente: https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Complementariamente, el marco de reporte debe incluir evidencia experimental proveniente de ejercicios de ingeniería de caos en seguridad. Shortridge y Rinehart (2023) proponen el concepto de "confianza basada en evidencia": cada experimento genera datos concretos sobre cómo el sistema responde a condiciones adversas.

Recomendación: La transición de métricas de volumen a desempeño puede generar incomodidad inicial. Es necesario preparar al directorio para interpretar el incremento de la visibilidad de las fallas o brechas de seguridad como un indicador de madurez, no de deterioro de la postura de ciberseguridad.

*Estrategia No.3 Incorporación de la tolerancia a la falla en el apetito de riesgo*. Las declaraciones de apetito de riesgo deben incorporar explícitamente dimensiones de tolerancia a la falla: ¿Qué magnitud de interrupción es aceptable? ¿Durante cuánto tiempo? ¿Afectando qué funciones críticas? Shortridge y Rinehart (2023) proponen enmarcar la resiliencia en términos de funcionalidad crítica, obligando a los directivos a especificar qué puede ser sacrificado temporalmente para proteger la promesa de valor de la empresa.

Redefinir el apetito, no como la ausencia de incidentes, sino como la capacidad adaptativa para absorber y recuperarse de eventos adversos preservando las funciones críticas, permite construir "capacidad de amortiguación" y emplear la ingeniería de caos para validar los umbrales de operación empresarial, transformando el riesgo en una competencia operativa verificable.

Recomendación: La definición de lo "aceptable" requiere alineación entre junta, alta gerencia y equipos operativos alrededor de la promesa de valor empresarial. Las declaraciones desconectadas de la realidad operativa generan expectativas directivas que erosionan la confianza del cliente y de los accionistas.

*Estrategia No.4 Institucionalizar el aprendizaje post-incidente*. La junta directiva debe institucionalizar revisiones post-incidente "sin buscar culpables" como práctica estándar de gobernanza. Shortridge y Rinehart (2023) sugieren que las revisiones deben privilegiar los factores sistémicos de los eventos analizados como pueden ser presiones productivas, propiedades del diseño, brechas de observabilidad, en lugar de errores individuales.

La implementación de una cultura que "no busca culpables" en la gestión del riesgo cibernético exige una transformación estructural que priorice la seguridad psicológica sobre el castigo individual, permitiendo que el personal reporte fallas sin temor a represalias. Este paradigma desestima el "error humano"

como causa raíz, tratándolo en cambio como un síntoma de deficiencias sistémicas y de diseño en los sistemas.

Recomendación: La cultura que "no busca culpables" puede ser percibida como ausencia de responsabilidad por las acciones ejecutadas. Es fundamental distinguir entre responsabilidad sistémica, la organización aprende y mejora, y la culpa individual. La primera fortalece la resiliencia; la segunda la deteriora (Shortridge & Rinehart, 2023).

*Estrategia No.5 Supervisión directiva de la capacidad experimental*. La junta directiva debe incluir en su agenda la revisión de resultados de los ejercicios de la ingeniería de caos en seguridad. Esta supervisión no implica que los directivos diseñen o ejecuten experimentos; implica que demanden evidencia experimental y práctica de los resultados de las pruebas realizadas como estándar de gobernanza y forma de retar la postura de ciberseguridad actual. La pregunta directiva fundamental debe ser:

**Tabla 2**. *Síntesis de estrategias de transformación directiva*

| Estrategia | Objetivo | Ventajas | Retos | Métricas de seguimiento |
|---|---|---|---|---|
| **1. Reencuadre de modelos mentales** | Modificar el vocabulario directivo sobre riesgo cibernético | Mayor comprensión sistémica; decisiones más contextualizadas | Resistencia al cambio conceptual; percepción de minimización del riesgo | Calidad de las preguntas directivas en sesiones de reporte |
| **2. Rediseño del marco de reporte** | Capturar capacidades de resiliencia, no estados de control | Decisiones de inversión más efectivas; visibilidad real del riesgo | Incomodidad con métricas que revelan más vulnerabilidades | Adopción de métricas DORA; cobertura de experimentos |
| **3. Apetito de riesgo con tolerancia a la falla** | Especificar funcionalidades críticas y niveles aceptables de interrupción | Priorización estratégica de la inversión | Dificultad para acordar qué es "aceptable" | Tiempo de recuperación de funciones críticas en ejercicios |
| **4. Institucionalizar el aprendizaje post-incidente** | Extraer conocimiento sistémico de cada incidente | Cultura de mejora continua; supresión reducida de información | Confusión entre cultura "sin buscar culpables" y ausencia de responsabilidad | Número de mejoras sistémicas implementadas post-incidente |
| **5. Supervisión de capacidad experimental** | Incluir evidencia de ingeniería del caos en seguridad en la agenda directiva | Decisiones de inversión basadas en comportamiento observado | Interpretación negativa de los hallazgos del SCE. | Frecuencia y cobertura de ejercicios; acciones tomadas en los sistemas |

Nota: Elaboración propia.

"¿Qué hemos aprendido sobre nuestros sistemas este trimestre que antes no sabíamos?"

Recomendación: Los primeros ejercicios frecuentemente revelan comportamientos adversos con efectos sistémicos (en cascada) inesperados. Los directivos deben estar preparados para recibirlos sin interpretarlos como un fallo del equipo de seguridad, sino como el propósito mismo del ejercicio y como un "foro de la verdad" sobre la realidad de la ciberseguridad de la empresa.

En la tabla 2, se presenta una síntesis de las cinco estrategias planteadas.

## Apropiación del paradigma "resistente ante las fallas": recomendaciones para los miembros de la junta directiva

Las siguientes recomendaciones, detalladas en la tabla 3, están orientadas para que los miembros individuales de la junta directiva adopten conductas concretas que permitan una mejor apropiación de la perspectiva "*safe-to-fail*" en su práctica cotidiana de gobernanza.

## Conclusiones

La gestión moderna del riesgo cibernético ha llegado a un punto de inflexión donde las estrategias tradicionales de defensa conocidas resultan insuficientes ante la naturaleza dinámica de las amenazas digitales y el avance de la inteligencia artificial como herramienta base de los atacantes. La transformación necesaria para las organizaciones no es sólo tecnológica, sino que exige un cambio de paradigma en la toma de decisiones estratégicas que debe ser liderado desde la junta directiva. Esta transformación implica transitar de una mentalidad de prevención de riesgos conocidos hacia una de resiliencia operativa y aprendizaje continuo en un entorno de amenazas incierto y asimétrico (Smeets, 2022).

El paradigma "*fail-safe*" ("a prueba de fallas") ha sido el pilar de la ciberseguridad tradicional, basándose en la premisa de que los riesgos pueden predecirse y controlarse con precisión, y bloquearse mediante las herramientas tecnológicas disponibles. Este enfoque, enraizado en una visión determinista de la ciencia del siglo XX, busca eliminar vulnerabilidades y amenazas antes de que ocurran, operando bajo un factor de seguridad formalmente diseñada (Shortridge & Rinehart, 2023).

En contraste, el paradigma "*safe-to-fail*" ("resistente a las fallas") representa una evolución necesaria hacia la resiliencia operativa, aceptando la inevitabilidad de la falla en entornos sociotécnicos complejos y evolución permanente. Este modelo de diseño estratégico se enfoca en permitir que la infraestructura falle de manera contenida, priorizando la minimización de las consecuencias del impacto por encima de la simple reducción de la

**Tabla 3**. *Recomendaciones para apropiar el paradigma "resistente ante las fallas" en las juntas directivas*

| Estrategia | Objetivo principal | Preguntas clave para la Junta |
|---|---|---|
| Reformulación del Cuestionamiento | Pasar de un enfoque de protección pasiva a uno de aprendizaje y respuesta. | • ¿Qué aprendimos sobre nuestras capacidades de respuesta este trimestre?<br>• ¿Cuánto tiempo tardamos en recuperar nuestras funciones críticas?<br>• ¿Qué hipótesis sobre nuestros sistemas resultaron incorrectas? |
| Reportes basados en evidencia | Incentivar la inversión en capacidades de aprendizaje organizacional. | • ¿Qué hipótesis de la aplicación de la ingeniería del caos en seguridad se probaron recientemente?<br>• ¿Qué descubrimientos se hicieron y qué mejoras concretas se implementaron luego de las pruebas? |
| Definición de prioridades críticas | Establecer una estrategia "*safe-to-fail*" ("resistente ante fallas"). | • ¿Qué funciones del negocio son verdaderamente vitales?<br>• ¿Qué procesos pueden suspenderse para proteger la promesa de valor de la empresa? |
| Cultura de revisión "sin buscar culpables" | Fomentar el aprendizaje sistémico tras un incidente. | • ¿Nuestro marco actual de responsabilidad incentiva la transparencia o el ocultamiento de errores?<br>• ¿Cómo estamos transformando las fallas identificadas en mejoras del sistema? |
| Calibración del apetito de riesgo | Alinear la estrategia con las capacidades reales de la empresa. | • Si nuestra meta de recuperación es de 24 horas pero los ejercicios muestran 72, ¿debemos ajustar la declaración o aumentar la inversión? |
| Diversidad de competencias | Fortalecer la supervisión experta del riesgo cibernético. | • ¿Contamos con directores con experiencia técnica suficiente para cuestionar la estrategia de ciberseguridad?<br>• ¿Qué mecanismos de asesoría experta tenemos hoy? |
| Práctica de "espera vigilante" | Evitar decisiones emocionales por sesgo de acción durante crisis. | • ¿Cuál es el costo real de esperar 30 minutos más para recopilar información antes de aprobar una respuesta drástica? |

Nota: Elaboración propia.

probabilidad de daño. Un diseño "*safe-to-fail*" privilegia la modularidad, la diversidad funcional y el empoderamiento de agentes autónomos descentralizados que pueden responder ágilmente a contextos locales de crisis (Shortridge & Rinehart, 2023).

De otra parte, la Ingeniería del caos en seguridad constituye la disciplina práctica para operacionalizar

esta filosofía "*safe-to-fail*" mediante el uso sistemático del método científico. Su objetivo primordial es generar "memoria muscular" tanto en los sistemas técnicos como en los equipos humanos, dosificando proactivamente fallos controlados y escenarios de ataque para observar la respuesta real del sistema. A diferencia de las pruebas de penetración tradicionales, que validan resultados conocidos, la SCE busca descubrir los "desconocidos desconocidos" y debilidades sistémicas ocultas antes de que se conviertan en incidentes que afecten al cliente, a la reputación corporativa y la promesa de valor de la empresa (Shortridge & Rinehart, 2023).

Finalmente, esta transformación impone retos críticos para los miembros de la junta directiva, quienes deben liderar el cambio cultural hacia una organización resiliente y luego antifrágil. Por tanto, el desafío es mitigar el "sesgo de acción" reactivo tras un incidente, evitando la implementación de sanciones o medidas tecnológicas costosas que privilegian la falsa sensación de seguridad (Dykstra et al., 2022).

Solo mediante la aceptación de la falla como una condición normal de los sistemas complejos, y un enfoque en basado en la flexibilidad de la respuesta y la capacidad adaptativa, podrá la junta directiva asegurar la viabilidad y permanencia de la organización en un entorno digital agresivo y competitivo.

La ciberseguridad del futuro no será construida sobre la ilusión del control, sino sobre la sabiduría de los sistemas que saben cómo fallar bien, esto es, *aprender* de lo que sabe y conoce en la actualidad sobre las vulnerabilidades para asegurar el resultado esperado, *desaprender* aquello que no suma o aporta, o ha quedado obsoleto de la práctica de seguridad y control vigente, para incorporar los nuevos retos, contextos y escenarios no lineales, acelerados, volátiles e interconectados donde se pueden perseguir objetivos valiosos para la empresas, y así *reaprender*, esto es, conectar los puntos inconexos y puntos ciegos identificados hasta ahora para avanzar en las asimetrías que propone el adversario (Gundu, 2024).

## Referencias


Ahern, J. (2011). From fail-safe to safe-to-fail: Sustainability and resilience in the new urban world. *Landscape and Urban Planning*, *100*(4), 341–343. https://doi.org/10.1016/j.landurbplan.2011.02.021

Dykstra, J., Stevens, R., & Olson, L. (2022). Opportunity cost of action bias in cybersecurity incident response. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, *66*(1), 1116–1120. https://doi.org/10.1177/1071181322661368

Forsgren, N., Humble, J. & Kim, G. (2018). *Accelerate: The science of lean software and DevOps: Building and scaling high performing technology organizations*. IT Revolution Press.

Fortinet. (2023). 2023 global threat landscape report. https://www.fortinet.com/blog/threat-research/2023-global-threat-landscape-report

Gartner. (2023). Gartner predicts 70% of boards will have a dedicated cybersecurity committee by 2026. *Gartner Research.* https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-predicts-70-percent-of-boards-will-have-a-dedicated-cybersecurity-committee-by-2026

Gundu, T. (2024). Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture Model. *Proceedings of The 19th International Conference on Cyber Warfare and Security*, *19*(1), https://doi.org/10.34190/iccws.19.1.2177

IBM. (2023). Cost of a data breach report 2023. https://www.ibm.com/reports/data-breach

Kim, Y., Newman, G. & Güneralp, B. (2017). Fail-safe and safe-to-fail adaptation: Decision-making for urban flooding under climate change. *Climatic Change, 145*(3), 397–412. https://doi.org/10.1007/s10584-017-2100-5

National Association of Corporate Directors - NACD. (2023). *2023* NACD director survey: Cybersecurity oversight. *NACD*. https://www.nacdonline.org/globalassets/public-pdfs/nacd_cyber-risk-oversight-handbook_pages_web-compressed.pdf

PwC. (2023). 2023 global digital trust insights survey. *PricewaterhouseCoopers*. https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html

Rasmussen, J. (1997). Risk management in a dynamic society: A modelling problem. *Safety Science,* 27(2–3), 183–213. https://doi.org/10.1016/S0925-7535(97)00052-0

Reason, J. (1990). *Human error.* Cambridge University Press. https://doi.org/10.1017/CBO9781139062367

Shortridge, K. & Rinehart, A. (2023). *Security chaos engineering: Sustaining resilience in software and systems*. O'Reilly Media.

Smeets, M. (2022). *No shortcuts. Why states struggle to develop a military cyber-force*. New York, NY. USA: Oxford University Press.

World Economic Forum. (2024). Global risks report 2024. *WEF*. https://www.weforum.org/reports/global-risks-report-2024/

***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–.*