Brechas de ciberseguridad en la administración de las instalaciones

Dra. Erika Pärn Jeffrey Saunders

INTRODUCCIÓN

Este informe presenta un resumen ejecutivo exhaustivo de las principales conclusiones del Análisis Comparativo Cualitativo de Conjuntos Difusos (fsQCA) sobre la preparación en ciberseguridad en el ámbito de la gestión de instalaciones. El análisis se fundamenta en datos obtenidos de encuestas realizadas a miembros de la IFMA y se enfoca en cómo las diversas combinaciones de preparación interna, presiones externas y barreras percibidas afectan la probabilidad de una brecha de ciberseguridad. Nuestra encuesta, la más amplia de su tipo distribuida entre gestores de instalaciones a través de la IFMA, tiene como objetivo contribuir de manera significativa a la comprensión actual de los desafíos y la preparación en ciberseguridad en el sector de la gestión de instalaciones.

En el momento de la distribución, la IFMA contaba con más de 24.000 miembros, profesionales en la gestión de instalaciones de más de 100 países. La encuesta fue enviada a 15.022 miembros que gestionan activamente instalaciones, excluyendo a consultores, estudiantes, académicos y otros miembros afiliados a FM que no son practicantes.

Esta sección transversal de miembros ofreció un marco de muestreo óptimo de profesionales informados que abarcan diversas organizaciones e industrias que emplean servicios de gestión de instalaciones.
El cuestionario final fue transformado a un formato electrónico a través de la plataforma de encuestas en línea Qualtrics, con el fin de facilitar su distribución y el registro de respuestas. Se otorgó acceso a la encuesta anónima a 15.022 miembros de la IFMA mediante campañas de correo electrónico y promoción en línea durante un periodo de cuatro meses (abril-julio de 2023). Un total de 372 encuestados completaron la encuesta.

Al concluir la recopilación de datos, la encuesta recibió 372 respuestas. No obstante, para el análisis de fsQCA, filtramos las respuestas e incluimos únicamente aquellos casos en los que se presentó una brecha de ciberseguridad.

Se omitió la información relativa a las violaciones de seguridad. Se excluyeron las respuestas en las que los profesionales indicaron no haber experimentado ninguna infracción o no tener conocimiento de si se habían producido. Asimismo, se eliminaron las respuestas incompletas de la muestra.

Tras esta evaluación, se procesaron 200 respuestas completas y válidas sobre incidentes de ciberseguridad para fsQCA. El enfoque específico en los escenarios de brechas proporcionó la información necesaria para identificar las configuraciones que generan vulnerabilidades. Los 200 casos seleccionados ofrecieron un valioso conjunto de datos sobre la complejidad de la preparación y las repercusiones de la ciberseguridad en contextos de gestión de instalaciones globales.

Este estudio aporta de manera significativa al ámbito de la ciberseguridad en la gestión de instalaciones al revelar diez configuraciones únicas que frecuentemente conducen a incidentes cibernéticos. Identificamos estas configuraciones a través de un análisis exhaustivo de 200 respuestas a encuestas de profesionales del sector. Nuestro estudio trasciende las meras relaciones de causa y efecto, indagando en cómo interactúan múltiples dimensiones para incrementar el riesgo de ciberseguridad.

A través de un meticuloso fsQCA, hemos evaluado las percepciones de los encuestados en seis factores internos y externos: conocimiento de la ciberseguridad (KDIG), niveles de amenaza percibidos, preparación para incidentes cibernéticos (TCYBERSEC), barreras para una ciberseguridad efectiva (BAR), criticidad de los activos (CRT) y el impacto de la turbulencia tecnológica (TECHTURB) y el dinamismo del mercado (MARKDYN). Este enfoque multidimensional nos ha permitido identificar patrones causales complejos que no son evidentes al analizar estas dimensiones de manera aislada. La lista completa de las variables medidas se presenta en la tabla de la página siguiente.

Conocimiento

KDIG | ¿Cuáles son tus conocimientos sobre las aspiraciones de transformación digital de tu empresa?

KCYBSEC | ¿Cómo calificarías tus conocimientos sobre la ciberseguridad de su organización?

Percepción de riesgos

Clasifique las siguientes amenazas inminentes que enfrentan sus instalaciones.

TFIN | Riesgos financieros (por ej.: inflación, recesión, inversión, etc.)

TOPR | Riesgos operativos (por ejemplo, interrupciones en las operaciones debido a huelgas o conflictos laborales)

TCYBERSEC | Amenazas de ciberseguridad (por ejemplo, disruptivas para sistemas de construcción como resultado de errores de actualización o ataques)

Preparación para la ciberseguridad

Indique en qué grado está de acuerdo o en desacuerdo con las siguientes afirmaciones respecto a la preparación de su empresa en términos de ciberseguridad para sus instalaciones.

CYBERSECPOL | Nuestra entidad cuenta con una política definida de ciberseguridad.

PREPTRN | Nuestra organización ofrece formación anual. Formación y sensibilización en ciberseguridad.

PREPPOS | La formación en ciberseguridad de nuestra organización y los programas de concienciación se implementan de tal manera que fomenten un cambio positivo entre los usuarios finales.

PREPBMS | Política de ciberseguridad de la organización Incluye sistemas de gestión y operación de edificios.

Percepción de obstáculos

¿En qué medida se consideran los siguientes aspectos como obstáculos para la ciberseguridad de sus instalaciones?

BARLOI | Grado de inversión en concienciación y preparación en ciberseguridad

BARRA | Ventaja relativa en ciberseguridad

BARLEG | Sistemas legados

BARCOMP | Interoperabilidad de sistemas

BARDTMNG | Administración de datos

BARKNG | Conocimientos y competencias de los empleados en ciberseguridad

BARMNGT | Compromiso de la alta dirección con los activos ciberseguros

BARMA | Aceptación del mercado (cliente)

BARTEC | ¿En qué medida se consideran los siguientes aspectos como obstáculos para la ciberseguridad en sus instalaciones? - Proveedores y socios tecnológicos

Percepción de la gravedad de los incidentes

Si su edificio es objeto de un ataque por parte de piratas informáticos, ¿qué tan crucial sería cada uno de los siguientes factores?

CRTFINL | Un incidente provoca una pérdida financiera.

CRTILOS | La información confidencial se encuentra comprometida o robada

CRTBR | La imagen o reputación de la empresa se ve afectada

CRTLOC | La empresa pierde clientes

CRTLOP | La red se ralentiza o se vuelve ineficaz no disponible durante un período de tiempo (pérdida de productividad)

CRTIP | Propiedad intelectual, secretos comerciales u otros activos sustraídos.

CRTSUP | La empresa pierde socios y proveedores

CRTHL | Vidas humanas en riesgo

CRTCS | Empresa en litigio

Turbulencia tecnológica

Indique en qué grado está de acuerdo o en desacuerdo con las siguientes afirmaciones sobre la transformación tecnológica en la industria FM.

TECHTURB1 | La tecnología de la información en nuestra industria evoluciona con rapidez.

TECHTURB2 | Tecnologías de la información en nuestra industria que ofrecen oportunidades.

TECHTURB3 | Una amplia gama de nuevos productos y servicios Las ideas se han materializado gracias a los avances tecnológicos en nuestra industria.

Dinamismo del mercado

Indique el grado de conformidad con las siguientes afirmaciones sobre la transformación del mercado en la industria del FM.

MARKDYN1 | En nuestro sector, las preferencias de servicio de los clientes experimentan cambios significativos a lo largo del tiempo.

MARKDYN2 | Nuestros clientes buscan nuevos servicios todo el tiempo.

MARKDYN3 | Los nuevos clientes suelen presentar necesidades en relación con los productos que difieren de las de nuestra clientela actual.

MARKDYN4 | Las exigencias de los clientes son muy diversas. diversos segmentos de clientes.

HALLAZGOS

El análisis fsQCA revela diversos factores significativos que desempeñan un papel fundamental en la determinación de la preparación de una organización en el ámbito de la ciberseguridad. Estos factores abarcan la preparación operativa, la preparación en ciberseguridad, la solidez financiera y las presiones externas, tales como las turbulencias tecnológicas y la dinámica del mercado. Asimismo, las barreras percibidas, incluidas las legales, organizativas y basadas en el conocimiento, afectan de manera considerable la vulnerabilidad de una organización frente a las ciberamenazas. Las secciones siguientes examinan estos hallazgos con mayor profundidad.

Comparación de factores internos y externos.

El análisis revela que factores internos, como la preparación operativa y la ciberseguridad, tienen un impacto significativo en la disminución de la probabilidad de una brecha cibernética en comparación con las presiones externas (véase la figura 1). No obstante, factores externos, como la turbulencia tecnológica y la dinámica del mercado, también juegan un papel importante, especialmente cuando la preparación interna es deficiente. La figura 1 ilustra la presencia (1) o ausencia (0) de factores críticos, tales como financieros, operativos, de infraestructura de TI, entre otros, en diversas configuraciones.

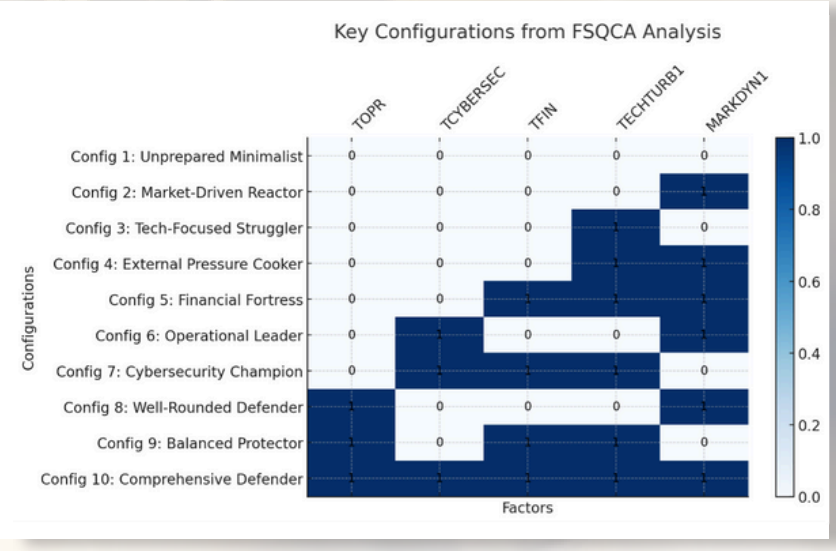
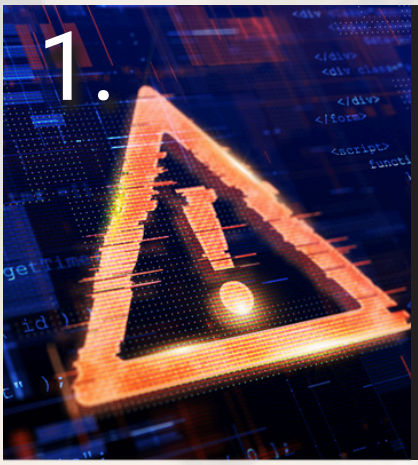


Fig. 1 Comparación de factores internos y externos. *Las barras indican la presencia (1) o la ausencia (0) de factores de criticidad como financieros, operativos, de infraestructura tecnológica, entre otros, en diversas configuraciones.*

A través del análisis fsQCA, se constató que las organizaciones con una sólida preparación interna (preparación operativa y de ciberseguridad) presentaban significativamente menores probabilidades de sufrir una violación cibernética, sin importar presiones externas.

Por otro lado, las organizaciones que dependían de factores externos, como la dinámica del mercado o las turbulencias tecnológicas, sin contar con sistemas internos robustos, enfrentaban un mayor riesgo.

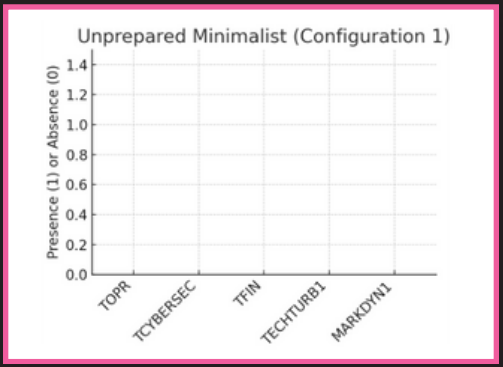
ANÁLISIS DE CONFIGURACIONES:



Configuración 1:
"Minimalista sin preparación"

• Descripción: Ninguno de los factores están presentes. Esta es la configuración más susceptible, ya que representa una organización que carece de preparación tanto interna como externa.

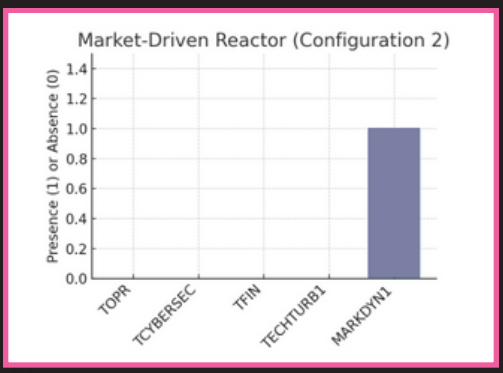
• Factores: Todos los factores están ausentes (0).



Configuración 2:
"Reactor impulsado por el mercado"

• Descripción: Exclusivamente dinámica del mercado (MARKDYN1) está presente, lo que sugiere una organización que responde a las presiones externas del mercado sin una adecuada preparación interna.

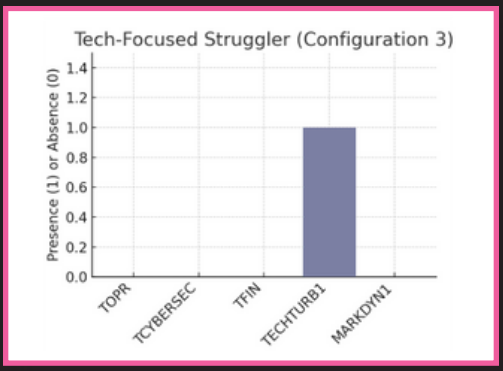
• Factores: Los factores internos están ausentes, mientras que MARKDYN1 se encuentra presente (1).



Configuración 3:
"Luchador enfocado en la tecnología"

• Descripción: Exclusivamente Technology Turbulence está presente (TECHTURB1), lo que sugiere una organización afectada por la inestabilidad tecnológica externa sin respaldo interno.

• Factores: TECHTURB1 está presente (1), mientras que los factores internos están ausentes.

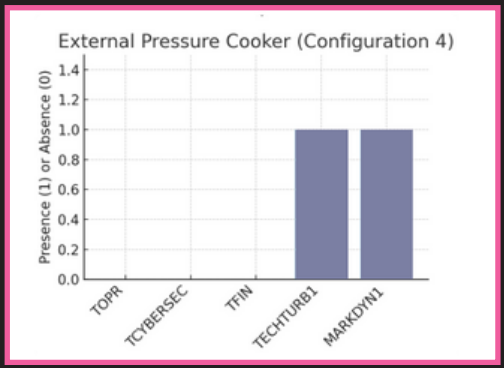


CONTINÚA EN LA PÁGINA SIGUIENTE

Configuración 4:
"Olla de presión externa"

• Descripción: Los dos factores externos (MARKDYN1 y TECHTURB1) están presentes, lo que indica una organización sometida a presión externa con escasa preparación interna.

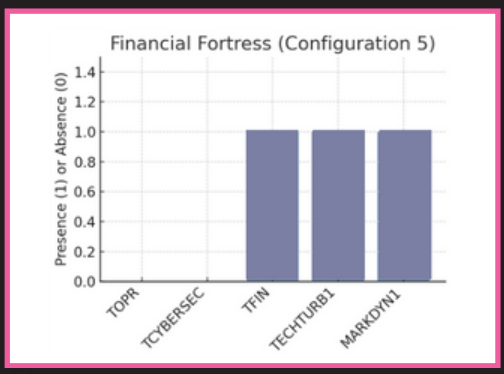
• Factores: Los factores externos están presentes; los factores internos están ausentes.

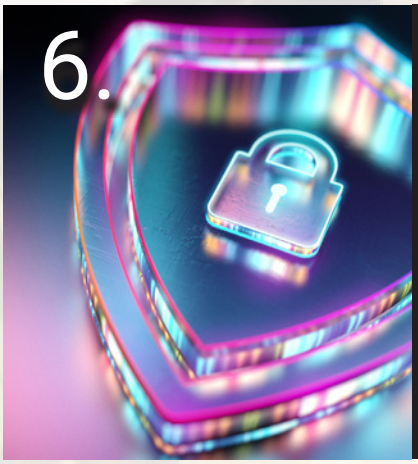


Configuración 5:
"Solidez financiera"

• Descripción: Planificación financiera (TFIN) está presente, lo que sugiere una organización con un sólido respaldo financiero, aunque enfrenta presiones externas derivadas de la tecnología y los mercados.

• Factores: TFIN, TECHTURB1 y MARKDYN1 están presentes; los factores internos están ausentes.

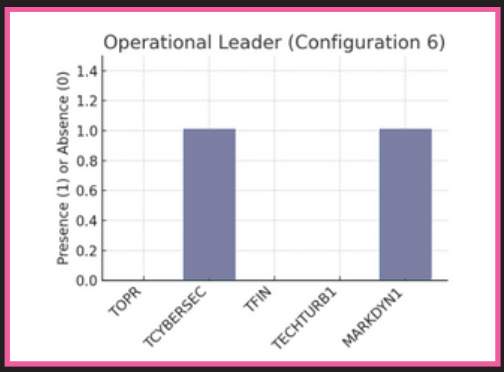




Configuración 6:
"Director Operativo"

• Descripción: Preparación operativa. (TOPR) está presente, lo que sugiere un enfoque en las operaciones internas, aunque carece de preparación externa.

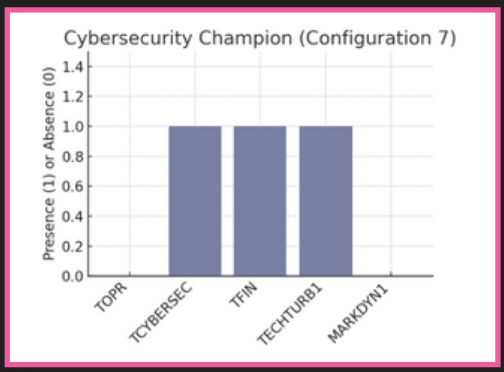
• Factores: TOPR está presente. Los factores externos están ausentes.



Configuración 7:
"Campeón en Ciberseguridad"

• Descripción: Seguridad Cibernética La preparación (TCYBERSEC) es robusta, lo que resalta una organización centrada en la defensa de la ciberseguridad interna sin influencias externas.

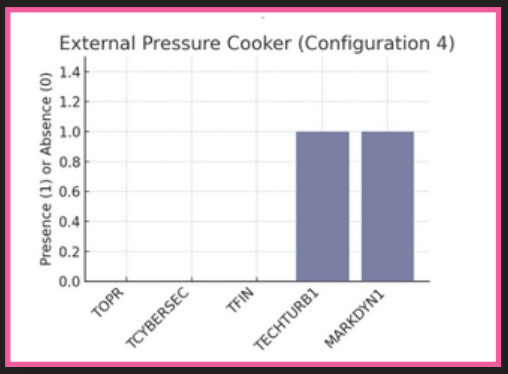
• Factores: TCYBERSEC se encuentra presente. No hay factores externos.



Configuración 8:
"Defensor polivalente"

• Descripción: Tanto TOPR como TCYBERSEC está presente, representando una organización internamente bien estructurada, aunque los factores externos son inexistentes.

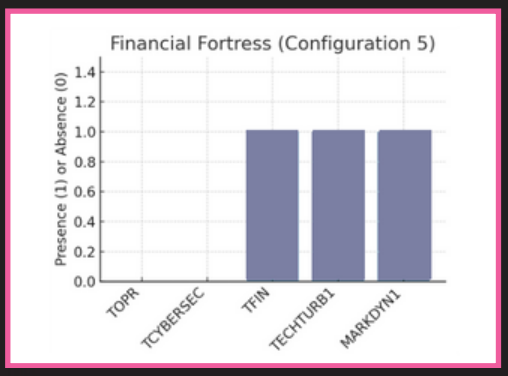
• Factores: TOPR y TCYBERSEC están presentes.



Configuración 9:
"Protector balanceado"

• Descripción: TOPR, TFIN y MARKDYN1 está presente, exhibiendo un equilibrio entre las operaciones internas, la planificación financiera y la reacción del mercado externo.

• Factores: TOPR, TFIN y MARKDYN1 están presentes.



Configuración 10:
"Defensor integral"

• Descripción: Todos los internos y Existen factores externos que sugieren que la organización posee una sólida fortaleza interna y es capaz de responder a las presiones externas.

• Factores: Se encuentran presentes todos los factores (1).

Cada configuración destaca diversas combinaciones de preparación interna y externa y cómo estas afectan los resultados de ciberseguridad.

Configuraciones de alto riesgo

Ciertas configuraciones, en particular aquellas que no presentan factores internos significativos, se catalogan como de alto riesgo (véase la figura 2). Estas incluyen configuraciones en las que las organizaciones dependen en gran medida de factores externos, pero carecen de una adecuada preparación interna. Particularmente en los ámbitos operativos y de ciberseguridad. La Figura 2 ilustra la presencia (1) o ausencia (0) de factores de riesgo en diversas configuraciones.

Comparación de configuraciones de alto riesgo.

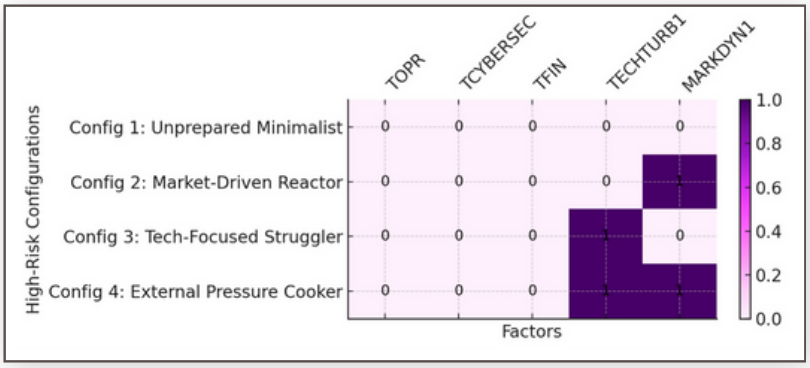


Fig. 2 Configuraciones de alto riesgo

El análisis identificó las siguientes configuraciones de alto riesgo:

Configuraciones de alto riesgo:

1.

"Minimalista desprevenido"

RIESGO: Esta configuración es la más vulnerable, careciendo de cualquier factor de protección. La organización no está preparada, ni a nivel interno ni externo, lo que implica un alto riesgo de brechas en la ciberseguridad.

MOTIVO: No existen vulnerabilidades internas (TOPR, TCYBERSEC, TFIN) ni externas (TECHTURB1, MARKDYN1) están presentes.

2.

"Reactor orientado al mercado"

RIESGO: Aunque la Dinámica del Mercado (MARKDYN1) está presente, no se cuentan con todos los factores de preparación internos. Esta organización depende en gran medida de las presiones externas del mercado, careciendo de las defensas internas necesarias.

RAZÓN: La falta de factores internos, como la capacitación en ciberseguridad y La preparación operativa incrementa el riesgo de una infracción, a pesar de la capacidad de respuesta ante las condiciones externas del mercado.

3.

"Luchador enfocado en la tecnología"

RIESGO: Existe una turbulencia tecnológica (TECHTURB1), lo que sugiere que la organización enfrenta una inestabilidad tecnológica externa; sin embargo, la falta de una sólida preparación interna coloca a la organización en una situación de alto riesgo.

MOTIVO: Insuficiente preparación interna en ciberseguridad y en sistemas operativos en una Un entorno tecnológico inestable incrementa el riesgo.

4.

"Olla a presión externa"

RIESGO: La presencia de ambos factores externos (tecnología y dinámica del mercado) sugiere una presión externa; sin embargo, la falta de preparación interna hace que esta organización sea susceptible a ataques.

RAZÓN: La falta de factores internos en un entorno externo inestable crea un entorno de alto riesgo.

Configuraciones de riesgo moderado:

5.

"Solidez financiera"

RIESGO: Existe una preparación financiera, lo cual ofrece una protección limitada, pero hay presiones externas derivadas de la tecnología y la dinámica del mercado, además de una insuficiente preparación interna en aspectos operativos o de ciberseguridad.

RAZÓN: Aunque la organización tiene estabilidad financiera; sin embargo, la falta de medidas operativas o de ciberseguridad incrementa el riesgo ante presiones externas.

Resumen de factores de alto riesgo:

DEBILIDADES INTERNAS:
Las configuraciones que carecen de factores internos sólidos (TOPR, TCYBERSEC) son las que enfrentan un mayor riesgo.

DEPENDENCIA DE FACTORES EXTERNOS:
Configuraciones como el Reactor impulsado por el mercado y el Luchador centrado en la tecnología destacan los riesgos de depender de factores externos sin controles internos apropiados.

Para mitigar estos riesgos, las organizaciones en estas configuraciones deben dar prioridad al fortalecimiento de su ciberseguridad interna y a su preparación operativa para resistir de manera más efectiva tanto las vulnerabilidades internas como las presiones externas.

Impacto de las barreras percibidas.

Se constató que la existencia de barreras percibidas —ya sean legales, organizativas o relacionadas con el conocimiento— se opone de manera más efectiva tanto a las vulnerabilidades internas como a las presiones externas (véase la figura 3). Las organizaciones que enfrentan estas barreras, especialmente en combinación con presiones externas, tienen una mayor probabilidad de experimentar brechas de seguridad si no disponen de sistemas internos robustos. La figura 3 ilustra la presencia (1) o ausencia (0) de barreras en diversas configuraciones.

El análisis reveló que las barreras relacionadas con el conocimiento y las organizacionales tuvieron el mayor impacto en la preparación para la ciberseguridad. Estas barreras representan desafíos para comprender las amenazas cibernéticas o para gestionar de manera eficaz las operaciones internas que protegen contra ellas. Las barreras legales, aunque siguen siendo relevantes, tuvieron un impacto menor en comparación con las barreras basadas en el conocimiento y las organizacionales.

El análisis indicó que las organizaciones que enfrentan significativas barreras relacionadas con el conocimiento a menudo no están adecuadamente preparadas para gestionar los riesgos de ciberseguridad. Las barreras organizativas, tales como la coordinación interna y la asignación de recursos, son igualmente fundamentales para evaluar la preparación. Estas barreras, junto con presiones externas como la dinámica del mercado, incrementan considerablemente la probabilidad de una vulneración.

Impacto de las barreras percibidas en las configuraciones

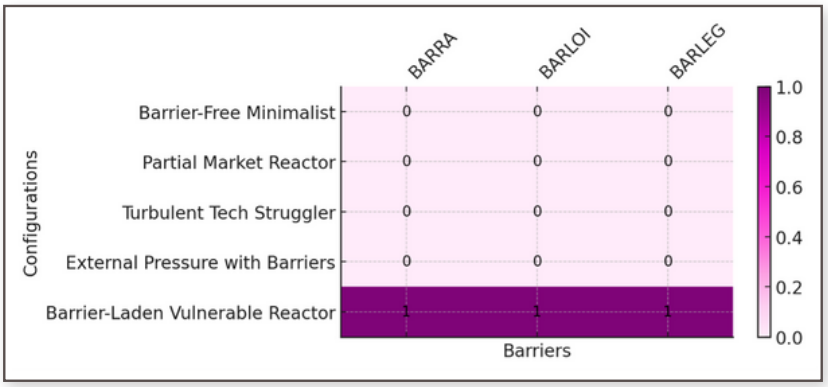


Figura 3 Efecto de las barreras percibidas

Se constató que la existencia de barreras percibidas (legales, organizativas o basadas en el conocimiento) ofrecía una mayor resistencia tanto a las vulnerabilidades internas como a la presión externa.

Las barreras organizativas, tales como la coordinación interna y la asignación de recursos, son igualmente fundamentales para evaluar la preparación.

Percepciones sobre la criticidad de los activos

Factores de criticidad evaluados:

CRTFINL
(Criticidad financiera)

CRTILOS
(Criticidad de la pérdida de información)

CRTBR
(Criticalidad de la reputación de la marca)

CRTLOP
(Criticidad operacional)

CRTIP
Criticidad de la infraestructura de tecnologías de la información.

CRTSUP
(Criticidad de la cadena de suministro)

CRTHL
(Criterio de salud y seguridad vital)

CRTCS
Criticidad del servicio al cliente

Observaciones sobre los resultados de fsQCA:

1. Criticidad financiera y operativa (CRTFINL, CRTLOP):

En la configuración en la que se encuentran presentes TOPR, TFIN y TCYBERSEC, la criticidad financiera (CRTFINL) y la criticidad operativa (CRTLOP) a menudo estaban ausentes, lo que sugiere que, incluso sin la consideración de estas como críticas, las organizaciones con una sólida preparación interna continuaban obteniendo resultados robustos.

2. Criticidad de la infraestructura tecnológica de la información (CRTIP):

CRTIP estuvo ausente en numerosas configuraciones, lo que sugiere que las organizaciones pueden no estar priorizando la infraestructura de TI con la seriedad que requieren, lo que podría exponerlas a vulnerabilidades.

3. Reputación de la marca y criticidad del servicio al cliente (CRTBR, CRTCS):

La CRTBR (reputación de marca) y la CRTCS (criticidad del servicio al cliente) no se presentaron con frecuencia en las configuraciones clave, lo que sugiere que estos factores reciben menos atención en la planificación de la ciberseguridad, aunque podrían volverse críticos si no se les protege adecuadamente.

4. Criticidad de la cadena de suministro y salud (CRTHL, CRTSUP):

Estos factores generalmente no se incorporaron en las configuraciones, lo que sugiere que las organizaciones podrían no considerarlos prioritarios. No obstante, representan áreas de riesgo potencial, especialmente para sectores vinculados a la infraestructura física o la atención médica.

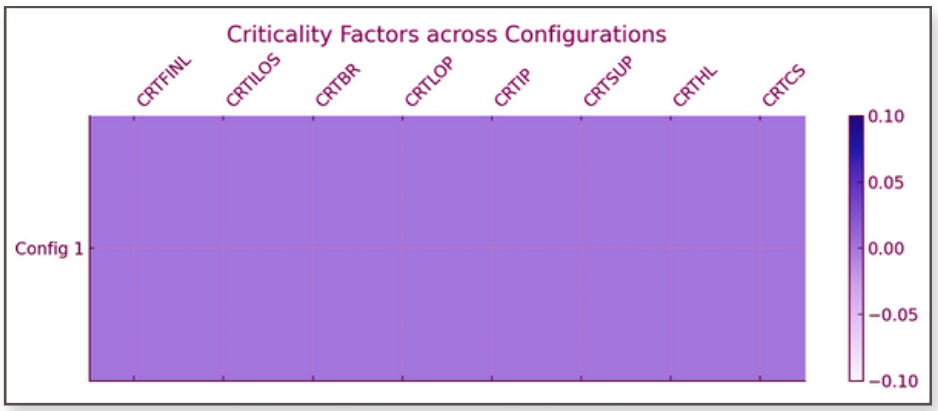
Según el análisis del mapa de calor y los hallazgos de fsQCA, la falta de percepciones sobre la criticidad de los activos (por ejemplo, CRTFINL, CRTLOP, CRTIP) generalmente se asocia con una mayor vulnerabilidad en diversas configuraciones. En aquellos casos en que los activos críticos, como la infraestructura de TI o los sistemas financieros, no son reconocidos como tales, las organizaciones pueden subestimar sus defensas de ciberseguridad, lo que las vuelve más propensas a sufrir brechas.

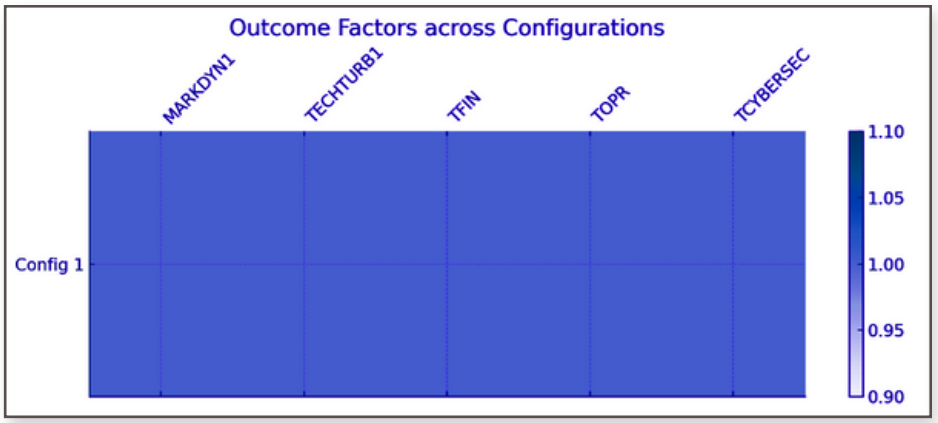
Por el contrario, la percepción de la criticidad de los activos puede conducir a una mayor priorización de las medidas de ciberseguridad, lo que disminuye la probabilidad de una brecha de seguridad. Cuando las organizaciones reconocen la relevancia de los activos críticos, es más probable que establezcan protecciones más robustas para ellos, mejorando así los resultados generales en materia de seguridad.

La configuración de **Comprehensive Defender** solo presentó un caso (n=1), que evidenció percepciones de criticidad de los activos. La visualización anterior ilustra los factores de criticidad y sus resultados asociados en diversas configuraciones:

• **Mapa de calor superior (púrpura):** indica la presencia (1) o ausencia (0) de factores críticos como financieros, operativos, infraestructura de TI, entre otros, en diversas configuraciones.

• **Mapa de calor inferior (azul):** representa los factores de resultado. (por ejemplo, preparación operativa, preparación en ciberseguridad, preparación financiera, etc.) en las mismas configuraciones.





HALLAZGOS PRINCIPALES Sobre la percepción de la criticidad:

La infraestructura de TI (CRTIP) y la criticidad operativa (CRTLOP) son elementos fundamentales que podrían ejercer una mayor influencia en los resultados de las infracciones si se les otorga la debida prioridad.

La criticidad financiera (CRTFINL) no siempre constituye un factor determinante para lograr resultados óptimos en el ámbito de la ciberseguridad, especialmente si se dispone de preparación interna (TOPR, TCYBERSEC).

Preparación financiera y operativa.

Las organizaciones que poseen una clara percepción de la criticidad de los activos y de los factores de preparación financiera y operativa (TFIN, TOPR) tienen una mayor probabilidad de destinar recursos adecuados a las medidas de ciberseguridad. En contextos donde la criticidad de los activos es manifiesta, también emergen otros factores como la preparación financiera (TFIN), lo que indica que las organizaciones están más dispuestas a invertir en las medidas de ciberseguridad necesarias cuando existe una percepción de criticidad de activos.

La criticidad de los activos, por sí sola, puede no ser suficiente para motivar la inversión en ciberseguridad, pero juega un papel crucial en el proceso de toma de decisiones. Al destinar recursos a medidas de ciberseguridad, las organizaciones tienden a considerar un contexto más amplio que abarca la preparación interna, las presiones externas y los riesgos percibidos. A continuación, se enumeran varios factores que influyen en la manera en que la criticidad de los activos afecta las decisiones de inversión:

1. Percepción del Riesgo:

• Si una organización recibe ciertos activos (p. ej., datos financieros, infraestructura de TI, sistemas de atención al cliente) como altamente críticos, es más probable que se invierta en la protección de estos activos. La percepción de criticidad genera una sensación de urgencia para asegurar la seguridad y disponibilidad de dichos activos.

• No obstante, frecuentemente se requiere más para activar el Inversión. Generalmente, debe integrarse con el entendimiento de las amenazas específicas de ciberseguridad para fomentar una asignación sustancial de recursos.

2. Preparación interna:

• Si una organización identifica sus activos críticos (por ejemplo, sistemas de TI) como muy importantes, pero también se siente preparado (con una sólida preparación operativa, marcos de ciberseguridad, etc.), es posible que no perciba la necesidad de una inversión adicional.

• Por otro lado, las organizaciones que cuentan con La escasa preparación interna, junto con la percepción de alta criticidad, podría dar lugar a una priorización más urgente de la inversión para abordar esas brechas.

3. Presiones externas:

• La dinámica del mercado y la turbulencia tecnológica pueden intensificar la influencia de la criticidad de los activos en las decisiones de inversión. Por ejemplo, si una organización opera en un entorno tecnológico en constante evolución, podría considerar la criticidad de los sistemas de TI como un motivo para incrementar su inversión en ciberseguridad.

• De manera similar, las industrias que se enfrentan a altos niveles de El escrutinio regulatorio (por ejemplo, en atención médica y finanzas) podría observar activos críticos que fomentan inversiones en ciberseguridad como parte de las medidas de cumplimiento.

4. Brechas en la ciberseguridad:

Los incidentes previos o casi accidentes pueden funcionar como Catalizadores. Si un activo crítico (como datos financieros sensibles o infraestructura de TI) se encuentra amenazado o comprometido, esta experiencia puede motivar una inversión considerable para prevenir incidentes futuros. La experiencia de una vulneración suele intensificar la percepción de la criticidad de ciertos activos y resalta la necesidad de inversión.

Si bien la percepción de la criticidad de los activos es un factor fundamental para determinar la asignación de recursos en las organizaciones, a menudo debe integrarse con otros factores contextuales, como la preparación interna, las presiones externas y las experiencias previas de infracciones, para fomentar una inversión significativa en ciberseguridad. Por sí sola, la percepción de criticidad puede generar conciencia, pero no necesariamente catalizar la inversión, a menos que la organización identifique riesgos directos para esos activos.

Conclusión

Este análisis de fsQCA subraya la relevancia de reforzar la preparación interna en ciberseguridad y la disponibilidad operativa. Aunque factores externos como la inestabilidad tecnológica y la dinámica del mercado impactan en los resultados de ciberseguridad, los factores internos continúan siendo los más determinantes para la protección contra las brechas de seguridad. Las organizaciones también deben enfrentar las barreras organizacionales y basadas en el conocimiento para asegurar una respuesta efectiva a las ciberamenazas.

- **La preparación interna es fundamental:** en todas las configuraciones, la existencia de preparación operativa (TOPR) y preparación para ciberseguridad (TCYBERSEC) ha contribuido de manera consistente a perfiles de riesgo más bajos. Estos son los dos factores más significativos para asegurar defensas robustas contra las ciberamenazas.
- **Las presiones externas afectan los resultados:** factores externos, como la turbulencia tecnológica (TECHTURB1) y la dinámica del mercado (MARKDYN1), añaden complejidad al panorama de seguridad. Las organizaciones que enfrentan estas presiones sin la preparación interna adecuada se encuentran en un mayor riesgo.
- **La criticidad de los activos guía el enfoque:** las percepciones sobre la criticidad de los activos, especialmente en relación con los sistemas financieros y la infraestructura de TI, juegan un papel crucial en la asignación de recursos por parte de las organizaciones. No obstante, la percepción de la criticidad por sí sola no es suficiente para garantizar la preparación; debe ir acompañada de sistemas internos y conciencia externa.
- **Un enfoque integral minimiza el riesgo:** configuraciones como Well-rounded Defender y Comprehensive Defender demuestran que un enfoque equilibrado, que incluye sistemas internos sólidos, conciencia externa y una comprensión de la criticidad de los activos, es más eficaz para mitigar los riesgos de ciberseguridad.

Recomendaciones finales

- **Invertir en sistemas internos:** Asegurar que tanto la preparación operativa como la seguridad operacional (B) sean las principales prioridades. Estas constituyen la base de una defensa robusta contra las ciberamenazas.
- **Comprender y actuar en consecuencia sobre la criticidad de los activos:** Fomentar que las organizaciones evalúen periódicamente la criticidad de sus activos, especialmente la infraestructura de TI y los sistemas financieros, y alineen las inversiones en ciberseguridad en consecuencia.
- **Responder a las presiones externas:** Monitorear factores externos como la dinámica del mercado y la turbulencia tecnológica, y ajustar las estrategias de ciberseguridad para abordar estos riesgos en constante evolución.
- **Apostar por una ciberseguridad integral:** Buscar un enfoque equilibrado y holístico que integre la preparación interna, la concienciación externa y la priorización de activos para establecer una defensa sólida contra las ciberamenazas.

El presente documento es una traducción al español realizada por el equipo de IFMA España del informe *Cybersecurity Breaches in Facility Management* elaborado por la Dra. Erika Pärn Jeffrey Saunders.

Visita la web **www.ifma-spain.org** para más información.


IFMA®