CIBERSEGURIDAD MODERNA: NUEVA ERA, NUEVAS ESTRATEGIAS

Noviembre 2024

isms forum

Ciberseguridad Moderna: Nueva Era, Nuevas Estrategias

Sergio Álvarez-Teleña [1 2] **Marta Díez-Fernández** [2] **ISMS Forum** [3]

Abstract

El presente artículo *(a)* ofrece una visión exhaustiva de la literatura existente en torno a la Algoritmización, con el propósito de establecer una base teórica robusta que permita al lector analizar y debatir de manera fundamentada los desafíos y oportunidades que presenta la Ciberseguridad Moderna; *(b)* se identifican nuevos riesgos de alta prioridad que deben ser abordados conjuntamente por los equipos de negocio y ciberseguridad; *(c)* fundamenta la asignación de recursos en ciberseguridad en la hibridación entre negocio, cumplimiento normativo y ciberseguridad; *(d)* identifica capacidades innovadoras facilitadas por una plataforma nativa algorítmica que permite la coordinación armónica entre las funciones de negocio y las estrategias de ciberseguridad; *(e)* propone la tecnología táctica como la base para garantizar la continuidad de negocios y su futuro; y *(f)* motiva una nueva corriente de investigación aplicada resultante de la colaboración entre empresas y centros de investigación, basada en plataformas que siguen el modelo de la Empresa en Tres Capas.

1. Introducción

Este documento examina cómo tomar decisiones fundamentadas en un entorno de ciberseguridad cada vez más desconocido y en constante evolución. La rápida transformación de las empresas en entidades *algorithmic-driven* actúa como detonante de este artículo sobre ciberseguridad[1]. Antes de profundizar en detalles específicos y casos de estudio en trabajos posteriores, este documento busca retroceder un paso para ofrecer una perspectiva más amplia sobre esta nueva era. Nuestro objetivo es ayudar al lector a comprender la situación actual, permitiéndole ver el bosque en lugar de perderse entre los árboles.

En el segundo capítulo, exploramos la literatura existente sobre la medición del impacto de la ciber inseguridad, un método tradicionalmente utilizado para asignar presupuestos de defensa. Comenzamos analizando datos de encuestas a nivel nacional y cuestionando su relevancia en el contexto actual. A partir de este punto, se adopta un enfoque que trasciende los datos históricos, orientándose hacia la literatura sobre transformación avanzada con el fin de priorizar dinámicas y escenarios plausibles, favoreciendo el uso de datos proyectivos en lugar de información retrospectiva. Los lectores que no estén interesados en las complejidades relacionadas con la medición del impacto de la ciberseguridad pueden dirigirse directamente al capítulo tres.

El capítulo tres presenta un primer *zoom-out* sobre transformación avanzada, cuestionando si la inteligencia artificial actúa como el elemento fundamental de las nuevas infraestructuras o si es simplemente *la guinda del pastel*. Para abordar esta cuestión, dividimos las empresas en dos tipos de factorías: la tradicional, compuesta por trabajadores *blue-collar* y una nueva, centrada en empleados *white-collar*.

El cuarto capítulo hace un nuevo *zoom-out*, abordando el hecho de que las factorías *white-collar* existirán en un equilibrio económico general debido a las necesidades de eficiencia y productividad en un entorno competitivo. Para ello, dividimos la naturaleza de la empresa en tres capas: Core I (infraestructura), Core II (todos los departamentos en una única plataforma) y Órbita (idiosincrasia que conduce a la diferenciación). Este enfoque permite a la alta dirección controlar de manera precisa los cambios en la curva de oferta de la empresa, orientando sus esfuerzos estratégicos para dominar y expandirse dentro de su mercado.

El capítulo cinco presenta el tercer y último *zoom-out* sobre transformación avanzada del documento. Aquí, centramos la atención en una condición necesaria para los dos capítulos

[1]Departmento de Computer Science, University College London, Inglaterra [2]SciTheWorld, España [3]ISMS Forum, España. Correspondence to: Sergio Álvarez-Teleña <sergio@scitheworld.com>, Marta Díez-Fernández <marta@scitheworld.com>, ISMS Forum <info@ismsforum.es>.

[1]Financiado por ISMS Forum (International Information Security Community).

anteriores: la continuidad de negocio. A medida que los atacantes se profesionalizan a través de la Algoritmización, la discontinuidad del negocio se convierte en un problema crítico para todos los departamentos de la empresa. Por ello, seremos testigos de una hibridación en el proceso de toma de decisiones entre negocio, ciberseguridad y cumplimiento normativo. Dado que los presupuestos tecnológicos en las empresas están limitados por la rentabilidad y los datos históricos no son suficientes para prever el impacto de los presupuestos de los CISOs, tal y como se explica en el capítulo 2, resulta crucial que las empresas aprovechen el potencial de la hibridación, particularmente en el reparto del presupuesto. Las organizaciones deben reevaluar la forma en que consideran sus *legacies* tecnológicos para que el presupuesto se acuerde entre las tres áreas y, por lo tanto, se optimice para esta nueva era. Más interesante aún, presentamos un conjunto de nuevos riesgos y nuevas mitigaciones en un mundo *algorithmic-driven* - Tecnología Táctica, Teoría de Juegos aplicada a CNE (explotación de redes de comunicación) y la manipulación de precios de mercado son ejemplos que se verán en detalle.

El capítulo final expone las conclusiones del estudio y propone direcciones para futuras investigaciones.

2. Antecedentes: Sólo la Acción Genera Tracción

Comenzamos este capítulo revisando la literatura existente sobre la medición del impacto de la ciberseguridad, con el objetivo de identificar los desafíos y limitaciones de su uso como indicador clave de desempeño (KPI) para orientar las decisiones presupuestarias corporativas en ciberseguridad. Este análisis sienta las bases para comprender las complejidades que implica alinear las inversiones en ciberseguridad con resultados medibles. Posteriormente, presentamos una revisión exhaustiva de las investigaciones recientes sobre la transformación digital avanzada, estableciendo el fundamento para una exploración más detallada de este tema en las siguientes secciones del documento.

2.1. No Todo se Puede Medir: los KPIs, una Carga en Transformación

Para ayudar a las organizaciones a determinar los niveles de inversión apropiados necesarios para abordar los riesgos crecientes asociados con la ciberseguridad, inicialmente consideramos llevar a cabo una encuesta a nivel nacional con el objetivo de estimar los costes potenciales a escala nacional. La principal razón detrás de este enfoque era cuantificar estos costes como un porcentaje del PIB, proporcionando así referencias estandarizadas que las empresas podrían utilizar para alinear su presupuesto de defensa con sus cuentas de resultados (P&L). Esta metodología estaba destinada a permitir una toma de decisiones informada en relación con las inversiones en ciberseguridad, asegurando que las empresas estén adecuadamente preparadas para mitigar las amenazas emergentes.

Tras una revisión exhaustiva de los documentos públicos existentes relacionados con esfuerzos previos en este ámbito, [1], [2], [3], [4]..., se hicieron evidentes varias limitaciones significativas:

1. **Insuficientes datos públicos sobre capacidades cibernéticas:** La disponibilidad de datos sobre capacidades cibernéticas, tanto clasificados como no clasificados, es significativamente limitada. Esta escasez de datos plantea desafíos significativos para llevar a cabo comparaciones precisas entre países, ya que la insuficiencia de información completa y consistente obstaculiza la evaluación y comparación de la fortaleza y preparación en ciberseguridad entre diferentes naciones.

2. **Disponibilidad limitada de información en inglés:** En algunos países, la información crucial no está fácilmente disponible en inglés, lo que complica aún más los esfuerzos por obtener datos fiables y comparables entre diferentes regiones.

3. **Falta de datos sobre proxies en el ciberespacio:** Existe una escasez significativa de datos sobre proxies en el ciberespacio - entidades o intermediarios que operan en nombre de otros actores, a menudo ocultando la verdadera fuente de las actividades cibernéticas. Esta falta de información plantea un desafío crítico, ya que limita severamente la capacidad de comprender plenamente el alcance, la escala y la complejidad de las operaciones cibernéticas. Sin datos detallados sobre estos proxies, se vuelve difícil atribuir con precisión los ciberataques, comprender las redes y estrategias empleadas por los ciberdelincuentes, y evaluar el impacto más amplio en la ciberseguridad global. Esta laguna en el conocimiento también complica los esfuerzos para desarrollar mecanismos de defensa efectivos y políticas internacionales, ya que la naturaleza oculta de las actividades de los proxies oscurece las verdaderas capacidades e intenciones tanto de actores estatales como no estatales en el ciberespacio.

4. **Falta de datos homogéneos:**

    - *Entre países:* La disponibilidad y calidad de los datos sobre ciberseguridad varían significativamente de un país a otro. Esta inconsistencia se debe a diferencias en los estándares de reporte, las

metodologías de recolección de datos y el nivel de transparencia respecto a las capacidades e incidentes cibernéticos. Como resultado, realizar comparaciones directas entre países es un desafío, ya que los datos pueden no ser directamente comparables debido a estas discrepancias. Esta variabilidad socava la capacidad de desarrollar una comprensión cohesiva de las tendencias globales en ciberseguridad y dificulta la cooperación internacional para abordar las amenazas cibernéticas.

- *Entre sectores:* La inconsistencia de datos también es prevalente en diferentes sectores económicos. Industrias como la financiera, la de salud y la energética pueden tener niveles variados de disponibilidad de datos y prácticas de reporte, influenciadas por factores como requisitos regulatorios, riesgos específicos del sector y la adopción de medidas de ciberseguridad. Esta falta de uniformidad dificulta la realización de análisis confiables específicos por sector, ya que los datos pueden no reflejar con precisión la verdadera postura de ciberseguridad o los riesgos dentro de cada sector. En consecuencia, esta variabilidad complica los esfuerzos para evaluar el rendimiento, identificar vulnerabilidades y asignar recursos de manera efectiva entre diferentes industrias.
- *A lo largo del tiempo:* La uniformidad de los datos recolectados en diferentes años a menudo es deficiente, lo que dificulta la realización de estudios longitudinales o la identificación de tendencias a lo largo del tiempo. Los cambios en los métodos de recolección de datos, las amenazas cibernéticas en evolución y los cambios en las prácticas de reporte contribuyen a esta inconsistencia. Como resultado, los esfuerzos para rastrear el progreso de las medidas de ciberseguridad, evaluar la efectividad de las políticas o prever tendencias futuras se ven obstaculizados por la falta de un conjunto de datos estable y comparable. Esta variabilidad temporal representa un desafío significativo para los investigadores y responsables de políticas que intentan evaluar los desarrollos a largo plazo en el campo de la ciberseguridad.

5. **Datos de encuestas poco confiables:** Las encuestas son una herramienta común para recopilar datos sobre las capacidades y actividades de ciberseguridad; sin embargo, la fiabilidad de estos datos a menudo se ve comprometida por factores estratégicos. Los países pueden ocultar intencionalmente o tergiversar sus verdaderas capacidades e intenciones cibernéticas para proteger intereses de seguridad nacional. Este ocultamiento deliberado suele estar motivado por el deseo de mantener una ventaja estratégica, evitar revelar vulnerabilidades o engañar a posibles adversarios. Como resultado, los datos recopilados a través de encuestas pueden no reflejar con precisión el estado real de la infraestructura de ciberseguridad de un país, lo que lleva a una subrepresentación o tergiversación significativa en índices y estudios globales.Por ejemplo, en [4], se ha sospechado que Israel podría estar significativamente subclasificado debido a su elección estratégica de ocultar sus capacidades cibernéticas. Esta subdeclaración puede distorsionar los rankings y análisis globales, conduciendo a una representación inexacta del poder cibernético de un país en relación con otros. Tal comportamiento estratégico complica los esfuerzos para crear evaluaciones precisas y completas de la ciberseguridad global, ya que los datos a menudo son incompletos o engañosos debido a estas omisiones intencionadas. Este problema resalta el desafío más amplio de depender de datos autoinformados en un ámbito donde el secreto y el engaño estratégico son comunes.
6. **Metodología:** La mayoría de los artículos sostienen haber seguido una metodología rigurosa y, posteriormente, enfatiza que la verificación de su análisis se ha llevado a cabo utilizando Procesamiento de Lenguaje Natural (NLP), el cual, como se ha visto en [5], no constituye una práctica óptima. El proceso de validación debe guiarse por una combinación de experiencia en el dominio, métodos estadísticos robustos y una cuidadosa consideración de factores contextuales específicos. Por lo tanto, las mejores prácticas en la investigación de ciberseguridad deberían adoptar un enfoque más integral para la verificación, asegurando que las metodologías empleadas sean adecuadas y efectivas para abordar los desafíos particulares del ámbito.
7. **Inconsistencia entre estudios:** A pesar de la variedad de estudios existentes, la mayoría se basa en diferentes medidas y herramientas, como costes anuales, costes específicos por sector o costes por ataque. Esta diversidad en los enfoques de medición conduce a una variabilidad significativa en los resultados, lo que a menudo resulta en estimaciones y pronósticos inconsistentes que complican los esfuerzos para realizar comparaciones o conclusiones fiables en diferentes contextos. Por ejemplo, un estudio podría centrarse en el impacto financiero anual de los ciberataques en grandes corporaciones, mientras que otro podría medir el coste promedio por incidente en varios sectores. La falta de métricas estandarizadas significa que estos estudios a menudo no son directamente comparables, lo que dificulta la agregación de datos o la identificación de tendencias más amplias.

Esta inconsistencia se ve agravada por las diferencias

de recopilación, reporte y análisis de datos entre los estudios. Algunas investigaciones pueden depender de datos autoinformados de las empresas, que pueden estar sujetos a sesgo o subdeclaración, mientras que otras pueden utilizar bases de datos propietarias o informes de terceros que no son universalmente accesibles o verificados. Además, las metodologías empleadas para calcular costes - ya sea a través de encuestas, modelos econométricos o simulaciones - pueden variar ampliamente, lo que conduce a discrepancias en el impacto estimado de eventos cibernéticos similares.

La naturaleza fragmentada de estos estudios también plantea desafíos para los responsables de políticas, líderes de la industria e investigadores que buscan comprender el alcance completo del riesgo cibernético global. Sin un enfoque unificado de medición, se vuelve difícil desarrollar estrategias efectivas para mitigar estos riesgos o asignar recursos de manera apropiada. La falta de consistencia también puede obstaculizar la colaboración internacional, ya que los países y organizaciones pueden basar sus políticas de ciberseguridad en diferentes conjuntos de datos, lo que lleva a una respuesta global desarticulada ante las amenazas cibernéticas.

Además, el enfoque en costes específicos - como los asociados con ataques individuales o impactos sectoriales - frecuentemente pasa por alto los riesgos más amplios y sistémicos que plantean las amenazas cibernéticas. Estos riesgos más amplios, que pueden incluir interrupciones en infraestructuras críticas, pérdida de propiedad intelectual y daños económicos a largo plazo, son más difíciles de cuantificar pero no menos importantes. Los enfoques actuales pueden no capturar estas dimensiones, lo que lleva a una comprensión incompleta del verdadero costo del riesgo cibernético.

En resumen, la diversidad en los enfoques de medición dentro de los estudios existentes resalta los desafíos significativos para producir cifras comparables y consistentes en el contexto de la evaluación del riesgo cibernético global. Esta falta de estandarización no solo complica la comparación de resultados entre diferentes estudios, sino que también limita la capacidad de formar una imagen integral del paisaje de riesgo cibernético global, dificultando así los esfuerzos para desarrollar respuestas coordinadas y efectivas ante estas amenazas cada vez más complejas.

8. **Dinámicas emergentes de nuevos riesgos:** Además, las nuevas dinámicas asociadas con los riesgos emergentes no fueron identificadas adecuadamente en la investigación existente, lo que destaca una brecha significativa en la comprensión y abordaje de la naturaleza evolutiva de las amenazas cibernéticas. A medida que las empresas adoptan tecnologías avanzadas, se exponen a un espectro más amplio de riesgos. La integración de tecnologías digitales en todos los aspectos de las operaciones comerciales ha creado nuevas vulnerabilidades, particularmente a medida que las organizaciones realizan la transición hacia la computación en la nube, el Internet de las Cosas (IoT) y la inteligencia artificial (IA). Estas tecnologías, si bien ofrecen beneficios enormes, también amplían la superficie de ataque, brindando a los ciberdelincuentes más oportunidades para explotar debilidades.

Además, la sofisticación de los atacantes ha crecido en paralelo con los avances tecnológicos. Los adversarios cibernéticos ahora son capaces de aprovechar innovaciones algorítmicas de última generación. Las defensas tradicionales en las que las empresas han confiado pueden ya no ser suficientes para contrarrestar estas amenazas avanzadas, lo que genera una necesidad urgente para que las organizaciones reevalúen y fortalezcan sus estrategias de ciberseguridad. Consideramos que este problema es particularmente preocupante, ya que indica que las evaluaciones de riesgo actuales pueden estar subestimando significativamente el impacto potencial de estas nuevas amenazas. La incapacidad para tener en cuenta completamente la naturaleza dinámica de los riesgos cibernéticos significa que las empresas pueden estar inadecuadamente preparadas para los desafíos que se avecinan. Esta insuficiencia podría resultar en pérdidas financieras severas, daños a la reputación e interrupciones en la continuidad del negocio.

Reconociendo estas limitaciones, decidimos pasar de un enfoque predominantemente estadístico a uno más microeconómico, centrándonos en desarrollar un razonamiento bien fundamentado dentro del campo. Al adoptar este enfoque, buscamos justificar mejor los cambios clave que pueden ser necesarios para que las empresas se adapten al entorno evolutivo de amenazas cibernéticas. Esto implica no solo reevaluar las medidas de seguridad actuales, sino también considerar cambios organizativos más amplios, como reestructurar la gobernanza de la ciberseguridad, invertir en capacidades avanzadas de detección y respuesta ante amenazas, y fomentar una cultura de aprendizaje continuo y adaptación dentro de la fuerza laboral. En última in-

stancia, esta comprensión más matizada ayudará a las empresas a tomar decisiones informadas sobre dónde asignar recursos, cómo priorizar diferentes riesgos y qué estrategias implementar para salvaguardar sus operaciones en un paisaje digital cada vez más complejo.

Después de todas estas complejidades, la pregunta es: cuando los datos no pueden ser aprovechados para tomar decisiones informadas, ¿qué se puede hacer?.

2.2. Literatura sobre la Transformación Avanzada: una Disciplina Profunda y Novel

Los economistas han estado trabajando con modelos impulsados por datos o por teoría durante varios años. El primero dio origen a la Econometría, que es la raíz de la Ciencia de Datos actual, mientras que el segundo, más complejo y relevante para este documento, se relaciona con la modelización en términos de Microeconomía y Macroeconomía.

No crearemos un modelo que establezca con precisión cuánto debe gastar cada empresa en ciberseguridad. Las dinámicas dentro del mundo corporativo y las de los atacantes están cambiando de manera tan drástica debido a su avanzada digitalización que resulta prematuro elaborar dicho modelo. En su lugar, en esta etapa, identificaremos los *inputs* que serían más significativos para el modelo - sin dar forma adicional al mismo - para que el CISO pueda decidir si permanecer anclado a los datos del pasado o adoptar otras estrategias de comunicación con la alta dirección para abordar las necesidades emergentes de ciberseguridad.

Primero, es esencial comprender a fondo el papel de la inteligencia artificial (IA) y los riesgos asociados. La implicación de la IA en los procesos transformativos a menudo conduce a la difusión de medias verdades, frecuentemente propagadas por individuos con credenciales académicas limitadas y motivados por tácticas de marketing viral. Para abordar esta confusión generalizada, hemos sido pioneros en una nueva disciplina en la última década: la Algoritmización. Esta disciplina redefine la Transformación Digital al enfatizar el núcleo como eficiencia y la productividad, marcando una evolución más allá de la mera digitalización. La Algoritmización representa un cambio de empresas impulsadas por datos a convertirse en empresas impulsadas por modelos, operando de acuerdo con protocolos avanzados y sistematizados por diseño. Estos modelos pueden definirse matemáticamente (como en estadísticas), desarrollarse a través de enfoques de prueba y error (como en estadísticas computacionales o IA), o basarse en reglas heurísticas propuestas por expertos. A medida que esta transformación se extiende a todos los departamentos, la empresa en sí se convierte esencialmente en un algoritmo. Este cambio no solo introduce nuevas vulnerabilidades, sino que también presenta oportunidades novedosas para desarrollar estrategias de defensa.

La tecnología fundamental que sustenta este cambio fue desarrollada y articulada meticulosamente en [6]. El rol de la alta dirección en la gestión de esta transición fue examinado a fondo en [7] y [8], mientras que la sutil distinción entre la *ciencia aplicada* y la mala aplicación de principios científicos, o *aplicar ciencia*, fue analizada críticamente en [9]. Además, el enfoque innovador de ejercer influencia sobre las naciones comprometiendo no sólo sus empresas, sino también sus juntas corporativas, fue un concepto innovador introducido para la OTAN en [10]. Ejemplos adicionales de vanguardia en sectores como finanzas y construcción se proporcionaron en [11], [12], y [13],[14],[15]. Por último, la integración exhaustiva de la Algoritmización con la Súper Inteligencia Artificial (ASI) fue explorada en profundidad en [5]. Este análisis destacó la relación simbiótica entre estos conceptos, ilustrando que la ASI se desbloquea a través de la Algoritmización de los departamentos—lograda mediante la agregación de Inteligencias Artificiales Estrechas (ANI) -cuando la eficiencia y la productividad son los principales motores del cambio. Esta intersección representa un nuevo equilibrio económico y realista que moldeará cada vez más el - comportamiento corporativo y, más significativamente, los riesgos asociados con él en el futuro.

2.3. Conclusión

Si bien es posible invertir tiempo y recursos en analizar los impactos pasados de la ciberseguridad, la realidad es que, incluso si tal análisis fuera sencillo - lo cual no es - tendría una relevancia limitada desde una perspectiva dinámica. Esto se debe a que casi todos los sectores están experimentando transformaciones fundamentales hacia la digitalización, lo que hace que los datos históricos sean menos relevantes en un contexto de constante evolución.

El resto del documento profundiza en conceptos clave sobre la Algoritmización de atacantes y defensores, que podrían ser fundamentales para definir nuevas dimensiones de riesgos, así como para identificar mitigaciones efectivas y evaluar sus impactos potenciales.

3. La IA es un Aspecto Menor: Las Factorías White Collar es lo Relevante

La IA es una palanca para desbloquear la transformación en una empresa, pero debe estar lejos de ser el objetivo en sí mismo, un error común que hemos presenciado en diversas industrias en los últimos años. De hecho, confundir la IA con la Algoritmización, siendo sólamente la última milla de ésta, genera no solo confusión, sino también legados no deseados.

La Algoritmización de las empresas se refiere a la transformación de sus departamentos en unidades operativas que aprovechan métodos científicos, manteniendo una clara énfasis en la experiencia profesional sobre supuestos puramente teóricos o científicos. Un error común, como se ilustra en [9], es la mala interpretación de *Ciencia Aplicada* como *Aplicar Ciencia*, lo que a menudo resulta en soluciones parciales que no logran generar un impacto significativo dentro de la organización. Para lograr resultados significativos, el papel de la ciencia debe ser adecuadamente minimizado, y esto requiere juicio en los tres ámbitos: ciencia, tecnología y negocios; algo muy escaso en esta época, ya que los tres deben superponerse en el conocimiento de una sola persona, el líder natural, y no simplemente combinarse en un equipo con especialistas en cada ámbito - debido a que la clave en el diseño de la transformación pivota sobre el desbloqueo de las interrelaciones de esos campos.

En este capítulo, esbozamos las razones detrás del *hype* que se ha creado en torno a la IA. Entender la complejidad de la transformación avanzada, que cambiará significativamente las prioridades en ciberseguridad, requiere no sólo una perspectiva amplia, sino una serie de tres *zoom-outs* que nos ayuden a poner orden. Este capítulo sirve como el primero en esa serie, ofreciendo una base esencial para comprender las implicaciones más amplias de estas complejas transformaciones.

3.1. Factorías Blue-Collar: la Producción ya es un Algoritmo

Desde la introducción del Modelo T en las fábricas de Henry Ford, las empresas han ganado progresivamente control sobre el tiempo, los costes y la calidad a través del empleo de trabajadores de cuello azul. El enfoque tradicional de la artesanía fue reemplazado por un sistema meticulosamente organizado en el que trabajadores - ahora menos cualificados y más fácilmente reemplazables - se situaban alrededor de las máquinas para gestionar todo el proceso de producción. Estos trabajadores adaptaron sus roles de manera sistemática a la secuencia de máquinas, así como a los legados operativos de las máquinas a lo largo de la fábrica. En este sentido, la fábrica misma opera como un algoritmo, donde convergen humanos y máquinas - esto es, en general, se podría decir que son las máquinas las que están *aumentadas* por el trabajo humano y no al revés.

Es importante señalar que el algoritmo que rige las operaciones de la fábrica no proviene de un modelo de autoaprendizaje, sino que está diseñado heurísticamente por ingenieros en colaboración con expertos en negocios, adaptado específicamente a las necesidades de la empresa y a su idiosincrasia física (tamaño de sus naves, orientación, distribución…). Como resultado, este algoritmo es poco probable que sea matemáticamente óptimo, pero es *suficientemente bueno* en términos de eficiencia y productividad para permitir que la empresa se mantenga competitiva en el mercado.

3.2. Factorías White-Collar: las Oficinas son la Algoritmización Pendiente

A medida que las empresas adoptan cada vez más tipos similares de maquinaria, sus procesos de producción se han vuelto más estandarizados y menos una ventaja competitiva. En consecuencia, el enfoque de la innovación ha cambiado de la fábrica (blue-collar) a negocio (white-collar), impulsado por el movimiento de transformación digital.

En este contexto, la inteligencia artificial (IA) ha tomado protagonismo, dominando la narrativa en torno a la digitalización y absorbiendo una porción sustancial de los presupuestos de innovación corporativa. Sin embargo, es esencial reconocer que la IA es solo un componente dentro de una transformación más amplia y fundamental, que no siempre requiere de la IA en cada etapa. Las empresas están evolucionando hacia entidades completamente algorítmicas, convirtiéndose esencialmente en factorías white-collar, donde los procesos estratégicos, operativos y de toma de decisiones se traducen prácticamente en fórmulas tal y como se rigen las factorías blue-collar. Esta transformación señala un cambio profundo en la manera en que funcionan los negocios, ya que estos marcos algorítmicos encapsulan las operaciones centrales de la empresa. Como tal, estas fórmulas representan la nueva propiedad intelectual del mundo corporativo y deben ser protegidas con un nivel de diligencia sin precedentes, marcando un cambio significativo en las exigencias de la gobernanza corporativa.

3.3. Estandarización de Negocios: Acorrallados hasta ser NPCs (Figurantes en el Juego)

La forma en que las empresas han construido su infraestructura tecnológica ha estado lejos de ser óptima. Los proveedores de tecnología a menudo obligan a sus clientes a adaptarse a sus propias necesidades de escalar entre múltiples clientes vía servicios estandarizados. Estos proveedores suelen operar como parte de un oligopolio, lo que significa que el stack tecnológico de la mayoría de las empresas tiene sólo ligeras variaciones entre sí. Además, los consultores que conectan estas plataformas también pertenecen a un oligopolio y, para escalar sus servicios, fomentan una mayor estandarización entre los clientes. Esto crea un riesgo empresarial considerable, derivado de la priorización de decisiones fragmentadas en lugar de poder establecer estrategias holísticas y orquestadas que alinean la tecnología con los objetivos comerciales tanto a corto como a largo plazo.

Como resultado, las empresas dentro de un sector se ven empujadas a un estado de competencia perfecta, careciendo de cualquier ventaja competitiva significativa sobre sus pares en la dimensión tecnológica. Además, esta estandarización aumenta la vulnerabilidad a los ciberataques. Cuanto más similares son las plataformas, más atractivo y rentable se vuelve para los hackers atacarlas.

Por lo tanto, evolucionar la tecnología de una manera más propietaria y diferenciada se ha convertido en una necesidad urgente; el *riesgo de estandarización* de negocios es uno que debe explorarse adecuadamente en el futuro, ya que trae consigo riesgos no sólo cibernéticos sino también de una nueva generación de competidores, desde proveedores hasta empresas de otros sectores.

3.4. Conclusión

A medida que las empresas avanzan en su transformación digital, evolucionan naturalmente hacia algoritmos end-to-end, abarcando tanto entornos de producción como de oficina. Este cambio fundamental en su estructura operativa ejerce una presión creciente sobre el papel de la ciberseguridad, elevando su importancia tanto a nivel de la Junta Directiva como del CISO. La naturaleza algorítmica de estas organizaciones intensifica las vulnerabilidades, haciendo que la protección de los datos, los procesos y la propiedad intelectual sea más crítica que nunca. La ciberseguridad debe adaptarse ahora para salvaguardar no solo los activos tradicionales, sino también los marcos algorítmicos que sustentan todo el negocio, lo que requiere una supervisión estratégica y una gobernanza más robusta a los niveles más altos.

En última instancia, las empresas deben ahora no sólo defenderse de ciberataques, sino también enfrentar riesgos más sutiles y orientados al negocio. Por ejemplo, el riesgo de estandarización, ya que deben protegerse de los proveedores de tecnología que, intencionadamente o no, actúan como *hackers* de la eficiencia y la diferenciación de la empresa al imponer diseños arquitectónicos ineficientes. Tales diseños pueden encerrar a las empresas en sistemas desfavorables, reduciendo su agilidad y competitividad. Además, las empresas deben abordar el riesgo de que competidores importantes aprovechen estas ineficiencias para dominar el mercado. Este panorama de amenazas en expansión requiere que la ciberseguridad evolucione más allá de los mecanismos de defensa tradicionales, incorporando un enfoque más estratégico para proteger las dimensiones empresariales más amplias de la compañía.

4. Desplazando la Curva de la Oferta: Eficiencia y Productividad, el Dúo Ganador

Si se da un paso atrás para hacer zoom-out una vez más, se puede reconocer que, a pesar de su relevancia, la Algoritmización no es un objetivo final, sino una herramienta estratégica destinada a un objetivo superior: llevar la eficiencia y la productividad a un nuevo nivel.

Este capítulo arroja luz sobre el estado actual de la tecnología de vanguardia disponible para lograr dicho enfoque. Por lo tanto, tiene como objetivo proporcionar al lector una base sólida antes de adentrarse en sus implicaciones en ciberseguridad.

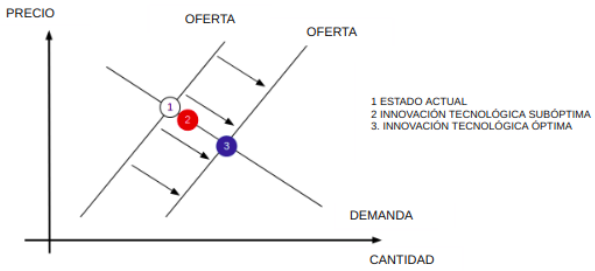


Figure 1. Desplazamiento de la curva de la oferta gracias a la innovación tecnológica: no es suficiente con moverla, sino que hay que moverla de manera máxima e, idealmente, de forma continua a lo largo del tiempo. Fuente: [6]

4.1. Eficiencia Extrema: la Empresa en Tres Capas

Aquellas empresas que están completamente algoritmizadas - las que cuentan tanto con las factorías blue-collar como con las white-collar - son las que pueden desbloquear los niveles más altos de eficiencia en sus industrias[2].

Nos referimos a estas empresas como *organizaciones sobre plataforma*, y están estructuradas en tres capas distintas:

1. **Core I:** la arquitectura del software, federada como en Data MAPs (ver [6]).
2. **Core II:** las aplicaciones de software para los diferentes departamentos, nativo algorítmicas.
3. **Órbita:** el ajuste idiosincrático del Core II que busca la diferenciación, avances propietarios.

Todos ellos están descritos en detalle en [8], pero a continuación destacaremos sus principales características para que el lector construya una base sólida hacia la discusión final sobre la ciberseguridad moderna.

4.2. Core I: Federación

Esta capa de tecnología profunda representa el núcleo de la disrupción; es el catalizador que permite todo lo algorítmico dentro de una empresa. Después de publicar su teoría en [6], SciTheWorld desarrolló la primera instancia de este enfoque apalancándose en su tecnología de trading algorítmico. La lógica es sencilla: si esta tecnología puede gestionar con éxito algunas de las estrategias más complejas en diversos sectores, entonces, cuando se diseña de una forma más generalista, debería ser igualmente capaz de gestionar de manera universal las necesidades estratégicas de otros departamentos dentro de una misma empresa. En relación con el enfoque de este documento, esta innovación permite:

- **Negocios algorítmicos:** De tal manera que los departamentos comparten tecnología de backend, lo que permite que su mantenimiento y mejoras sean gestionados sinérgicamente.
- **Ciberseguridad algorítmica:** Dado que la tecnología se distribuye a través de nodos sin importar los servidores en los que se encuentre, puede aprovechar su nueva naturaleza para desbloquear nuevas estrategias para la gestión y protección del hardware y software, entre otros.
- **Cumplimiento algorítmico:** Descomponer algoritmos complejos en nodos facilita la aplicación y el seguimiento del cumplimiento por defecto, lo que lleva a una nueva capacidad para descontar, en tiempo real, las consecuencias de la regulación global.

Es importante señalar que los tres aspectos pueden fusionarse de manera nativa. Cuanto más esfuerzo dedique la empresa a estos elementos, más ventajas competitivas podrá desbloquear. Existen una multitud de ejemplos, tales como:

- **Resiliencia ante la rotación:** En una era caracterizada por el movimiento frecuente de talento experto en tecnología entre empresas, mantener un sistema federado es esencial para salvaguardar la propiedad intelectual y facilitar la sustitución rápida en roles clave. Este enfoque asegura la continuidad y mitiga los riesgos asociados con la rotación de empleados.
- **Cumplimiento cutting-edge:** Las empresas que garantizan rápidamente el cumplimiento mientras innovan superarán a sus competidores. Cuanto más integre una empresa la innovación algorítmica a través de la federación, más podrá capitalizar esta ventaja. **Continuidad del negocio:** Establecer la resiliencia como un diferenciador clave permite a una empresa destacarse entre sus pares, como se explora más a fondo en el capítulo 5.

4.3. Core II: E2E Sobre Plataforma

Con la tecnología base establecida en la capa anterior, una empresa puede comenzar a construir sus propios sistemas de extremo a extremo (E2E) para diversos departamentos. Sería como una versión más ambiciosa de las plataformas ERP actuales: más amplia en alcance, con más alcance en términos de características y lo suficientemente flexible como para ser adaptada en la siguiente capa.

Ésta es la capa que da forma a la *factoría white-collar* dentro de una empresa. Su flexibilidad a menudo conduce a la creación de nuevos protocolos más precisos y eficientes, elaborados por expertos en negocios. Éstas no son innovaciones aisladas; son la evolución natural en la que los profesionales del sector convergerán - esto es, pueden ser ventaja competitiva durante algún tiempo pero no en el largo plazo. Tomamos como ejemplo, [13],[14],[15] en la gestión de activos, un poderoso caso de transformación a nivel de industria financiera.

[2]Es importante señalar que no todas las industrias ponen el mismo énfasis en ambas factorías. Algunas industrias están equilibradas hacia la parte blue-collar (como la industria automotriz), otras hacia la white-collar (banca y seguros) y otras evitan una de ellas (la moda de alta gama evita la blue-collar en favor de los artesanos como parte de la firma de su marca). Todo depende de la naturaleza de la empresa y de su capacidad para buscar una ventaja competitiva en uno u otro.

Como exploraremos en la sección 4.5, esta capa forma la columna vertebral del cerebro digital: el centro neurálgico de la transformación avanzada de una empresa. Esta transformación puede avanzar en dos direcciones:

- **Top-down:** La alta dirección orquesta la adopción de esta capa, designando ciertos departamentos o filiales como buques insignia. Estos grupos son los pioneros de los cambios, heredando tecnología, abordando la resistencia cultural y estableciendo mejores prácticas que el resto de la organización puede seguir. A partir de ahí, hay una herencia entre departamentos priorizada por el impacto en la transformación de la empresa, hasta que todos los departamentos que deben estar interconectados lo estén.

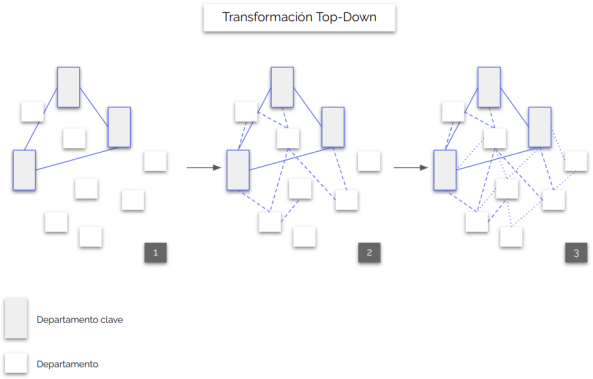


Figure 2. Transformación Top-Down en tres departamentos clave (o empresas dentro de un grupo) que primero se interconectan y luego se utilizan gradualmente para impulsar la interconexión y transformación del resto de los departamentos.

- **Bottom-up:** Es crucial que, incluso sin un proyecto de transformación formal, los departamentos que adopten el modelo de Empresa en Tres Capas de manera descentralizada, de forma independiente en cada departamento, aún pueden provocar el mismo cambio a nivel organizacional que el Top-Down por vía de contagio. Aunque este método es menos eficiente a lo largo del tiempo ya que los buques insignia no se eligen de manera estratégica.

Para que una empresa pueda adoptar la transformación de una forma realista, necesita hacerla compatible con sus sistemas actuales aunque estén obsoletos (*legacy*). Como se detalla en [6], la arquitectura de producción existente de la empresa debe estar rodeada por una versión extendida y avanzada (*Extended Production Architecture - EPA*). Solo así podrá mantener el ritmo de forma continua en un entorno competitivo y en rápida evolución.

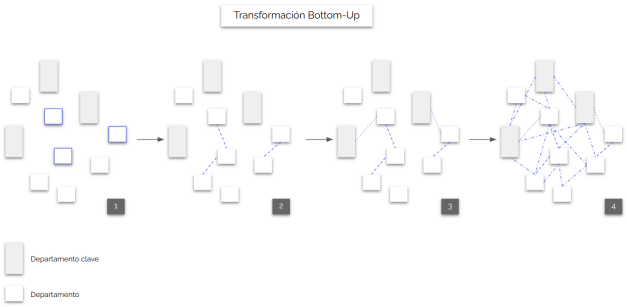


Figure 3. La transformación Bottom-Up sobre el modelo de la Empresa en Tres Capas conduce al mismo punto (organización sobre plataforma), pero de una manera menos eficiente, ya que el contagio ocurre de manera aleatoria en lugar de estar estructuralmente orquestado.

4.4. Órbita: Ventaja Competitiva Idiosincrática

Una vez que los equipos tengan tecnología nativa algorítmica - que sirve como base para crear versiones *suficientemente buenas* de una amplia gama de aplicaciones existentes - podrán iniciar el proceso de transformación a través de:

- **Personalización:** Pueden adaptar estas tecnologías de maneras que los proveedores tradicionales, limitados por sistemas heredados y la necesidad de escalar entre casuísticas de clientes, no podrían ofrecer. Esto permite a los equipos liberarse de las limitaciones tecnológicas actuales y ampliar los límites de lo que es posible.
- **Innovación:** Los equipos también pueden crear herramientas completamente nuevas que nunca estuvieron disponibles pero que son esenciales para aumentar la eficiencia y la productividad, avanzando mucho más allá de su modelo de negocio actual - lo veremos en el capítulo 5.

Adicionalmente, cada departamento puede operar como si fuera una entidad independiente impulsada por tecnología, aprovechando una tecnología de extremo a extremo que está completamente interconectada a lo largo de la empresa. Esto permite a cada equipo personalizar sus herramientas mientras sigue beneficiándose de las sinergias compartidas dentro de la organización - la parte clave de la federación, equilibrando la libertad de Negocio con las necesidades de IT.

Este proceso, donde la diferenciación y la ventaja competitiva surgen en el mundo corporativo actual, también abre la puerta a nuevas vulnerabilidades, que exploraremos en el capítulo 5.

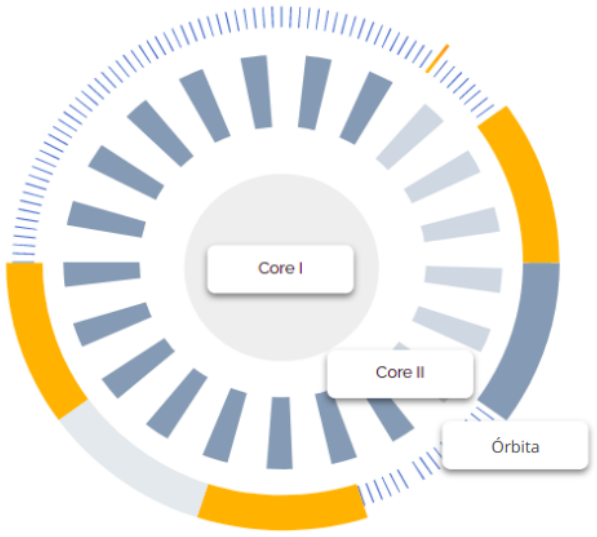


Figure 4. Representación gráfica de la Empresa en Tres Capas [8].

4.5. El Camino hacia la ASI

El lector habrá notado que consideramos que a la IA se le ha otorgado un rol para el cual las empresas aún no están preparadas. Carecen de la estructura algorítmica necesaria antes de dar el paso adicional con IA. Sin embargo, esto no significa que la IA deba ser eliminada de las conversaciones corporativas - al contrario: orienta el rumbo.

Para que una empresa destine cantidades significativas de su presupuesto a tecnología, debe estar segura de que no necesitará cambiar su infraestructura durante muchos años. El abuso de *low-hanging-fruits* en la creación de una plataforma holística ha generado ineficiencias que, con el tiempo, deben ser revisadas. El uso de parches es una práctica frecuente que conduce a callejones sin salida, donde, en momentos imprevistos, la empresa se ve obligada a reservar grandes presupuestos no para consolidar ventajas competitivas importantes, sino simplemente para desbloquear su evolución o asegurar la continuidad del negocio - para el *right-to-play* en lugar de para el *right-to-win*.

En [5] se propone el estado ideal de la tecnología corporativa, desde un año de plazo hasta décadas en el futuro, y analiza el continuum tecnológico capaz de alinear objetivos a largo y corto plazo. Este enfoque se basa en la implementación de factorías white-collar como un equilibrio común entre las empresas que buscan el éxito a través de la eficiencia y la productividad. Al mapear esos algoritmos - que, nuevamente, superan las visiones parciales y, a menudo, desactualizadas basadas únicamente en datos - con áreas del córtex cerebral y éstas, a su vez, con Inteligencias Artificiales Estrechas (ANIs), el artículo define de manera elocuente el objetivo último de la empresa: la creación de un cerebro digital que integre todo el conocimiento de la organización (*know-how*) en primera instancia - Inteligencias Artificiales Generales (AGIs) -, y posteriormente, combinando las ANIs de los mejores entornos posibles, la construcción de sus propias Inteligencias Artificiales Corporativas Superiores (CASIs) - no en vano se trata de combinaciones Pareto-superiores a las AGIs corporativas.

Curiosamente, contrariamente a como se espera del futuro de la aplicación de la IA en las empresas, estas CASIs no pierden el valor idiosincrático de los expertos con los que la empresa cuenta. Es importante recordar que el mencionado *know-how* incluye a estos expertos de dos formas:

1. **Racionales:** los profesionales constituyen la base del algoritmo sobre el cual se emplea la IA como refuerzo y/o como optimizador de la heurística del experto. Los racionales rigen los protocolos *on-platform* de los departamentos, y su impacto en la evolución sigue una curva sigmoidea para los humanos; es decir, al principio aportan un valor clave, pero con el tiempo este valor se vuelve estructuralmente marginal. Sin embargo, siguen siendo - y lo seguirán siendo durante muchos años - superiores a las máquinas en la detección de cambios en la distribución de datos (noticias, variaciones en el marketing, nueva naturaleza de un producto, etc.) y sus consecuencias. Por ende, pueden ser incorporados en las CASIs a través de Máquinas Aumentadas.
2. **Máquinas Aumentadas:** inputs con los que el ser humano puede añadir valor a la máquina de formas que aún no han sido descubiertas. Un ejemplo sería la investigación de alta frecuencia para ayudar a la máquina a decidir si debe entrar o no en una inversión y con qué peso (oportunidad versus confianza), tal y como se ilustra en el caso de uso abierto en *www.wallstreetland.xyz*.

Por lo tanto, las empresas deben asegurarse de no solo aprovechar al máximo el poder de las máquinas, sino también, y de manera crucial para las próximas décadas, definir y preservar el rol de los seres humanos en un entorno corporativo dirigido por máquinas - esto es, hemos de redefinir los trabajos en base a la naturaleza de las máquinas.

4.6. Conclusión

En conclusión, la Algoritmización de las empresas ofrece inmensas oportunidades en términos de eficiencia y productividad, pero también da paso a una nueva era

de amenazas cibernéticas, más sofisticadas, escalables e industrializadas que nunca.

Para navegar en este contexto, las organizaciones deben replantear su enfoque hacia la ciberseguridad, alejándose de soluciones genéricas y adoptando estrategias a medida que integren tecnologías avanzadas, teoría de juegos y defensas dinámicas.

Cabe destacar que, cuanto más proactiva sea una empresa en desarrollar estrategias de defensa propietarias, mayor será la probabilidad de que algunas de estas estrategias aborden de manera efectiva tanto las amenazas actuales como las emergentes. En la actualidad, muchas empresas se concentran en analizar los datos de ataques pasados, con la esperanza de que dichos patrones permanezcan constantes o evolucionen de manera predecible. Sin embargo, este enfoque presenta numerosos desafíos: a menudo existen cientos de métodos de ataque distintos que pueden dejar huellas digitales similares, lo que dificulta enormemente identificar con exactitud la estrategia utilizada.

En lugar de depender exclusivamente de los datos históricos, las empresas pueden tomar el control haciendo que sea estructuralmente más complejo para los atacantes desplegar cualquier estrategia. Este enfoque proactivo desplaza el énfasis de las defensas reactivas hacia las defensas preventivas, donde el objetivo no es solo analizar los ataques a posteriori, sino crear un entorno que interrumpa de manera inherente las amenazas potenciales antes de que se materialicen. Al incrementar la complejidad y la imprevisibilidad de la infraestructura de la empresa, se vuelve considerablemente más difícil para los atacantes lograr establecerse.

Al hacerlo, no solo pueden protegerse de las amenazas actuales y futuras, sino también convertir la ciberseguridad en un poderoso diferenciador competitivo que impulsa su negocio en un mundo cada vez más digital.

A la luz del contexto anterior, finalmente estamos listos para mostrar al lector el último *zoom-out* en relación al rol de la transformación avanzada en la ciberseguridad moderna.

5. Discontinuidad de Negocio: el Nuevo BAU cuando los Hackers se Convierten en Organizaciones Sobre Plataforma

Las empresas no están acostumbradas al nivel de competencia desatado por la nueva era del hacking. En términos de innovación, existe un desequilibrio entre el lado de negocio y el lado de la ciberseguridad de una corporación. Mientras que los rivales corporativos tienden a evolucionar de manera gradual y similar entre sí, los grupos de hacking operan de forma diferente. En ciberseguridad, las apuestas son exponencialmente más altas, y la carrera es implacable. La industria del hacking, impulsada por una rentabilidad masiva, avanza rápidamente hacia una Algoritmización de vanguardia, con los cibercriminales a menudo construyendo factorías *white-collar* por defecto. Estos grupos no solo están adoptando tecnologías de última generación, sino que también están estableciendo empresas falsas para reclutar de manera encubierta a los mejores talentos, a menudo sin que los reclutas se den cuenta de su participación en actividades ilegales. Esto conduce a una mayor eficiencia y productividad, culminando en ciberataques más inteligentes, a gran escala e industrializados, que representan una amenaza sin precedentes para las empresas. Más elocuentemente, mientras las corporaciones dividen su presupuesto tecnológico entre la mejora de sus factorías *blue-collar* y *white-collar*, la industria del hacking está prácticamente 100% enfocada en su factoría *white-collar*, con un enfoque total en generar ataques con el mínimo esfuerzo.

En este contexto, comprender cómo gestionar los ataques dentro del marco de la Algoritmización se vuelve crucial para manejarse en este nuevo ecosistema altamente competitivo. Aprovechando el conocimiento adquirido en los capítulos anteriores, este capítulo aborda una serie de ejemplos elocuentes para facilitar dicha navegación.

5.1. Federación: la Primera Línea de Defensa Nativa

Uno de los riesgos más pasados por alto en la era de la Digitalización es el robo de la ventaja competitiva, particularmente en áreas corporativas con una alta rotación de empleados, como se señala en 4.2. En el extremo, la propiedad intelectual (PI) de los departamentos *algorithmic-driven* está a solo un *copia-pega* de caer en manos de un competidor.

Protección de Algoritmos. Las tecnologías tradicionales no fueron diseñadas para proteger de manera específica contra este tipo de robo de propiedad intelectual (PI), lo que a menudo requiere protocolos forzados y ad-hoc para proteger información sensible. Sin embargo, aquí es donde entra en juego la lógica detrás de Data MAPs, construido sobre tecnología federada[3]. Al descomponer

[3]Donde la Federación aborda la optimización entre la Centralización y la Descentralización, buscando la libertad de esta última mientras aprovecha las sinergias de la primera.

los microservicios del software en unidades aún más pequeñas y distribuirlos a través de diversas aplicaciones, los algoritmos se fragmentan en piezas que residen en diferentes nodos entre servidores. De este modo, múltiples equipos pueden contribuir a la evolución iterativa de un algoritmo masivo sin que ningún equipo tenga una visión completa de todo el sistema, mientras están nativamente orquestados. Los protocolos federados hacen que el robo de propiedad intelectual sea exponencialmente más difícil.

Protección de Datos. Cuando se trata de datos, los protocolos de Federación incompletos presentan un problema importante. Se puede argumentar que, en el contexto de la Digitalización, la Federación no ha sido lo suficientemente ambiciosa; simplemente esparcir datos a través de los servidores departamentales para mejorar la calidad y la disponibilidad no es suficiente para una protección integral. En su lugar, los datos de los departamentos deben distribuirse en múltiples servidores de tal manera que, si se produce un ataque, solo se comprometan colecciones de datos aleatorias y no relacionadas. Por ejemplo, una brecha podría exponer el nombre de un cliente, una dirección de oficina, comentarios del departamento de recursos humanos sobre un empleado (no identificable) y el coste de una campaña de marketing (tampoco identificable), pero no lo suficiente como para causar daños[4]. Una estrategia de gestión de datos impulsada por algoritmos garantizaría la disponibilidad de los datos, mientras que la reorganización contínua de las colecciones de datos en los distintos nodos añadiría ruido a cualquier servidor comprometido. Más sobre esto en 5.3.

Como se examinará con mayor detalle, la implementación de la Algoritmización en el Core I ofrece un mecanismo de defensa robusto mediante la federación de algoritmos a través de múltiples nodos. Esta estructura no solo protege contra el hacking y la explotación externa, sino que también mitiga los riesgos operativos. Ya sea a través de las ventajas inherentes del modelo federado, como se ha expuesto en esta discusión, o aprovechando este marco para crear nuevas tecnologías de seguridad adaptativas, las empresas ahora pueden proteger sus operaciones de maneras que los sistemas tradicionales no son capaces de proporcionar.

[4]El atacante necesitaría permanecer en el servidor el tiempo suficiente para observar datos complementarios significativos. Y, para extraer su valor, se deben realizar un alto número de iteraciones a través de algoritmos específicos. Por lo tanto, se requeriría un esfuerzo considerable. Sin embargo, incluso si tiene éxito, solo podría realizar una reconstrucción parcial de la base de datos que, de otro modo, estaría directamente disponible para el hacker.

5.2. Tecnología Táctica: la Mejor Cómplice del CISO

Una vez implementado el modelo de la Empresa en Tres Capas, el Chief Technology Officer (CTO) puede desarrollar herramientas (*crafting vs stacking*) ad-hoc que permiten a la empresa evolucionar y garantizar el cumplimiento normativo. Este modelo mejora la resiliencia de la compañía, haciéndola robusta frente a riesgos operacionales y ataques informáticos, al mismo tiempo que apoya el crecimiento empresarial y el cumplimiento de la regulación.

Definimos *tecnología táctica* como una solución de software *suficientemente buena* que asegura las funciones esenciales de una aplicación especializada en un servicio. El primer paso es identificar los activos más críticos de la empresa, aquéllos que son vitales para su operativa y sostenibilidad continuas. Estos activos deben ser replicados internamente para asegurar un control absoluto sobre ellos, abarcando dónde se despliegan, cómo se protegen y cómo pueden evolucionar. El primer objetivo de la tecnología táctica es lograr una base sólida y robusta que pueda asumir el papel de un software de terceros frente a ataques o riesgos operacionales. Para ello, la empresa debe aprovechar las estrategias algorítmicas de la tecnología, como se explica en el capítulo 4.

En esta sección, veremos la relevancia de crear y mejorar gradualmente la tecnología táctica hacia una evolución ahora estratégica para dar forma a la plataforma propietaria de la empresa a largo plazo.

5.2.1. El *Good Enough* de Todo: desde el Control de Riesgo Operacional hasta el Refuerzo del Legacy

A medida que una empresa construye su stack tecnológico, inherentemente incorpora sistemas heredados de sus proveedores - a menudo en forma de rigideces. Estas limitaciones surgen porque los proveedores deben diseñar soluciones que se escalen a través de múltiples clientes. Para superar estas restricciones, las empresas suelen contratar consultores tecnológicos, quienes actúan como el *pegamento* entre diversas aplicaciones de software. Sin embargo, esta capa intermedia a menudo se convierte en su propia forma de legado adicional, ya que los consultores también diseñan soluciones con la escalabilidad en mente, con la intención de aplicarlas a su base de clientes más amplia.

Además, como se apuntó más arriba, dado que tanto los proveedores de tecnología como los consultores a menudo

operan en mercados oligopolísticos, las prácticas estándar involucradas en la construcción del stack tecnológico rápidamente restringen a las empresas de diversos sectores en su capacidad para diferenciarse tecnológicamente. Como resultado, la Digitalización, en lugar de permitir la diferenciación a través de la personalización, impulsa sutilmente la estandarización. Esto limita la capacidad de la empresa para destacarse frente a sus competidores, ya que la dependencia de soluciones ampliamente adoptadas reduce el alcance de la innovación tecnológica única.

Esta tendencia presenta desafíos significativos tanto para el negocio como para la ciberseguridad:

1. **Negocio:** Introduce dos nuevos riesgos de supervivencia. En primer lugar, existe la amenaza de competencia disruptiva por parte de los proveedores de tecnología, quienes controlan los sistemas heredados y obtienen un conocimiento muy amplio y preciso sobre la operativa de sus clientes. En segundo lugar, las empresas de diferentes sectores que comparten legados tecnológicos similares pueden buscar diversificarse, intensificando así la competencia entre industrias.

2. **Ciberseguridad:** La estandarización exacerba las vulnerabilidades. A medida que la tecnología se vuelve más uniforme, también lo hace la naturaleza de los ciberataques. Los hackers pueden concentrar sus esfuerzos en ataques generalizados, aprovechando las plataformas estandarizadas (aplicaciones y consultores), lo que facilita la explotación de debilidades comunes en un amplio rango de empresas.

La solución gira en torno al modelo de la Empresa en Tres Capas. Al aprovechar la capacidad de crear estrategias algorítmicas, la empresa puede competir de manera disruptiva con sus proveedores en términos de calidad y velocidad de implementación. Cabe destacar que el objetivo en este punto no es sustituir los servicios tecnológicos de esos proveedores, sino apoderarse de las piezas más relevantes del stack tecnológico, aquéllas clave para la empresa, de modo que recupere el control sobre los riesgos en cada momento y la evolución a lo largo del tiempo[5].

Este enfoque ofrece ventajas significativas tanto desde una perspectiva de negocio como de ciberseguridad:

1. **Negocio:** La mayoría del software altamente especializado alcanza, digamos, el 100% de las necesidades estándar de un departamento de la empresa en una tarea específica. Y, con un esfuerzo razonable de tres a cuatro meses, se puede crear, a bajo coste, una versión *suficientemente buena*[6] de muchas de las aplicaciones especializadas que el departamento necesita. Pero la plataforma que resuelve la complejidad holística de la transformación de cada departamento no se limita solo a los servicios de su propio departamento, sino que incluye otros de distintos departamentos: nos referimos aquí a Recursos Humanos incentivando a los miembros del equipo en sus nuevos quehaceres, ciberseguridad para proteger su propiedad intelectual, gestión de proyectos para rastrear el rendimiento del equipo, cuadros de mando a nivel de alta dirección para entender la evolución de la tecnología del departamento... La transformación hacia factorías white-collar y la riqueza de posibilidades tecnológicas disponibles significa que los jefes de departamento están acercándose más al rol de un CEO de una empresa pequeña (modo start-up) que al de un directivo tradicional. Además, tener la capacidad de interconectar toda esa tecnología de manera nativa abre un sinfín de posibilidades para pasar de estar por debajo del 100% en comparación con el estándar de la industria con esas versiones *good enough*, a superar con creces ese umbral.

2. **Ciberseguridad:** El Chief Information Security Officer (CISO) juega un papel clave en la detección de una amplia gama de riesgos operacionales. Por ejemplo, un banco puede seguir cumpliendo con las regulaciones contra el lavado de dinero (AML) incluso si los servidores de su proveedor externo - los que actualmente deciden si un pago es limpio o no - experimentan un apagón[7]. De manera más general, las empresas podrían evitar interrupciones comerciales debido a riesgos operacionales como la crisis generada por Crowdstrike en el verano de 2024. Si las empresas hubieran desplegado tecnologías tácticas en nodos que operan con diferentes sistemas operativos (por ejemplo, Ubuntu), habrían asegurado que sus activos fundamentales continuaran operando sin problemas a pesar de

[5] Basado en nuestra experiencia, el desarrollo de una versión táctica de software estándar de la industria suele tardar entre 5 semanas y 5 meses. La integración con el legacy tecnológico generalmente depende de proveedores externos, pero normalmente se logra en un plazo de 1 a 2 semanas, facilitada por la creciente "APIficación" del stack tecnológico. Una vez integrado, la evolución continua del software lo convierte en el estado del arte.

[6] Una que se enfoque en los usos principales y deje fuera las colas cubiertas por el software estándar de la industria.

[7] Y esto, como se mencionó anteriormente, también conduce a la hibridación de negocio, ciberseguridad y cumplimiento. Aún más, dado que los bancos centrales y las organizaciones supranacionales ya han mostrado interés en su proceso de Algoritmización, los próximos errores empresariales debido a la falta de tecnología táctica pueden no ser consideradas dentro del alcance de una excepción de fuerza mayor, sino como una imprudencia tecnológica. Y, por lo tanto, una nueva generación de ataques cibernéticos que buscan generar desconfianza entre los reguladores y en la prensa podría convertirse, indudablemente, en una realidad.

la disrupción externa. Así, esta flexibilidad en la arquitectura de ciberseguridad mejora la resiliencia y la continuidad operativa frente a fallos de terceros.

5.2.2. El Estado del Arte de Todo: Donde las Necesidades de Negocio y de Cumplimiento se Encuentran con las de Ciberseguridad

Una vez que la tecnología táctica está implementada, cubriendo una amplia gama de servicios esenciales a través de los departamentos y siguiendo el enfoque de la Empresa en Tres Capas, la progresión natural es la evolución continua. En esta etapa, la implementación inicial se centra principalmente en la mitigación de riesgos, replicando los activos y aplicaciones clave de la empresa. Sin embargo, a medida que la organización avanza, comienza a destinar esfuerzos alrededor de esta tecnología - primero, para actuar como una capa adicional de inteligencia, reforzando los sistemas existentes, y, eventualmente, para asumir plenamente nuevas funciones.

La tecnología propietaria de la empresa, que inicialmente funcionaba como una capa secundaria, comienza a ocupar un lugar central como la aplicación principal, mientras que el sistema original del proveedor externo se convierte en un elemento de apoyo, actuando como mitigador de riesgos y refuerzo. Este cambio no se trata únicamente de añadir complejidad, sino de ganar mayor control, flexibilidad y resiliencia frente a los desafíos en constante evolución.

La Capa Inteligente: Modernización del *Legacy*
Una vez que la empresa cuenta con dos sistemas de software ejecutándose en paralelo para el mismo servicio - la plataforma del proveedor externo y su propia tecnología táctica - se puede obtener información muy valiosa a partir de las discrepancias en sus resultados. Dado que estos sistemas se han desarrollado de manera independiente, cualquier divergencia entre sus salidas representa una oportunidad de optimización.

Cuando los resultados no se alinean, se presenta un punto de decisión. Al analizar las diferencias, la empresa puede tomar decisiones que, a priori, sean Pareto-superiores, es decir, que mejoren los resultados sin comprometer otros aspectos, en comparación con depender exclusivamente de la salida del software de terceros. Este enfoque de sistemas duales no solo optimiza la toma de decisiones, sino que también permite a la organización evolucionar más allá de las limitaciones de su arquitectura tecnológica original, creando un marco más adaptable y resiliente.

Innovación Personalizada y Control: Toma el Control de tu *Legacy*
A medida que el desarrollo avanza, esta tecnología base se transforma gradualmente en un sistema de refuerzo más sofisticado. En esta etapa, se superponen soluciones inteligentes y personalizadas sobre el software estándar de la industria, lo que permite a las empresas mejorar significativamente sus operaciones mientras mantienen dependencias con proveedores externos. Esta evolución se refleja en el aumento de su relevancia en el paso tres de la Fig. 5. El resultado dista de ser una mera protección temporal: representa un fortalecimiento sólido de las capacidades core de la empresa.

Una vez completada esta fase de refuerzo, las soluciones tácticas se convierten en activos estratégicos. Con un mayor control sobre estos sistemas críticos, las empresas pueden reducir su dependencia de proveedores externos, aumentando tanto su autonomía como su flexibilidad. A largo plazo, este enfoque facilita la creación de una infraestructura a medida y adaptable que se convierte en un elemento clave de la ventaja competitiva de la empresa. Esta infraestructura no solo es resiliente, sino también adaptable, evolucionando en paralelo con el crecimiento de la compañía y las amenazas que enfrenta.

5.2.3. La Consecuencia de la Hibridación: Eficiencia y Productividad en la Asignación del Presupuesto

El desafío ahora no radica en la tecnología de Core I en sí misma, que ha sido ampliamente investigada y validada por nuestro centro de excelencia y firma de consultoría (véase [5] para una explicación más detallada de la creación del grupo empresarial como objetivo para conseguir innovación disruptiva), el desafía radica en la asignación de recursos. El factor decisivo será cuánto presupuesto para la construcción de la Empresa en Tres Capas es asignado a los CISOs por sus organizaciones en comparación con los recursos que los ciberdelincuentes destinan a sus *líderes de Negocio*. Es decir, la tecnología para los ataques modernos y las defensas modernas ya está aquí y es totalmente operativa; la verdadera batalla ahora se centra en las prioridades presupuestarias entre los dos tipos de *agentes profesionales* - los legales y los ilegales.

Esta guerra presupuestaria es crucial porque refleja el compromiso de la empresa con su seguridad a largo plazo y su posicionamiento competitivo. Una empresa que entiende la importancia de esta inversión estará mucho mejor preparada para construir la infraestructura robusta, flexible y controlada internamente necesaria para proteger

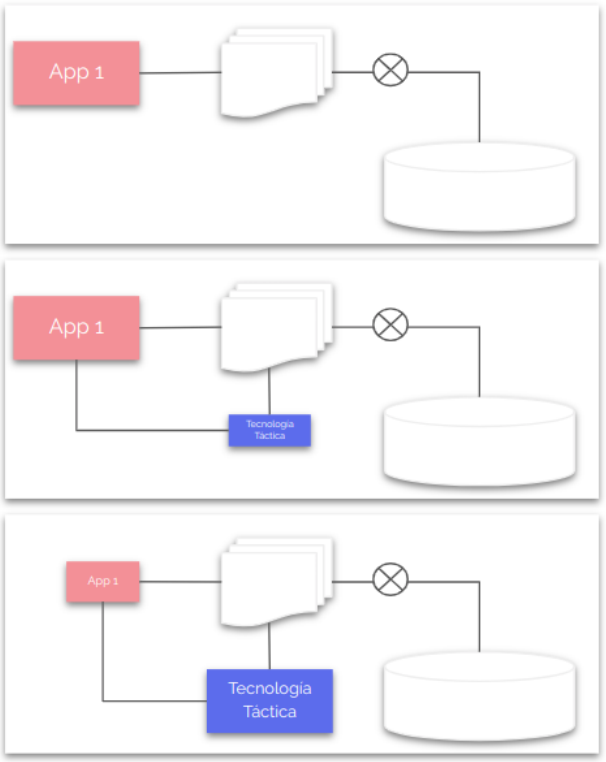


Figure 5. Evolución orgánica de la tecnología táctica: de refuerzo a líder.

sus activos críticos. Como se ha visto, tal inversión en la Empresa en Tres Capas no solo protege la operativa actual de la compañía, sino que también la posiciona para el crecimiento futuro al hacerla menos vulnerable a amenazas externas y dependencias empresariales. Además, pasando a tener un enfoque proactivo hacia la transformación algorítmica, las organizaciones pueden alejarse de su postura reactiva actual - donde responden constantemente a las amenazas a medida que surgen - de modo que un gran número de riesgos actuales se neutralicen de forma natural antes de que se conviertan en críticos.

Además, esta estrategia proactiva permite la integración fluida de nuevas tecnologías e innovaciones a medida que surgen, asegurando que el negocio se mantenga a la vanguardia sin comprometer sus sistemas core. A medida que las industrias continúan evolucionando y emergen nuevas amenazas, contar con una infraestructura flexible y personalizable será un diferenciador clave, permitiendo al negocio adaptarse rápida y eficazmente mientras mantiene una sólida ventaja competitiva. En última instancia, este enfoque transforma la ciberseguridad de una necesidad defensiva a una ventaja estratégica, que impulsa tanto la eficiencia operativa como el crecimiento de la empresa a largo plazo. Aquí es

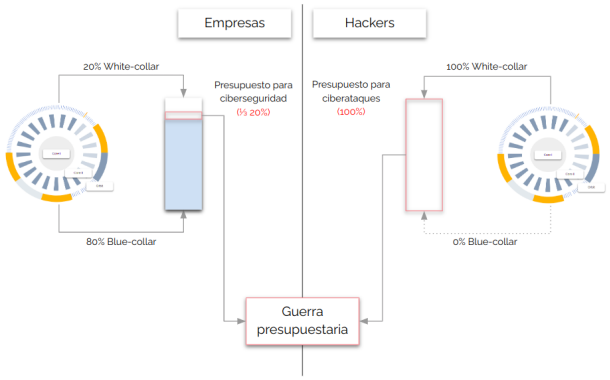


Figure 6. Guerra presupuestaria: distribución elocuente entre factorías en empresas y organizaciones de hacking.

donde la explotación de sinergias lleva el presupuesto del CISO a niveles completamente nuevos. Al involucrarse con el Core I, los CISO pueden apalancar sus recursos a través de varios mecanismos clave:

1. **Comenzando desde una Posición Privilegiada:** Los CISOs pueden remodelar el contexto tecnológico de manera propietaria al aprovechar la distribución de nodos, dándoles un mayor control sobre la seguridad sin tener que comenzar desde cero.

2. **Reciclaje de Recursos:** Las piezas de tecnología financiadas por Negocio o Cumplimiento Normativo pueden ser reutilizadas para ciberseguridad, maximizando el valor de las inversiones anteriores y reduciendo la necesidad de financiación adicional.

3. **Oportunidades de Compartición de Costes:** Los componentes esenciales requeridos tanto por Negocio como por Cumplimiento Normativo pueden compartirse entre departamentos, reduciendo los gastos generales mientras se mantiene una defensa robusta.

Este apalancamiento de recursos permite a los CISOs nivelar el campo de juego, equilibrando sus presupuestos limitados por negocio frente a los presupuestos de los atacantes. Mientras que los cibercriminales utilizan tecnología avanzada como motor de ingresos, las corporaciones a menudo consideran la ciberseguridad como una carga financiera. Sin embargo, este enfoque cambia la dinámica, permitiendo a las empresas aprovechar estas sinergias para una seguridad a largo plazo, al tiempo que optimizan la eficiencia financiera.

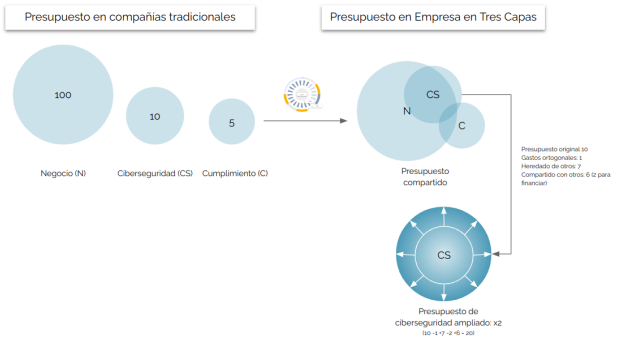


Figure 7. Sinergias presupuestarias: apalancando la Empresa en Tres Capas para duplicar el presupuesto del CISO.

5.3. CNE: de ser el Outlier a ser BAU

Las Explotaciones de Redes Informáticas (CNE, por sus siglas en inglés) se basan en comprometer un servidor y comenzar una vigilancia profunda para obtener una comprensión exhaustiva de cómo opera una empresa. Cuanto mayor sea el servidor y más centralizado esté su código y datos, más fácil se vuelve para un hacker comprender aspectos significativos del negocio. Al dedicar tiempo a perfeccionar su estrategia de ataque y esperar el momento más sensible para atacar, el hacker maximiza la relación riesgo-recompensa, haciendo que su inversión en la explotación sea altamente lucrativa.

Sin embargo, las CNE son relativamente raras en comparación con los Ataques a Redes Informáticas (CNA), que son más fáciles de ejecutar y proporcionan un retorno financiero más rápido. Los CNA suelen tener como objetivo obtener ganancias rápidas o visibilidad causando daños y adquiriendo notoriedad.

La pregunta que surge es: ¿Continuará esta tendencia o las empresas deben esperar un cambio hacia una mayor proporción de CNE en el futuro? Esta sección tiene como objetivo analizar ésta evolución y determinar si las empresas deben prepararse para CNEs más sofisticadas y específicas en los próximos años.

5.3.1. Calma: la Nueva Característica de los Hackers

La paralelización de ciberataques sobre estrategias algorítmicas cuando los hackers siguen el modelo de la Empresa en Tres Capas representa un cambio significativo en el panorama de amenazas, convirtiendo de forma efectiva cada vector de ataque en una fuente de ingresos separada para los cibercriminales. A medida que estas operaciones se automatizan y escalan, los hackers tendrán la paciencia y los recursos (diversificación entre empresas y a lo largo de horizontes temporales) suficientes para centrarse en objetivos altamente rentables a largo plazo.

Para defenderse de las amenazas cibernéticas cada vez más sofisticadas, las organizaciones deben adoptar un enfoque proactivo y dinámico. Esta estrategia abarca varias tácticas clave dirigidas a neutralizar preventivamente a los adversarios cibernéticos y mitigar posibles daños:

1. **Simulaciones Ágiles:** ejecutar simulaciones de manera continua que, aprovechando la Algoritmización, anticipen las tácticas de los ciberdelincuentes. Estas simulaciones deben diseñarse para identificar vulnerabilidades antes de que los adversarios puedan explotarlas y proporcionar información valiosa sobre posibles vectores de ataque, de modo que se puedan desarrollar nuevas defensas, basadas nuevamente en Algoritmización.

2. **Cambios de Contexto:** alterar el contexto de manera dinámica y en formas propietarias siguiendo Teoría de Juegos para añadir ruido, confusión y controlar el esfuerzo adicional requerido por la organización de hackers para perpetuar CNEs[8]. Por ejemplo, mover componentes de las aplicaciones (nodos) y datos siguiendo estrategias avanzadas de gestión de hardware y software. Dado que el ataque requiere primero resolver un problema complejo de Teoría de Juegos, incluso una vez dentro del sistema, el hacker profesional probablemente evitará atacar a una empresa con este nivel de complejidad y preferirá enfocarse en otras con un mayor retorno de inversión o impacto.

3. **Enfoques novedosos:** aprovechar el control que se tiene sobre la tecnología propietaria para implementar algoritmos avanzados. Por ejemplo, reciclar técnicas recientes como la Calibración Avatar para monitorear el comportamiento de los usuarios a través de aplicaciones, rastreando desviaciones respecto a los patrones típicos del *avatar* o comportamiento del usuario. Esta técnica ayuda a identificar posibles casos de suplantación de identidad y permite al sistema algorítmico desplegar contramedidas inmediatas, fortaleciendo el control sobre intentos de acceso fraudulentos.

4. **Sistemas automatizados de CERT (Equipo de Respuesta ante Emergencias Informáticas):** elevar las respuestas automatizadas a amenazas cibernéticas in-

[8] En adelante, en realidad es una buena práctica trabajar con la premisa *el hacker está dentro*, de modo que los mecanismos de mitigación de riesgos se implementen de manera constante y de forma nativa.

tegrando conocimientos provenientes de diversas aplicaciones y desencadenando respuestas algorítmicas sistemáticas ante ataques potenciales. De manera similar a los sistemas de trading algorítmico en hedge funds (ver [13],[14],[15]), estos sistemas deben ejecutar de manera autónoma las acciones defensivas óptimas, sin esperar la intervención humana. Cuantas más tareas puedan automatizarse, mejor será el tiempo de respuesta, dejando a los humanos como segunda línea de defensa.

5. **Máquinas aumentadas y firewall humano:** si bien la automatización es fundamental, es igualmente importante mantener la participación humana. Los expertos deben integrarse en el proceso, asumiendo nuevos roles que potencien la defensa algorítmica. Esto implica que los seres humanos actúen como un firewall en sí mismos o como agentes que aumenten las capacidades de la máquina. Al utilizar su experiencia para detectar anomalías que los sistemas automatizados puedan pasar por alto, los expertos humanos aportan un contexto crítico y, en ocasiones, actúan como barreras ante ataques totalmente autónomos. De este modo, la información sensible, que a menudo sólo reside en la mente de las personas, permanece inaccesible para los atacantes.

Al implementar estas estrategias, las empresas pueden crear un sistema de defensa robusto que no solo responda a las amenazas actuales, sino que también anticipe y frustre las amenazas futuras, otorgándoles una ventaja estratégica en un entorno de ciberseguridad en constante evolución.

5.3.2. Teoría de Juegos: la Protección Natural a Impulsar

Este cambio hacia soluciones personalizadas exige la integración de Teoría de Juegos en todos los aspectos de la ciberseguridad. La Teoría de Juegos, que modela las interacciones estratégicas entre adversarios, proporciona un marco para anticipar y contrarrestar los movimientos de los atacantes cibernéticos. Al aplicar dichos principios, las organizaciones pueden diseñar protocolos de comunicación dinámicos, arquitecturas adaptables y sistemas de software flexibles que no sólo respondan a las amenazas, sino que también interrumpan activamente la estrategia del atacante. Por ejemplo:

1. los protocolos de comunicación podrían ser diseñados para cambiar su comportamiento a tiempo real, creando un entorno de incertidumbre que aumenta el coste y el riesgo para los atacantes. De manera similar,
2. cuando las arquitecturas de software se diseñan siguiendo componentes modulares que pueden reconfigurarse rápidamente, como los de Core I, los sistemas pueden mantener su funcionalidad incluso bajo un ataque activo. Además,
3. al mover dinámicamente partes de las aplicaciones (nodos) y los datos a través de diferentes hardware y software, las empresas pueden crear un entorno impredecible que obliga a los adversarios a resolver problemas complejos antes de proceder. Esta táctica puede hacer que atacar a la empresa sea mucho menos atractivo, ya que el retorno de inversión para un hacker profesional disminuye en comparación con objetivos más fáciles.

Además, la integración de Teoría de Juegos en la ciberseguridad va más allá de las medidas técnicas. También implica una planificación estratégica a nivel organizacional, donde la ciberseguridad comienza a ser vista no solo como una medida defensiva, sino como una ventaja competitiva de Negocio. Las empresas que destacan en el cumplimiento algorítmico y en la defensa cibernética estarán mejor posicionadas para superar a sus competidores, no solo al proteger sus activos, sino al crear una marca más segura y confiable a los ojos de los clientes y socios. Este enfoque transforma la ciberseguridad de una postura reactiva y defensiva en un activo estratégico proactivo que puede impulsar el crecimiento empresarial, fomentar la innovación y asegurar el éxito a largo plazo.

5.4. IA: la Ignorancia Científica como Eslabón Débil

Por un lado, está la herramienta, la innovación en ciberseguridad impulsada por la inteligencia artificial. Es crucial entender que el estado actual de la innovación *data-driven* en ciberseguridad, dadas las técnicas avanzadas que los hackers profesionales tienen a su disposición, es propensa a cometer errores significativos. El problema radica en la diferente naturaleza de la distribución de los datos a través de las observaciones. A medida que las estrategias de hacking evolucionan, los datos del pasado se convierten en una guía poco fiable, representando solo una pequeña parte de las amenazas potenciales del futuro. Cada observación, cada estrategia de ataque, es un fenómeno singular, y agruparlas aumenta el ruido a la hora de detectarlas. El verdadero desafío que se presenta consiste en la transición de los conocimientos *data-driven* a las simulaciones algorítmicas, simulaciones que anticipen no solo las amenazas de ayer, sino también las de mañana. Ahí es donde comienza la verdadera evolución en la dinámica entre el *red team* y el *blue team*.

Por otro lado, está el uso de la inteligencia artificial en sí misma. Para los responsables de ciberseguridad, éste es un momento crucial. Necesitan confiar en expertos en apren-

dizaje automático que puedan detectar los riesgos de los ataques emergentes - ataques que se sitúan en ese complicado terreno intermedio entre los CNA y los CNE. Estos ataques intermedios no se centran en romper datos, sino en alterarlos sutilmente, distorsionando los modelos *data-driven* para favorecer resultados diferentes e involuntarios. Los ataques estándar y directos a los datos son una cosa, pero el verdadero peligro proviene de enfoques más sofisticados destinados a obtener conocimientos más profundos, tales como:

- Romper las asunciones subyacentes de los modelos, de tal manera que su aplicación sea errónea por diseño.
- Aprovechar la sensibilidad natural de los modelos, en las regresiones lineales a los *outliers*, o las redes neuronales a los umbrales (temas discutidos a fondo en [5]).
- Explotar las limitaciones de los *Large Language Models* (LLMs), que tienen dificultades para procesar *outliers*, especialmente en resúmenes. Los LLMs no analizan cada documento en sus propios términos; lo fusionan con la memoria que han construido en torno a temas relacionados alrededor del ecosistema abordable en internet.

Y no solo los datos están en riesgo. Variaciones menores, casi imperceptibles, en librerías de modelos pueden pasar desapercibidos y causar estragos. Aquí es donde el control en tiempo real de las librerías se vuelve esencial. Sin una estrategia para rastrear, auditar y controlar estas librerías mientras se están utilizando, los equipos de ciberseguridad podrían encontrarse luchando en una batalla de la que ni siquiera son conscientes que están perdiendo. El monitoreo en tiempo real a través de estrategias algorítmicas ya no es un lujo; es una necesidad. La pregunta no es si sus sistemas están bajo ataque; es si puede verlo suceder a tiempo para detenerlo.

5.5. Cumplimiento: Fuera del Negocio de un solo Golpe

A medida que la innovación avanza, también lo hace la complejidad, y las implicaciones de esta evolución no siempre son claras ni fáciles de predecir. En respuesta, los gobiernos están intensificando sus esfuerzos regulatorios, lo que resulta en una red de requisitos de cumplimiento que a menudo se ven como una carga para las empresas. El incumplimiento puede acarrear multas elevadas y, en algunos casos, la revocación de licencias, lo que puede impactar drásticamente tanto en la operativa como en la reputación corporativa.

Dada la situación regulatoria, las empresas tienden a asignar recursos mínimos a cumplimiento, considerándolo como una preocupación necesaria pero secundaria. Esta falta de inversión presenta un terreno fértil para que los hackers lo exploten.

Sin embargo, imaginemos un escenario en el que el modelo de la Empresa en Tres Capas está completamente implementado. En este modelo, el cumplimiento regulatorio ya no sería solo un mero requisito regulatorio, sino un activo estratégico. Al integrar el cumplimiento regulatorio de manera nativa dentro de la infraestructura algorítmica de la empresa, se pasa de tener una obligación a tener una ventaja competitiva. Este enfoque no solo mejora el control sobre los procesos de cumplimiento, mediante soluciones algorítmicas avanzadas, sino que también asigna recursos para salvaguardar este vector crítico de riesgo con el mismo nivel de sofisticación aplicado a otras áreas del negocio.

En un marco así, el cumplimiento se convierte en un proceso proactivo e integral de la operativa de la empresa, entrelazada en el tejido de sus iniciativas tecnológicas y estratégicas. Esto no sólo mitiga el riesgo, sino que también posiciona a la empresa para responder de manera más efectiva a los cambios regulatorios, transformando lo que tradicionalmente se considera un desafío de cumplimiento en un activo estratégico.

5.6. Manipulación del Precio de Mercado: Privada o Pública

El hacking tiene muchas más dimensiones de las que se reconocen actualmente, y estamos a punto de presenciar la explotación de estas dimensiones de maneras sin precedentes, particularmente en los mercados. En lugar de limitarse a exigir un rescate o causar interrupciones en Negocio, los hackers ahora buscan obtener un beneficio más rápido y limpio: aprovechar los ataques para manipular los mercados. Estos ataques explotan las vulnerabilidades en las estructuras empresariales, reputacionales y de cumplimiento de una compañía y luego se dirigen a los mercados para recoger las recompensas.

En cierto sentido, este tipo de hacking no es muy diferente de las técnicas agresivas utilizadas por los hedge funds cuando publican informes negativos sobre empresas para hacer que los precios de sus acciones caigan[9]. Sin embargo, hay mucho más bajo la superficie. Esta sección explica cómo hackear el valor de una acción para obtener una

[9] Ej. Investigación de Gotham City sobre Grifols al inicio del 2024.

recompensa inmediata y con dinero limpio, y cómo hacer para evitarlo desde la empresa.

5.6.1. El Ataque: de Nuestra Predicción a la Realidad

Durante años, hemos estado advirtiendo a los CEOs de empresas de todos los tamaños y sectores sobre las estrategias más simples de manipulación del mercado que los hackers pueden emplear. No fue hasta el sonado caso de GameStop - donde se aplicaron técnicas similares, pero de forma inversa[10] - que comenzaron a comprender la gravedad de esta forma de ataque.

El funcionamiento sería el siguiente:

Imagina que un hacker profesional de este tipo quiere obtener ganancias vendiendo a precios altos o comprando a precios bajos. Ya sea el objetivo una startup en los mercados privados (altamente sensible a los eventos de hacking mencionados anteriormente), una empresa que cotiza en bolsa en los mercados públicos (cuanto más pequeña sea la empresa, mayor será su sensibilidad al precio) o incluso un país entero a través de la combinación de los dos anteriores[11]. Una estrategia eficiente sería la siguiente:

1. Vende las acciones (o compra una opción de venta, es decir, el derecho a venderlas a un precio determinado). Ya sea que tenga capital suficiente para mover el mercado o convenza a una red de otros hackers para que sigan su estrategia. A medida que todos venden, el precio comienza a bajar por mero impacto de mercado.

2. Después de vender, explican en las redes sociales por qué están vendiendo y por qué todos deberían seguirlos. Esta parte incluye *fake news* y podría beneficiarse de agentes falsos en redes sociales. Es clave hacerlo en manada para que el algoritmo de las diferentes redes sociales sobrepondere la relevancia del tema y lo priorice.

3. Los inversores reales ven la caída del precio y comienzan a preocuparse. Buscan información, y los motores de búsqueda los llevan directamente al contenido generado por el hacker - siempre, gracias al diseño del algoritmo del motor de búsqueda. Así, dada la desinformación, la aversión al riesgo y los sesgos conductuales, una cantidad significativa de ellos comienza a vender. El precio baja nuevamente.

4. Los inversores algorítmicos continúan la venta, ya que ya hay un patrón bajista consolidado significativamente en los datos de la acción, tanto en precios como en fuentes de información. La acción cae aún más.

A lo largo de este camino, representado en la Fig. 8, la riqueza de los inversores disminuye en decenas de millones, si no cientos. Así que, se puede esperar que los inversores exigirán a sus senior managers que sus acciones sean adecuadamente protegidas en el futuro. En particular, el servicio de protección se convertirá en una práctica habitual en empresas con una propiedad concentrada y significativa (como las empresas controladas por familias).

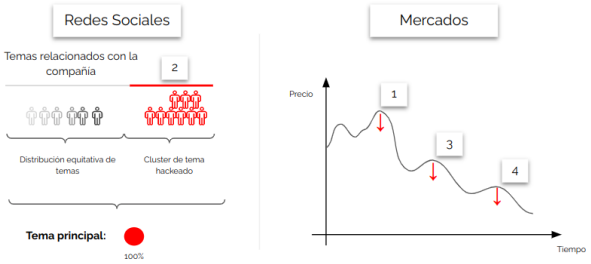


Figure 8. Una estrategia de hacking novedosa y altamente efectiva para manipular los precios de los mercados privados y públicos.

5.6.2. La Defensa: la Belleza de las Plataformas *All-in-One*

Una empresa que ha implementado el Modelo de la Empresa en Tres Capas puede orquestar, de manera algorítmica, la respuesta a estos ataques a través del departamento de Comunicaciones y la oficina del Director Financiero, especialmente si dentro del Core II está disponible *trading algorítmico*, como se representa en la Fig. 9.

1. La primera caída de precios debido al impacto en el mercado no se puede evitar, pero puede ser detectada por el algoritmo del Director Financiero.

2. La desinformación en las redes sociales tampoco puede ser evitada, pero puede ser detectada por el algoritmo de seguimiento del departamento de Comunicaciones.

3. El equipo de Comunicaciones despliega un contraataque. Inundan las mismas plataformas de redes

[10] En realidad, lo que se quería era derribar a un hedge fund, no a una empresa listada. Como el hedge fund tenía las acciones en corto, la estrategia consistía en aumentar el precio de las acciones comprándolas, añadiendo un componente romántico para que la gente no se sintiera como hackers manipuladores, sino como salvadores de la acción.

[11] [10], un documento que elaboramos para la OTAN, reflexionó además sobre las implicaciones geoestratégicas de tal enfoque. Un país puede apoderarse de otro sin necesidad de disparar un solo tiro. Simplemente al hackear el valor de las empresas en los mercados, controlando el país a través de los consejos de las principales compañías y obteniendo ganancias en el ínterin.

sociales con información oficial y precisa a la misma escala que la desinformación, replicando el número de *me gusta*, el número de veces que los comentarios se han compartido y el número de comentarios generados por los hackers. Para ello, hacen uso de agentes autónomos[12].

4. El Director Financiero comienza a montar autocartera con un nivel de agresividad y urgencia que dependen de las señales provenientes del departamento de Comunicaciones, es decir, de su algoritmo de seguimiento de la marca. A más agresividad en redes sociales que derive en mayor impacto en mercados, mayor agresividad de compra.

5. Cuando los inversores consultan el precio de las acciones, pueden notar el efecto de la primera caída (1), pero una parte de éste ya se habrá erosionado por el contraataque mencionado en el paso (4). Y, aunque la caída inicial haya sido considerable, al buscar información sobre la empresa, el algoritmo habría posicionado en la parte superior tanto las noticias sobre el hackeo como la respuesta oficial. Por lo tanto, la caída del precio debido a aquellos que aún desean vender sería mucho menor.

6. Los patrones de datos ya se habrían roto gracias al contraataque (4), de modo que los algoritmos no activarían ninguna venta adicional y, así, el movimiento no se amplificaría.

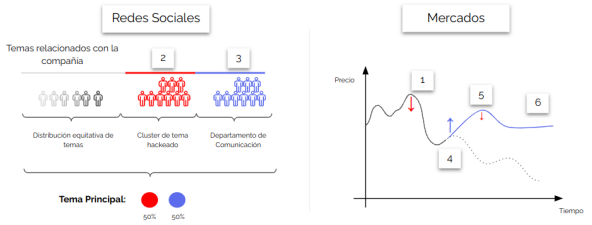


Figure 9. La respuesta algorítmica, a través de los departamentos, muestra los roles y dinámicas en la lucha contra la manipulación del mercado.

Lo mejor de todo es que esta estrategia es sistemática, transparente y completamente auditable. No solo cumple con las regulaciones, sino que es efectiva, convirtiendo un intento de manipulación del mercado por parte de un hacker en una oportunidad para que la empresa demuestre su resiliencia y proteja su valor.

[12]Observe la sinergia entre las tareas de las máquinas y las tareas de los humanos en este ejemplo.

5.7. Conclusión

Ha surgido una multitud de nuevos riesgos, y priorizarlos de manera efectiva es ahora más crucial que nunca. Uno de los aspectos más desafiantes de la Transformación es la autocrítica. La naturaleza humana tiende a resistirse al cambio y prefiere mantener el *momentum*, incluso cuando dicho *momentum* tiene su orígen en protocolos obsoletos. Muchos de estos protocolos, profundamente arraigados en la operativa de la empresa, son en realidad parches: soluciones temporales que abordaron limitaciones de años atrás, pero no lo que realmente era ideal. Las disrupciones causadas por innovaciones como Data MAPs y el modelo de la Empresa en Tres Capas abren nuevas posibilidades, permitiendo la consecución de objetivos que antes parecían imposibles en cada departamento de la organización.

Hemos hablado de varios protocolos nuevos que enfatizan la hibridación de los departamentos - ya sea centrados en tecnología, como en 5.6, o relacionados con el presupuesto, como en 5.2 -, al mismo tiempo que preservan su autonomía a través de una estructura federada. Esto es lo que define a una empresa moderna.

Y con las empresas modernas surge la necesidad de una ciberseguridad moderna. Ya no se trata simplemente de mantenerse al día con la evolución del negocio; la ciberseguridad se ha vuelto esencial porque los hackers son cada vez más profesionales y, sin duda, aprovecharán los avances logrados por estas empresas para aumentar su propia eficiencia y productividad a niveles nunca antes vistos. En consecuencia, las organizaciones deben comenzar a orquestarse de maneras nuevas y sofisticadas. Los ataques de hoy - y especialmente los del mañana - no solo buscarán interrumpir la operativa de la empresa, sino que serán más dirigidos, con el objetivo de causar daños en múltiples dimensiones de la misma.

Estos nuevos riesgos deben ser reconocidos, y los riesgos antiguos a los que nos hemos acostumbrado deben ser re-priorizados en función de este nuevo contexto en constante evolución. La Transformación no se trata solo de perseguir nuevas oportunidades, sino también de identificar las nuevas vulnerabilidades que éstas conllevan, y de abordarlas con una mentalidad proactiva y estratégica.

6. Conclusiones y Trabajo Futuro

A lo largo del documento, hemos llegado a la conclusión de que, del mismo modo que la IA moderna no será *data-driven*, sino *algorithmic-driven* - como se explica detalladamente en el [5] - , la ciberseguridad moderna

seguirá el mismo camino.

La Digitalización está avanzando hacia la Algoritmización a tal velocidad que los datos del pasado se han vuelto demasiado obsoletos para proporcionar información relevante a la defensa de hoy. Son sólo una instancia caprichosa, un fragmento de los tipos de ataques que podrían ocurrir. Y a medida que crece el potencial para nuevas formas de ciberataques, lo que realmente importa ahora son los datos estresados: escenarios simulados que llevan los sistemas al límite y ofrecen una visión de las amenazas futuras que podrían surgir.

Como resultado, desarrollar estrategias de ciberseguridad autónomas y altamente avanzadas ya no es solo una mejor práctica; es un imperativo: pasar de una defensa pasiva a una proactiva. Estas estrategias deben diseñarse para introducir un nivel de complejidad e imprevisibilidad que eleve significativamente la dificultad para los atacantes. El futuro de la ciberseguridad dependerá del despliegue de defensas inteligentes, a gran escala e industrializadas, capaces de igualar la sofisticación de las amenazas que buscan contrarrestar. Estas defensas no solo protegerán los sistemas actuales, sino que también permitirán a las organizaciones innovar con nuevas arquitecturas y protocolos más flexibles, mejorando su resiliencia y adaptabilidad frente a amenazas en constante evolución. Y esto no es teoría, es práctica - la tecnología ya está plenamente disponible.

Uno de los aspectos más críticos de este enfoque es el cambio de soluciones de ciberseguridad genéricas y preconfiguradas a estrategias personalizadas, adaptadas a las necesidades y vulnerabilidades específicas de cada organización, y capaces de aprovechar Teoría de Juegos para añadir ruido a los atacantes modernos. Las soluciones preconfiguradas, aunque convenientes, son intrínsecamente más vulnerables a la explotación, ya que son estandarizadas y ampliamente conocidas. Los ciberdelincuentes pueden estudiar estas soluciones, identificar sus debilidades y desarrollar ataques industrializados que se despliegan sobre múltiples objetivos. En contraste, las estrategias de ciberseguridad diseñadas a medida introducen capas únicas de complejidad que dificultan exponencialmente la sistematización y escalabilidad de los esfuerzos de los atacantes. Las plataformas tecnológicas modernas se construyen a medida - más piezas propietarias y menos stack de terceras partes. Al incorporar elementos personalizados en sus defensas, las organizaciones pueden crear un *target* que es dinámico para los atacantes - literalmente, a través de tecnologías federadas basadas en algoritmos como Data MAPs - que resulta mucho más difícil de penetrar.

El trabajo de nuestro Centro de Excelencia se dedicará, en un futuro cercano, a apalancarse en ser pioneros en el proceso de Algoritmización. Y dado que la ciberseguridad es uno de los campos más críticos que impactan a la sociedad en la actualidad, dedicará parte de sus recursos a este nuevo *greenfield*: la carrera armamentista entre la Ciberseguridad Algorítmica y el Hackeo Algorítmico. Utilizaremos nuestra plataforma desarrollada bajo el modelo de la Empresa en Tres Capas para generar más investigación que ayude a entrenar a los equipos de ciberseguridad - blue team y red team - a navegar apropiadamente esta nueva era. Además, investigaremos casos de uso que eduquen a las empresas sobre cómo financiar sus presupuestos de tecnología mediante la hibridación de negocio, ciberseguridad y cumplimiento al decidir su tecnología. Dicha tecnología debería pasar gradualmente de un conjunto amalgamado de software de terceros a una plataforma propietaria nativa algorítmica, respetando el *legacy* a través de una Arquitectura de Producción Extendida, como se explica en [6]. En lugar de evolucionar el *greenfield* de manera independiente, la intención es colaborar con asociaciones de CISOs en todo el mundo para captar información sobre lo que es más relevante para ellos en general, qué partes no comprenden completamente, etc., de modo que se puedan desbloquear rápidamente soluciones propietarias ad hoc en diversos sectores. Esto es, más que una mera evolución teórica, buscamos impacto. En este sentido, esta iniciativa comenzará con el ISMS Forum, sirviendo como punto de partida para compromisos más amplios con profesionales de ciberseguridad a nivel mundial.

En resumen, se trata más que un simple avance tecnológico; es un cambio fundamental en la forma en que las empresas deben concebir la ciberseguridad, convirtiéndola en un componente central, *algorithmic-driven*, de su estrategia corporativa para el futuro.

References

[1] Drayer, P., Jones, T., Klima, T., Oberholtzer, J., Srong, A., Welburn, J., & Winkelman, Z. (2018). Estimating the Global Costs of Cyber Risk. Justice, Infrastructure and Environment. Rand Corporation.

[2] Gavenaite-Sirvydiene, J., Miecinskiene, A. (2021). Forecasting Costs of Cyber Attacks Using Estimation The Global Cost of Cyber Risk Calculator V 1.2. Conference: International Scientific Conference ,Contemporary Issues in Business, Management and Economics Engineering.

[3] López Gutiérrez, J., Sánchez Jiménez, F., Herrera

Sánchez, D., Martínez Moreno, F., Rubio García, M., Gil Pérez, V., Santiago Orozco, A., Gómez Marín, M. (2020). Informe sobre la Cibercriminalidad en España. Secretaría de Estado de Seguridad (Ministerio de Interior).

[4] Voo, J., Hemani, I., Jones, S., DeSombre, W., Cassidy, D., Schwarzenbach, A. (2020). National Cyber Power Index. Belfer Center for Science and International Affairs (Harvard Kennedy School).

[5] Alvarez-Teleña, S. and Díez-Fernández, M. (2024). Advances in Artificial Super Intelligence: Calm is All You Need. SSRN.

[6] Alvarez-Teleña, S. and Díez-Fernández, M. (2022). Data MAPs: On-Platform Organisations. SSRN.

[7] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Transformation: Why and How CEOs are Moving from Digitalwashing to White Collar Factories. SSRN.

[8] Alvarez-Teleña, S. and Díez-Fernández, M. (2024). The Lean Aggregation Behind the Next M&A, Tenders and Organic Growth: Federation and the Three-Layer Companies. SSRN.

[9] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in AI: When Applied Science is not Science Applied. SSRN.

[10] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Cognitive Warfare: Augmented Machines upon Data MAPs towards a Fast and Accurate Turnaround. SSRN.

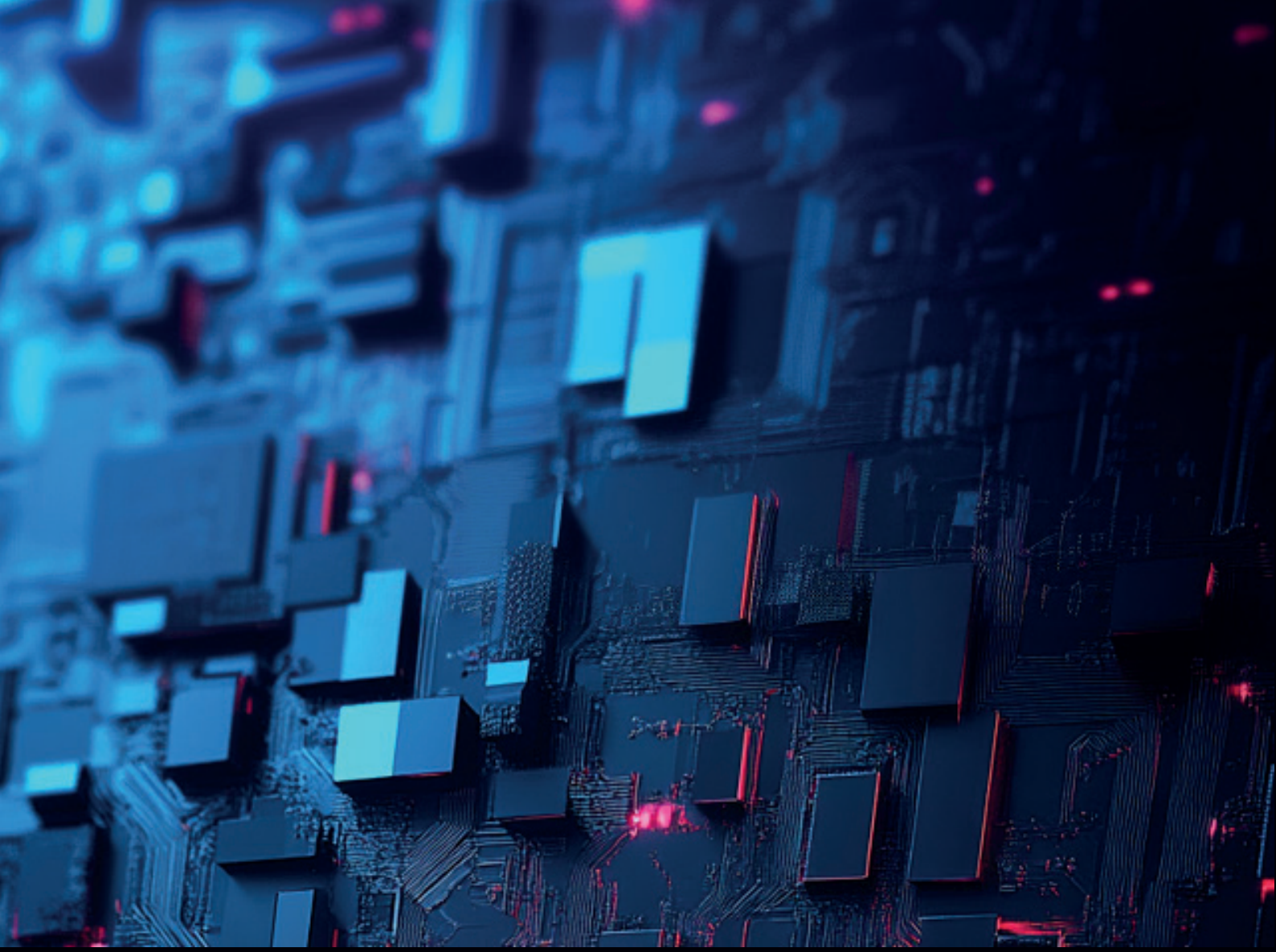
[11] Alvarez-Teleña, S. (2024). Transformación Avanzada. 3648, La Inteligencia Artificial Aplicada a la Ingeniería Civil. Revista de Obras Públicas.

[12] Alvarez-Teleña, S. and Díez-Fernández, M. (2024). Transformación Avanzada. Recuperando el Liderazgo Militar en Innovación. 80, Boletín de Observación Tecnológica en Defensa.

[13] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Portfolio Management: Dimension-Driven Portfolios. SSRN.

[14] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Portfolio Management: On-Platform Performance Attribution. SSRN.

[15] Alvarez-Teleña, S. and Díez-Fernández, M. (2023). Advances in Portfolio Management: On-Platform Governance for Portfolio Managers. SSRN.



CONTACTA CON NOSOTROS

Si estás interesado/a en colaborar con nosotros o necesitas más información sobre nuestros proyectos, escríbenos a:
proyectos@ismsforum.es

isms forum