PROSEGUR RESEARCH

Hybrid Security Series

Los datos en **seguridad híbrida**

2025

PROSEGUR
SECURITY

Este documento es **interactivo**

HOME

01

El océano en la oficina

HOME

01
El océano en la oficina

02
Data momentum

03
Cultura del dato: marco de competencias

04
Datos para una seguridad híbrida de confianza

EL OCÉANO EN LA OFICINA

Vivimos en la era del dato, fluyendo a nuestro alrededor como un vasto océano de información. En este entorno, la **capacidad de saber mirar** se ha convertido en una habilidad crucial, una especie de brújula que nos guía a través de la complejidad y la incertidumbre. Al igual que los fractales[1], donde cada parte refleja el todo en un patrón infinito y repetitivo, los datos esconden en su aparente caos una estructura subyacente que solo se revela a quienes tienen la perspicacia de observar con atención.

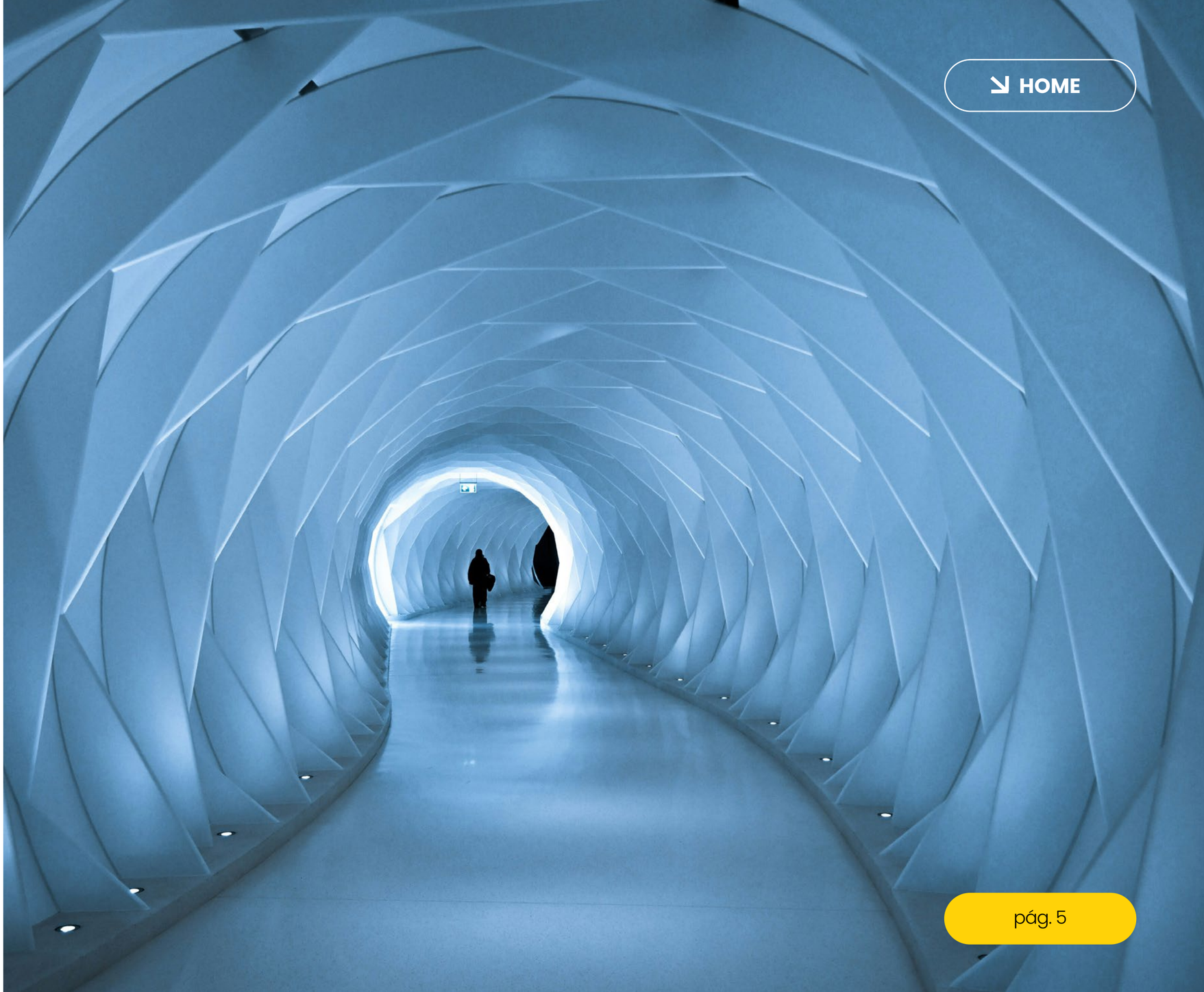
Quienes dominan el arte de interpretar datos se mueven con soltura en un mar de símbolos, encontrando patrones y conexiones indetectables a simple vista, igual que la medusa con su cuerpo transparente y enigmático se desplaza sin esfuerzo en las profundidades del océano, **adaptándose y evolucionando según las corrientes.**

Esta habilidad no es fortuita; hay que trabajarla de forma continua y en muchos casos se gesta en la infancia, **moldeada por los juguetes que nos rodean.** Estos primeros objetos de juego, aparentemente simples, siembran las semillas de nuestras futuras capacidades cognitivas y profesionales, influyendo en nuestra forma de **mirar lo que nos rodea.**

[1] Los fractales son estructuras geométricas que se caracterizan por tener una forma irregular, compleja y autosemejante, lo que significa que su patrón se repite a diferentes escalas. En otras palabras, si amplías una pequeña porción de un fractal, encontrarás una estructura que es similar (aunque no necesariamente idéntica) al fractal en su conjunto.

HOME

Si el desafío es **comprender un mundo en constante cambio**, donde los datos se generan de manera incesante, es claro que debemos **mejorar nuestras habilidades** para interpretar la información que nos rodea. Esto nos obliga a revisar nuestras formas de análisis, las fuentes y metodologías que utilizamos, y, sobre todo, a **replantear cómo entendemos los datos.** Lograremos una mejor comprensión de nuestro paradójico entorno de datos ordenados y caóticos a la vez si logramos ampliar y profundizar nuestra perspectiva, integrando diversas visiones, **encontrando el valor de los datos** que hasta ahora no nos parábamos a observar.



HOME

02

Data momentum

HOME

01
El océano en la oficina

02
Data momentum

03
Cultura del dato: marco de competencias

04
Datos para una seguridad híbrida de confianza

HOME

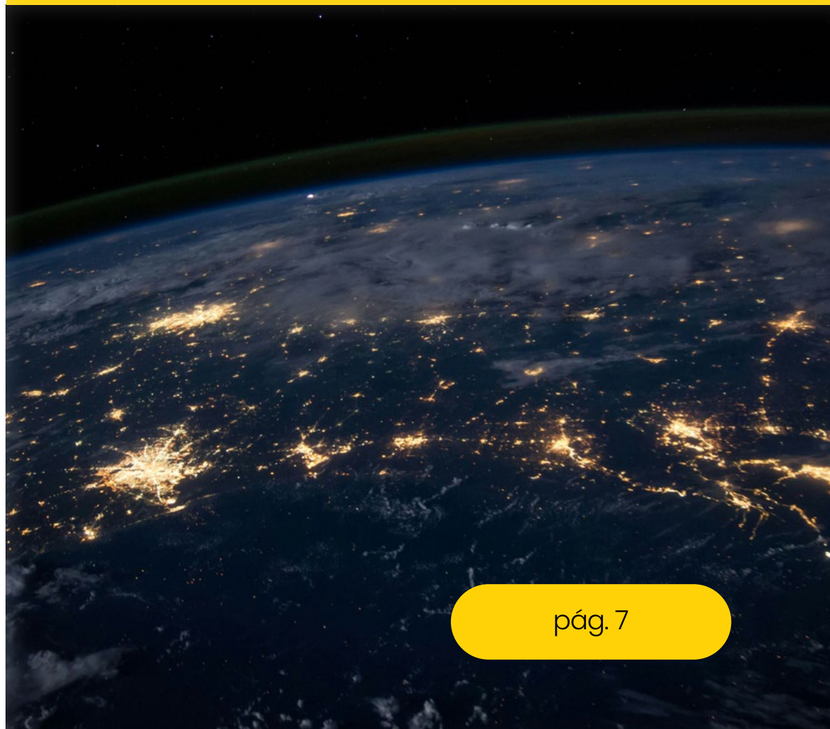
02

DATA MOMENTUM

La idea de que la realidad está compuesta por un conjunto de elementos regidos por normas y estructuras superiores no es nueva, tal y como Pitágoras explicaba que **todo es número.** En el siglo V a. C., Demócrito y Leucipo determinaron que el universo estaba compuesto por partículas indivisibles, eternas e indestructibles que, combinándose, constituían aquello que la humanidad podía observar y sentir. Todo ello, con base en el razonamiento y la intuición. Es lo que en la actualidad se puede denominar ***situational awareness:*** **la habilidad para analizar el contexto**, a diferentes niveles, para responder a cada situación de la manera más efectiva posible.

En el entorno empresarial de primer nivel, donde la agilidad y la eficiencia son esenciales, es fácil caer en la tentación de utilizar los datos de manera rápida y sin reflexión profunda. Ahora bien, para que los datos se conviertan en una herramienta verdaderamente poderosa, es crucial que las empresas **reserven y agenden tiempos y espacios específicos** para trabajar con ellos de manera reflexiva. Esto implica no solo entender qué son los datos, sino **también explorar críticamente para qué sirven**, cómo se alinean con los objetivos estratégicos y cómo pueden generar valor real. Sin estas pausas para el análisis, se corre el riesgo de tomar decisiones apresuradas, basadas en interpretaciones superficiales que podrían desviar el rumbo de la empresa.

En un contexto donde la tecnología y los métodos de análisis de datos evolucionan constantemente, la necesidad de ***upskilling*** y ***reskilling*** se vuelve crítica. Los empleados deben estar equipados no solo con las habilidades técnicas necesarias para manejar y analizar datos, sino también con la capacidad de **pensar de manera crítica y creativa** sobre el uso de esos datos. La formación continua en estas áreas no solo mejora la competencia técnica del equipo, sino que también fomenta una cultura empresarial en torno a los datos.



EN FOCO:
LA IMPORTANCIA DEL ANÁLISIS

¿Qué importancia tiene el diseño de un balón en un deporte como el fútbol? Con la reciente celebración de la Eurocopa, uno de los focos silenciosos se ha depositado en el esférico oficial del campeonato, el Fussballliebe. Y es que un grupo de ingenieros de Adidas ha permitido, a partir de un innovador diseño que toma elementos de otros deportes -como el golf-, que los lanzamientos de los jugadores no vieran su trayectoria desviada y que el juego se desarrollase de forma adecuada: un éxito invisible, aunque de gran calibre. Este es solo un ejemplo de una esencia velada en todo y todos: las matemáticas y los datos. En un primer momento de encuentro, los objetos y procesos del entorno pueden presentarse distintos y ajenos a nosotros. No obstante, a través de su estudio y observación, pueden desagregarse informaciones y datos con los que interpretar el hecho y establecer patrones y generalizaciones, finalmente capacitando el entendimiento y el progreso. Desde las erráticas trayectorias del Jabulani de la Copa del Mundo de 2010 al Fussballliebe de la Eurocopa de 2024.

2.1.
Del dato al insight

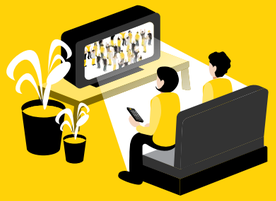
El valor del dato ha adquirido una **relevancia sin precedentes en el contexto empresarial actual**, impulsado por la digitalización y la creciente cantidad de información generada en todos los ámbitos de la vida cotidiana.

Vivimos en un contexto donde **la información y los datos no solo proceden del entorno físico;** nuestra actividad es también emisora de datos, por ejemplo, al usar determinadas plataformas digitales o al estar en contacto con cámaras de seguridad. En este nuevo escenario, donde existe una **sobrecarga de datos** importante y lo real es, en ocasiones, difícil de distinguir de lo falaz, cobra importancia destacar las **habilidades analíticas** a la hora de aproximarse a la información. De hecho, desde instituciones como el Foro Económico Mundial señalan que el **pensamiento analítico** es una de las habilidades más demandadas por los empleadores en la actualidad.

Fuente: Prosegur Research, 2025.

HOME

El crecimiento de la **densidad de información**

	Redes sociales	Hogar	Seguridad
2010			
	• 140 caracteres • Baja resolución y compatibilidad	• DVR, Blackberry (3G)	• CRA con tecnología instalada
2020			
	• 280 caracteres e introducción de gifs, vídeos, imágenes, hashtags, emojis, streamings, tweets, etc. • Alta resolución y compatibilidad. Inclusión de stickers, filtros, música.	• Smartphone (LTE o 5g), Netflix, Nintendo Switch, Apple Watch.	• iSOC con tecnología operada

En un entorno donde las decisiones deben tomarse con rapidez y precisión, **los datos se han convertido en un activo fundamental** que permite a las empresas anticipar tendencias y responder de manera efectiva a las necesidades de sus clientes. La capacidad de analizar grandes volúmenes de datos no solo facilita la identificación de patrones y comportamientos, sino que también permite a las organizaciones desarrollar estrategias más informadas y adaptadas a sus objetivos específicos.

Además, el uso de datos en la toma de decisiones se traduce en una mejora significativa en la eficiencia operativa y en la rentabilidad de las empresas. Al adoptar un enfoque basado en datos, las organizaciones pueden optimizar sus procesos, reducir costos y maximizar el retorno de inversión. Esto se refleja en la implementación de **estrategias data-driven, validadas por expertos**, donde cada acción se fundamenta en análisis concretos, lo que minimiza el riesgo de errores y maximiza las oportunidades de éxito. En este sentido, el dato no solo se convierte en un recurso valioso, sino en un motor de innovación y crecimiento. Con el objetivo de **optimizar** la **toma de decisiones**, en particular en contextos de seguridad, es de extraordinaria relevancia el apoyo en informaciones y **datos de carácter tanto estratégico como operativo.**

Por otro lado, la importancia del dato también radica en su capacidad para personalizar la experiencia del cliente. Las empresas que utilizan datos para segmentar su mercado y entender las preferencias de sus consumidores pueden ofrecer productos y servicios más ajustados a sus necesidades. Esto no solo mejora la satisfacción del cliente, sino que también fomenta la lealtad y la retención, aspectos cruciales en un mercado cada vez más competitivo. En resumen, **el valor del dato en la actualidad es esencial para que las empresas no solo sobrevivan, sino que prosperen** en un mundo donde la información es poder. Desde Prosegur Research, de acuerdo con nuestro modelo de **seguridad híbrida**, creemos que **los datos se deben analizar con calma y en un contexto específico**, con el uso de tecnologías convergentes y exponenciales orientadas a la obtención y procesamiento de estos, junto con las competencias y conocimientos humanos de los expertos de seguridad, para ofrecer soluciones eficaces en entornos marcados por la incertidumbre, detectando amenazas y oportunidades para las organizaciones.

HOME

2.2.
El imperativo del dato

Siguiendo una lógica inductiva, **se trata de crear respuestas personalizadas tras el filtrado e interpretación del dato en bruto.** Es en este contexto en el que la **maratón analítica del dato** cobra relevancia: se trata de un modelo conceptual que describe el **proceso que las empresas deben seguir para transformar datos en insights accionables**, es decir, en información útil que pueda guiar decisiones estratégicas y operativas. Este enfoque se compone de varias etapas, cada una de las cuales es crucial para garantizar que los datos recopilados se conviertan en acciones efectivas que mejoren el rendimiento empresarial.

El primer paso en esta maratón es la **obtención de datos**, donde las empresas recogen información de diversas fuentes, como transacciones, interacciones con clientes, redes sociales y otros puntos de contacto. Esta fase es fundamental, ya que la calidad y la relevancia de los datos recopilados determinarán el éxito de las etapas posteriores.

Una vez que se han obtenido los datos, el siguiente paso es la **preparación**, que implica limpiar y organizar la información para que sea adecuada para el análisis. Este proceso puede incluir la eliminación de duplicados, la corrección de errores y la estructuración en formatos que faciliten su interpretación.

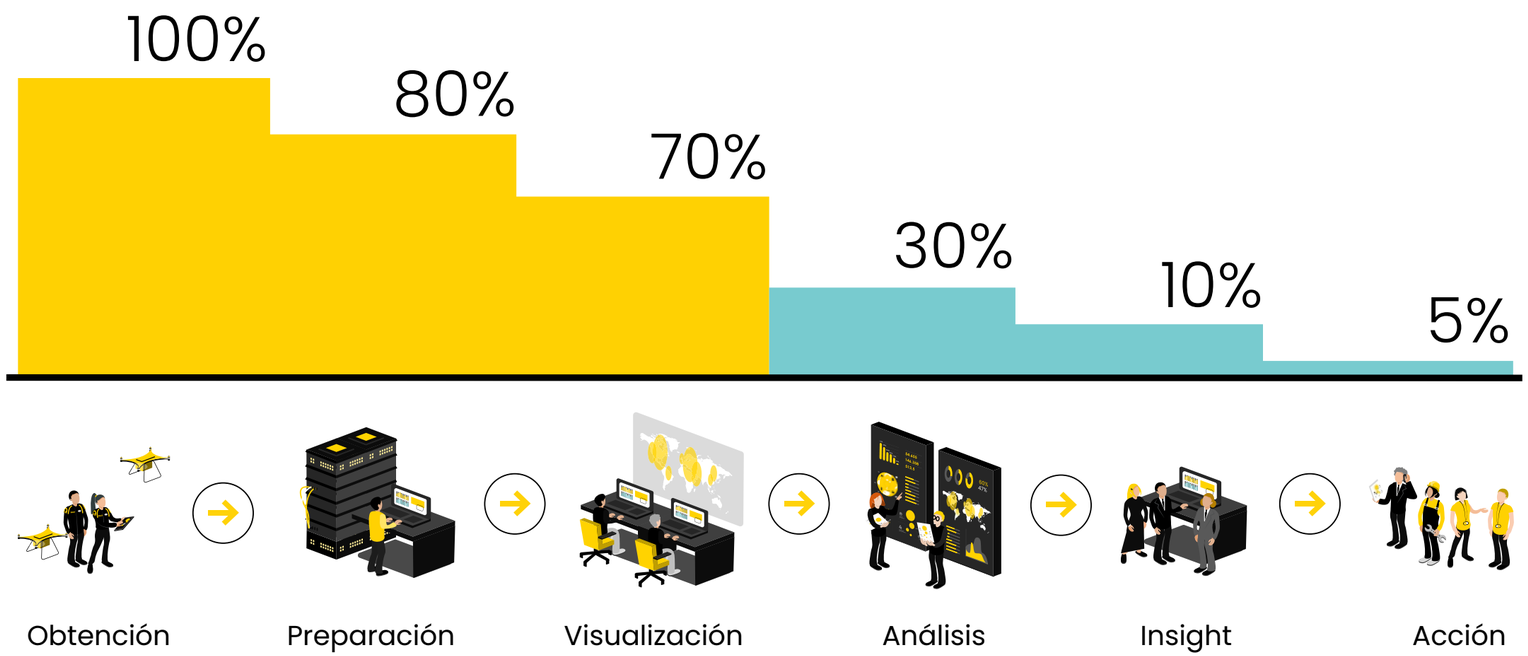
La **visualización** es la etapa siguiente, donde los datos se representan gráficamente para facilitar su comprensión. A través de gráficos, tablas y otros elementos visuales, las empresas pueden identificar patrones y tendencias que podrían no ser evidentes en un formato de datos crudo.

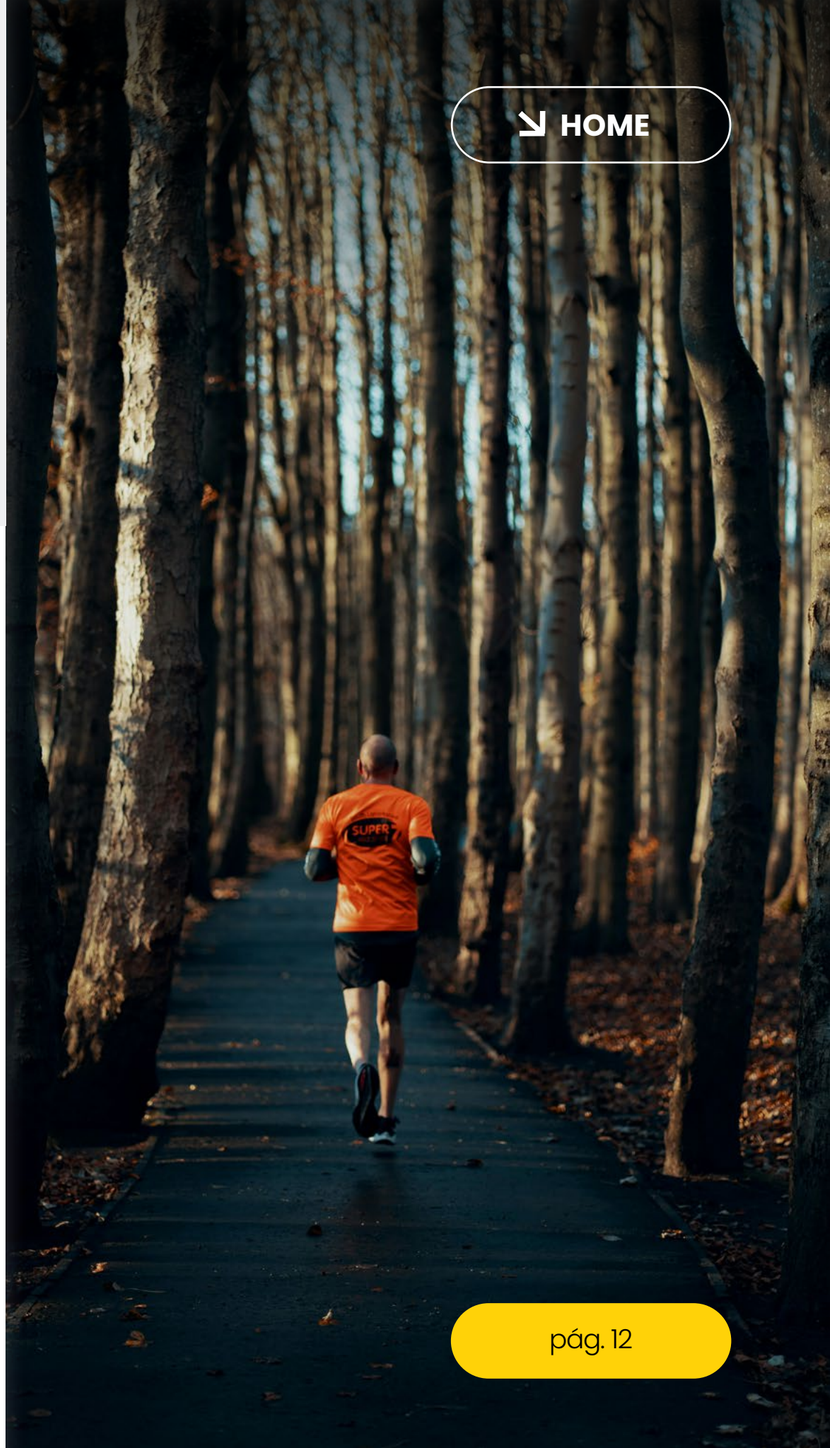
El siguiente hito es el **análisis**, donde se aplican técnicas estadísticas y algoritmos para extraer información significativa de los datos. En esta fase se busca responder preguntas específicas y obtener insights que puedan influir en la toma de decisiones.

Una vez que se han generado insights, el siguiente paso es la **interpretación** o insight, donde se evalúa la relevancia de la información obtenida en el contexto del negocio. Aquí es donde se traduce el análisis en recomendaciones concretas que pueden guiar acciones estratégicas.

Finalmente, la última etapa de la maratón del dato es la **acción**, donde las empresas implementan cambios basados en los insights obtenidos. Esta fase es crítica, ya que muchas organizaciones se quedan en las etapas anteriores y no logran llevar a cabo las acciones necesarias para capitalizar los insights. La capacidad de una empresa para cerrar esta "última milla" y actuar sobre los datos es lo que realmente determina su éxito en un entorno empresarial cada vez más competitivo.

Fuente: Prosegur Research, 2025 basado en Forbes.





HOME

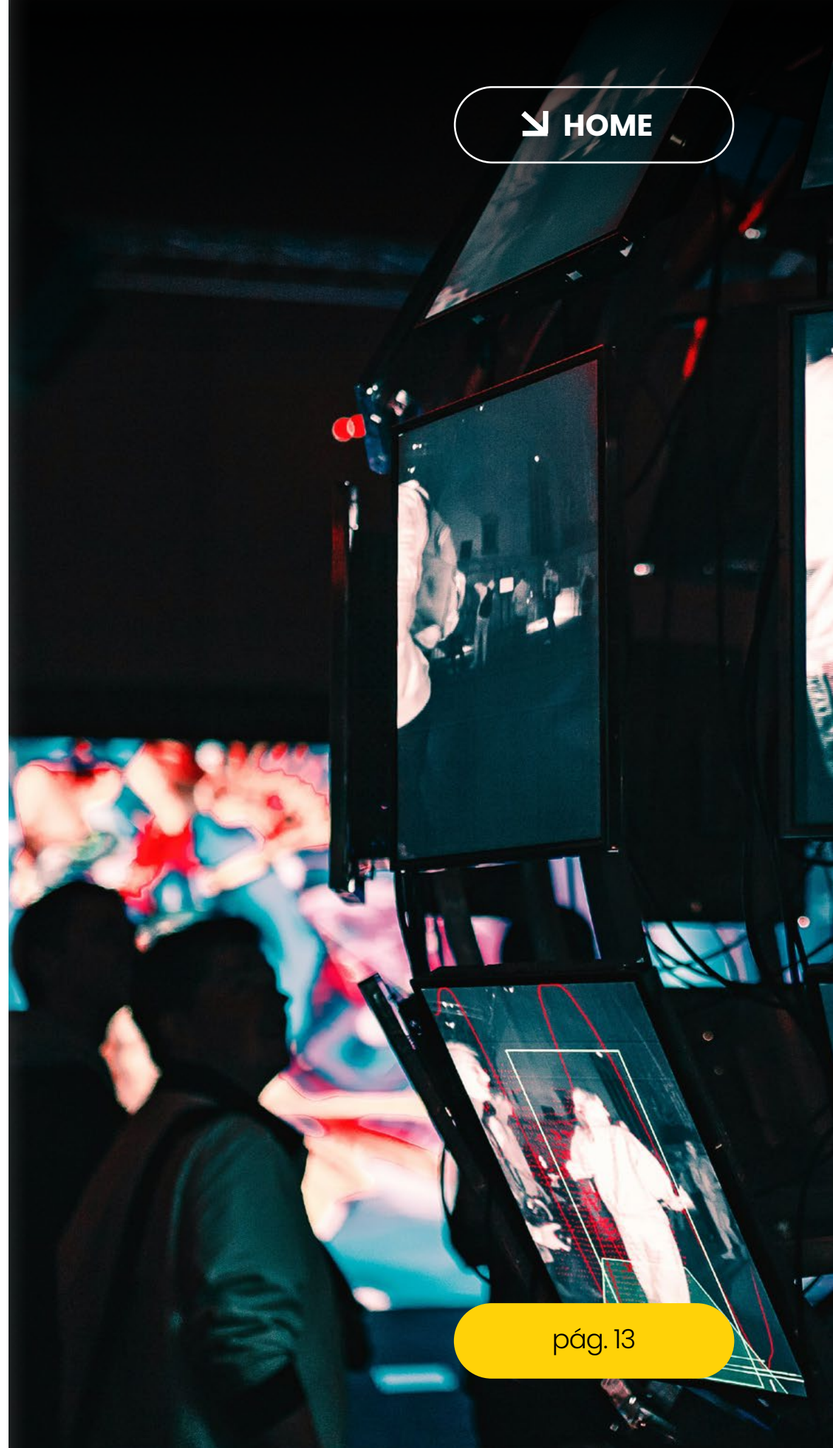
2.3.
El valor del dato en la seguridad híbrida

La **extracción de datos e informaciones procedentes del entorno** puede realizarse a través de tres mecanismos, que se coordinan entre sí: las **fuentes abiertas, fuentes humanas y fuentes tecnológicas.** Los datos son procesados en el iSOC, que a partir del uso combinado de tecnologías y expertos de seguridad se construye una visión integral capaz de producir soluciones de seguridad informadas y eficaces orientadas a la optimización de la toma de decisiones en el sector cliente y el corporativo.

A

Fuentes **abiertas**

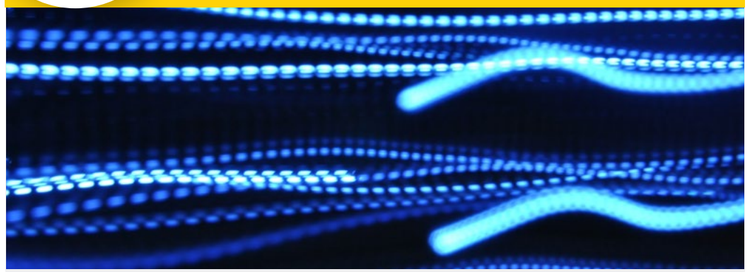
El **desarrollo exponencial de Internet** en las últimas décadas, más accesible y con mayores posibilidades de operabilidad, ha expandido las metodologías tradicionales orientadas a la obtención de datos, aumentando el alcance y proyección de labores de seguridad e inteligencia. La recolección y análisis de información y datos en fuentes abiertas habilita la **actualización en tiempo real de las informaciones,** potencia la **transparencia**, desarrolla capacidad de **alerta temprana** en la detección de señales débiles y es capaz de formular **tendencias prospectivas**, extendiendo el **situational awareness** de la organización. A la hora de analizar datos en fuentes abiertas es necesario advertir el papel que juega el analista, capaz de navegar en un mar informativo y en el **ruido de los datos**, determinando la fiabilidad y validez de estos, así como su interpretación en un contexto dado.



HOME

HOME

B Fuentes **tecnológicas**



La adopción de tecnologías exponenciales y convergentes, como la tecnología del ciberespacio o los drones -un **game changer en los conflictos armados actuales**-, se ha convertido en un aspecto fundamental para producir inputs y outputs de calidad. Su capacidad para **obtener y almacenar datos en tiempo real**, así como su **presencia ubicua en el entorno**, proporciona datos estratégicos con una profundidad y alcance de 360 grados. Estos se transmiten a los **centros de procesamiento** y a los expertos en seguridad con rapidez, eficacia y eficiencia, reduciendo la incertidumbre en la toma de decisiones y mejorando la implementación sobre el terreno.

C Fuentes **humanas**

La lucha contra los **sesgos cognitivos** propios y compartidos y la potenciación de sus capacidades habilita la obtención de información y datos de gran valor por parte de las fuentes humanas, entre las que se encuentran fuerzas y cuerpos de seguridad y los expertos en seguridad. En la obtención de datos, las fuentes humanas son capaces de **interpretar contextos complejos, humanos y culturales**, de acceder a información interpersonal y de adoptar una posición de flexibilidad y resiliencia ante los cambios y disrupciones del entorno en que operan.

Inputs

Fuentes humanas

- FFCCSS
- Vigilante conectado
- Clientes
- Otros expertos

Tecnologías

- Sensores IoT
- Drones
- Robótica
- Alarmas
- Ciberespacio
- CCTV

Fuentes abiertas

- Medios com.
- Redes sociales
- Academia
- Plataformas digitales

Tecnologías

- IA
- GIS
- Data Science
- Social listening
- ML
- Cloud Computing
- Cyber threat
- Social network analysis

iSOC

Expertos en seguridad

- Operadores
- Científicos de datos
- Analistas de inteligencia

Outputs

Clientes

- Informes
- Dashboards
- Acciones de mitigaciones de riesgos
- Alertas
- Recomend.

Corporativo

- Nuevos Productos y Servicios
- Inteligencia competitiva
- Inteligencia empresarial

Fuente: Prosegur Research, 2025.

De todos los datos obtenidos a partir de esta enorme diversidad de fuentes se extrae mediante las tecnologías más innovadoras y los expertos que trabajan en y con el iSOC una aportación de valor extraordinaria en el modelo de seguridad híbrida para la **consecución de outputs de calidad** como alertas anticipatorias, completos informes y nuevos productos y servicios diseñados a partir de las necesidades evolutivas de cada cliente:

1 Detección de amenazas

Los datos permiten identificar patrones y comportamientos anómalos que pueden indicar una amenaza actual o potencial. A través del análisis de grandes volúmenes de datos, los sistemas de seguridad pueden detectar actividades inusuales en tiempo real, lo que facilita una respuesta rápida y efectiva ante incidentes de seguridad por parte de los profesionales responsables.

2 Optimización de recursos

Los datos ayudan a las empresas a asignar recursos de manera más eficiente, indicando las necesidades de las tecnologías y las personas en tiempo real. Al comprender dónde y cuándo ocurren las amenazas, las organizaciones pueden dirigir sus esfuerzos de vigilancia y respuesta a las áreas de mayor riesgo, maximizando la efectividad de sus operaciones de seguridad.

3 Investigación de tecnología y expertos

Los datos son fundamentales para integrar diversas tecnologías y expertos, retroalimentando en tiempo real a los vigilantes, operadores, analistas, ingenieros, etc. Esta integración permite una visión holística de la seguridad, donde los datos de diferentes fuentes se combinan para ofrecer una respuesta más coordinada y efectiva.

4 Personalización de servicios

La recopilación y análisis de datos, cuando estos son de calidad, permiten adaptar los servicios de seguridad a las necesidades específicas de cada cliente, como un traje a medida. Esto incluye la personalización de soluciones de vigilancia, tecnología e inteligencia, lo que resulta en un servicio más relevante y efectivo.

5 Inteligencia para la anticipación

Al analizar datos históricos y en tiempo real las organizaciones pueden anticipar posibles amenazas y vulnerabilidades. La inteligencia permite a las empresas implementar medidas proactivas para mitigar riesgos antes de que se materialicen, mejorando así la resiliencia organizacional y su competitividad en el mercado que opere.

6 Cumplimiento normativo

La gestión de datos en el contexto de la seguridad también ayuda a las organizaciones a cumplir con regulaciones y normativas relacionadas con la protección de datos y la privacidad. Esto es especialmente importante en un entorno donde la transparencia es un valor central para la confianza.

7 Capacitación y concienciación

Los datos también pueden ser utilizados para formar y concienciar a los empleados sobre las mejores prácticas de seguridad, identificando donde se necesita más capacitación y desarrollar programas específicos para abordar estas necesidades.

8 Mejora continua

Los datos proporcionan una base para la evaluación y mejora continua de las estrategias de seguridad. Así, permiten ajustar políticas y procedimientos para abordar mejor las amenazas emergentes, entendiendo la flexibilidad que exige el mundo cambiante.

Pero esto **no se consigue solo por el hecho de contar con una organización que genere datos,** no se debe olvidar lo esencial del factor humano para el uso estratégico de los datos: la cultura del dato, a continuación, explicada.

HOME

03

Cultura del dato: marco de competencias

HOME

01
El océano en la oficina

02
Data momentum

03
Cultura del dato: marco de competencias

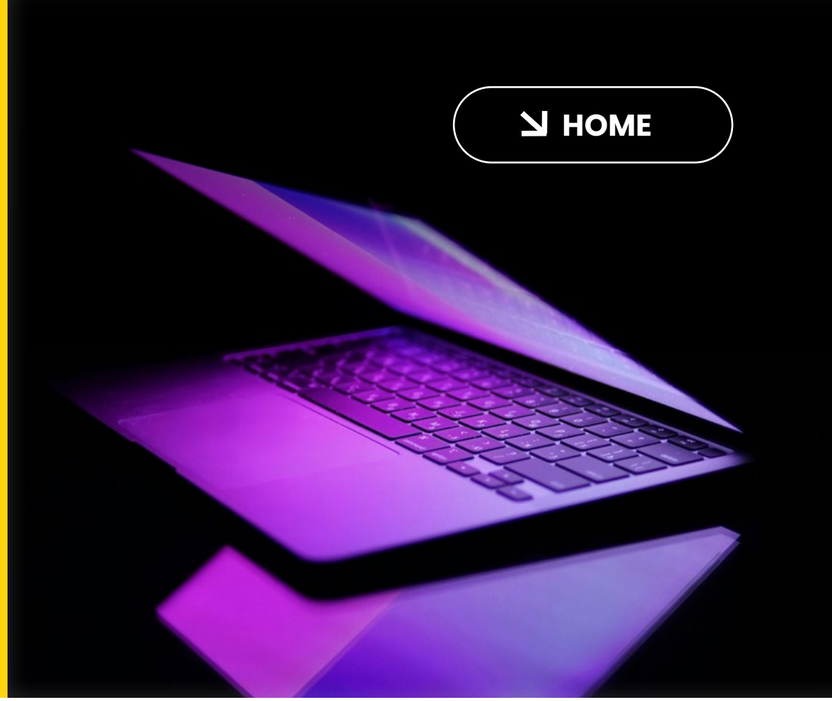
04
Datos para una seguridad híbrida de confianza

CULTURA DEL DATO: MARCO DE COMPETENCIAS

3.1. El desorden de la información

La complejidad y la escala de contaminación de la información en nuestro mundo digitalmente conectado plantea un reto sin precedentes

Claire Wardle, Information disorder. Toward an interdisciplinary framework for research and policy making

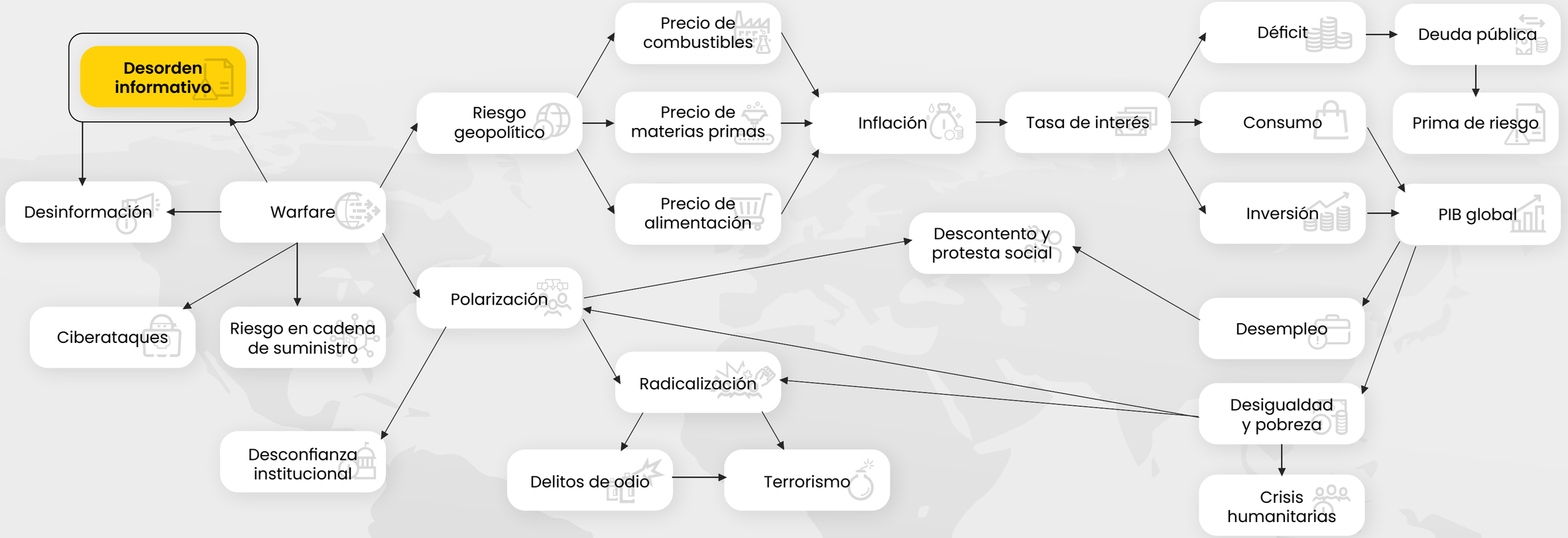


HOME

El entorno actual se caracteriza por el desorden informativo: si bien la información ha sido utilizada desde hace milenios tanto como potenciador del desarrollo humano como un arma, hoy el desarrollo exponencial de la tecnología y la conectividad ha hecho que la mayor facilidad en el acceso, la producción y la distribución -en tiempo y forma- de la información potencie la materialización de fenómenos como las campañas de desinformación -encontrándose en ellas las denominadas **fake news**-, la **posverdad** y la **falsificación de contenido por inteligencia artificial generativa.** También se ha profundizado en la forma de entender los conflictos armados; prueba de ello constituye el énfasis que desde **organizaciones internacionales** y Estados se ha realizado en materias como la **guerra híbrida** y las **amenazas híbridas.**

A pesar de ello, las tecnologías en relación con los datos y la información también poseen un **componente liberador**, pues han **empoderado** a la ciudadanía al habilitar nuevas formas de contestación y expresión de demandas frente a los centros de poder tradicionales, rompiendo las barreras de acceso a estos e incidiendo en el **carácter multipolar** y poder difuso del panorama actual.

Además, en el actual contexto de aplicación de tecnología con fines comerciales, como los **algoritmos de recomendación**, se pueden ver potenciados algunos errores de juicio o sesgos cognitivos, dando lugar a fenómenos como las **cámaras de eco** y las **burbujas de filtro.**



Fuente: Prosegur Research, 2025.

En definitiva, el **ambiente general del desorden informativo afecta a la seguridad**, erosionando la confianza en las instituciones y la democracia, manipulando la opinión pública y generando un potencial impacto negativo para las organizaciones. Además, posee **implicaciones en la seguridad personal**, potenciando las estafas y la radicalización de los individuos a través de la publicación de contenidos desinformativos o erróneos.

EN FOCO:
EL USO MALICIOSO DE LOS DATOS EN EL SENO EMPRESARIAL

El desorden informativo se extiende hacia el sector empresarial, materializándose en la **apropiación indebida de datos y la manipulación de información** desde la perspectiva del ***empoderamiento*** del empleado, con un progresivo acceso a los datos y una incremental dificultad de control por parte de las organizaciones. En un contexto de permacrisis y poder difuso, el ***fraude interno*** sacude a multitud de empresas y ***ninguna entidad está exenta de la comisión de este tipo de delitos.***

HOME

3.2.
La necesidad del componente humano

Cómo responder ante la era del desorden de la información no es una tarea sencilla, pues los retos que afrontar son complejos. Para ello, es necesario comprender la realidad -las personas y las cosas que en ella habitan- y apoyarse en los desarrollos tecnológicos, capaces de dirigirnos hacia un futuro más seguro.

> Los datos no hablan por sí mismos, [sino que] se necesitan interrogadores inteligentes
>
> ***Luciano Floridi, en Menos tech y más Platón***

Parte de ese avance actualmente se focaliza en la **alfabetización digital**, con el objetivo de operar en un entorno de información abundante y potencialmente contaminada. La alfabetización digital ayuda a comprender que la información y los datos poseen significados y valores impregnados en ellos, y que no son realidades inmutables. En otras palabras: **los datos no hablan por sí mismos.** Es necesaria la formación de **profesionales críticos** capaces de interrogar los datos disponibles, aportando valor cualitativo y contextual. **Michael Li**, fundador y presidente de The Data Incubator, va un paso más allá cuando explica que antes de que las empresas puedan monetizar los datos primero deben entenderlos. **Ser alfabetizado en datos es un imperativo competitivo** y lo es tanto para las empresas como para sus empleados.

En el contexto del desorden de información, y como conjunto de competencias personales y estructurales, la alfabetización actual lucha **contra la incredulidad y la desconfianza** al desarrollar la **capacidad crítica** de los expertos y ciudadanos, dominando las herramientas digitales para comprender significados y mensajes en los datos y la información.

3.3.

Las competencias del dato en la seguridad híbrida

En el marco conceptual de la **seguridad híbrida**, y en relación con los datos, se han determinado **cuatro tipos de competencias**, conformando un **enfoque sistémico**, pues cada categoría constituye un complemento del resto. Las competencias se ubican de forma transversal en el nivel organizacional y en el nivel humano.

A Competencias **en seguridad**

En **entornos de incertidumbre y de desorden informativo**, los profesionales deben adquirir y potenciar competencias de carácter político, económico, social y del entorno, con orientación a la gestión del riesgo que la información y los datos poseen. Por ejemplo, el **conocimiento en los requerimientos de seguridad físicos** de una infraestructura determinada ayuda a determinar las necesidades del servicio, analizando datos históricos sobre intrusiones hacia la misma.

Adicionalmente, el **conocimiento legal, normativo y sobre las mejores prácticas** empresariales garantiza una gestión óptima de los servicios operativos. La ISO31030 es un ejemplo de ello, sobre la gestión del riesgo en los viajes y desplazamientos. En el contexto actual en el que el **ámbito digital** cuenta con un gran protagonismo, las competencias en la materia, aplicadas a la seguridad, se configuran como esenciales para mantener la continuidad de negocio. A modo de ejemplo, se destaca la recolección de imágenes por parte de fuentes tecnológicas, como los drones, de acuerdo con la normativa vigente.

Asimismo, la **actualización periódica de protocolos de seguridad,** como las actuaciones en caso de amenazas de bomba, minimiza parcialmente los riesgos a los que se enfrentan los clientes o usuarios.

Por último, dada la diversidad de fuentes existente -noticias, reporteros, informes, think tanks, redes sociales, etc.-, los profesionales de la seguridad híbrida deben aprender a **manejar, gestionar y utilizar adecuadamente una correcta base de conocimiento.** En este sentido, la **detección de alertas tempranas** sobre incidentes de seguridad ayuda a prevenir riesgos que puedan afectar a las organizaciones; por ejemplo, la identificación de disturbios sociales que puedan afectar a la cadena de suministros en puntos críticos o estratégicos, como los puertos marítimos de elevada actividad comercial, puede ayudar a reajustar en el momento oportuno la planificación estratégica de las corporaciones potencialmente afectadas.

B Competencias **digitales**

Las competencias digitales aseguran el manejo óptimo de aquellas herramientas de recolección, procesamiento y análisis de multitud de fuentes de datos -cámaras de videovigilancia, drones, robótica, etc.-.

En primer lugar, se destaca el **diseño, implementación y uso de tecnologías para la obtención de información y datos.** Los ciclos tecnológicos acelerados –la presentación constante de nuevas herramientas y funcionalidades-, junto con la obsolescencia, requiere que los profesionales se adapten constantemente a las nuevas herramientas. La implementación de los drones en los servicios de vigilancia perimetral no ha sustituido al vigilante conectado, sino que ha creado la necesidad de contar con profesionales con mayores conocimientos específicos en su uso y manipulación. Además, estos dispositivos aportan información valiosa complementaria, como las imágenes aéreas o el acceso a lugares remotos.

Por otra parte, el desarrollo tecnológico crea nuevas oportunidades de negocio y, consecuentemente, **nuevos nichos de crecimiento profesional.** El uso ya tradicional de vehículos terrestres o la reciente incorporación de motos de agua a los servicios de vigilancia portuaria son ejemplos de ello, requiriendo profesionales que sepan utilizarlos de manera eficiente.

En segundo lugar, es relevante el ejercicio de **competencias ligadas al *know-how* tecnológico y digital.** Las organizaciones deben estar al tanto de las **últimas tendencias tecnológicas** y estudiar su integración en la línea de negocio, advirtiendo su evolución y expectativas contando con modelos como el **ciclo del hype de Gartner** o los **tres horizontes de crecimiento e innovación.** Al respecto, algunas de las últimas tendencias más relevantes con impactos en el sector de la seguridad se vinculan con las plataformas inteligentes reconfigurables o el computer vision para el análisis de imágenes.

Por tanto, los equipos multidisciplinares de expertos deben operar con herramientas tecnológicas, tanto básicas como avanzadas. En este escenario, la **alfabetización digital y de datos** por parte de los profesionales se consolida como una habilidad necesaria y ampliamente demandada, desarrollando competencias orientadas al uso efectivo de las tecnologías adoptadas en el espacio de trabajo.

HOME

pág. 24

C Competencias **humanas**

Son competencias eminentemente propias de los seres humanos, basadas en un aspecto cualitativo, o *soft skills.* **Los datos por sí mismos no tienen significado, por lo que son fundamentales las aptitudes de los expertos en seguridad**, como la resolución de problemas complejos y la creatividad -**pensar fuera de la caja**-, para aportar un verdadero valor añadido a las informaciones y para no caer en errores de aproximación, como la **falacia de McNamara.**

Con el gran volumen de datos que manejan las organizaciones en la actualidad, el **pensamiento crítico y el análisis de información** resulta uno de los aspectos más relevantes para el manejo del dato y avanzar en la maratón hacia la última milla. De este modo, la habilidad para identificar patrones y relaciones, así como evaluar su impacto, entre datos que afecten a la operativa de negocio de los clientes es una de las principales competencias demandadas. Por ejemplo, una incidencia de seguridad, como un hurto, en un punto concreto no indica necesariamente que exista un problema. Sin embargo, la identificación de modus operandi similares en diferentes puntos geográficos en un corto periodo de tiempo puede requerir el despliegue de medidas de mitigación y prevención.

Asimismo, la capacidad para **desagregar informaciones** de distinta procedencia para después integrarlas bajo un mismo significado constituye una aptitud necesaria para trabajar en entornos dinámicos, adecuándose en el contexto general de los datos recombinantes en seguridad híbrida.

Por otra parte, la **responsabilidad** es fundamental para comprender y manejar las implicaciones éticas del manejo de datos. La **integridad y la confidencialidad** para garantizar la privacidad, el buen trato con el cliente, las mejores prácticas de gobernanza y los límites establecidos por la ley solo lo pueden llevar a cabo los mejores empleados formados en la materia. Entre los ejemplos aplicados a las competencias se señala el respeto a la privacidad en caso de revisión de grabaciones por parte de operadores de zonas residenciales.

HOME

HOME

D Competencias **de autogestión**

La obtención y el tratamiento de datos puede resultar un proceso complejo, pues la información se encuentra desordenada, contaminada y en grandes volúmenes en el entorno informativo. Con el objetivo de poder navegar de forma eficaz en entornos cambiantes y desafiantes desde un punto de vista emocional, los expertos deben desarrollar actitudes que resultan un valor añadido en el modelo de seguridad híbrida. Algunas de ellas son la resiliencia ante las disrupciones del entorno -por ejemplo, en la actualización constante de los datos en fuentes abiertas-; la **tolerancia a la frustración** en el acceso a la información, que puede estar incompleta, alterada o eliminada; o la **flexibilidad** al tratar con grandes volúmenes de datos complejos y desordenados.

En la operativa diaria, el tiempo, en ocasiones, juega en contra de los profesionales de la seguridad. La **inmediatez** requerida en situaciones de riesgo deriva en la necesidad de contar con profesionales con sepan priorizar y mantener la calma. Por ejemplo, en situaciones de crisis, como un contexto violento en una disrupción social, requiere que los trabajadores aseguren una respuesta rápida y eficiente.

Así, en la adquisición y potenciación de estas competencias es de gran ayuda el **aprendizaje activo** y en conjunto al trabajar en **equipos multidisciplinares**, cuyos miembros son capaces de aportar visiones diferenciadas pero complementarias acerca de los datos obtenidos y sus implicaciones en la seguridad y las líneas de negocio.

En conclusión, la cultura del dato en las empresas es fundamental por diversas razones que impactan directamente en su capacidad para competir y adaptarse en un entorno empresarial en constante cambio. En primer lugar, **una cultura del dato fomenta la toma de decisiones informadas:** cuando los empleados en todos los niveles de la organización valoran y utilizan datos en su trabajo diario, se reduce la dependencia de suposiciones, lo que a su vez minimiza el riesgo de errores y sesgos, y si los datos son de calidad y adecuadamente contextualizados, **mejora la precisión** en la planificación y ejecución de estrategias.

Además, una sólida cultura del dato promueve la **colaboración y la transparencia** dentro de la organización: al compartir datos y análisis entre departamentos se facilita un enfoque más integrado y cohesivo para abordar problemas y oportunidades. Esto no solo mejora la comunicación, sino que también permite a los equipos trabajar juntos de manera más efectiva, aprovechando diferentes perspectivas y conocimientos para generar soluciones más flexibles y adaptadas al cliente, con la visión de Security-as-a-service.

La cultura del dato también **impulsa la innovación**, de forma que cuando los empleados se sienten empoderados para explorar y experimentar con datos, pueden identificar nuevas oportunidades de negocio, optimizar procesos existentes y desarrollar productos o servicios que respondan mejor a las necesidades del mercado. Esta **mentalidad proactiva** es esencial para que las empresas se mantengan relevantes y competitivas en un mundo donde la tecnología y las expectativas de los consumidores están en constante evolución.

Por otro lado, la cultura del dato contribuye a la **agilidad organizacional**, en un entorno empresarial caracterizado por la incertidumbre y el cambio rápido, las empresas que adoptan una mentalidad basada en datos pueden adaptarse más rápidamente a nuevas circunstancias. La capacidad de analizar datos en tiempo real permite a las organizaciones responder de manera más efectiva a las tendencias del mercado, a las necesidades de los clientes y a los desafíos emergentes.

Finalmente, fomentar una cultura del dato también ayuda a las empresas a desarrollar una **mayor confianza en sus decisiones** conscientes de la priorización de las personas a lo largo de todo el modelo de seguridad híbrida. Cuando los empleados ven que las decisiones se basan en datos concretos y análisis rigurosos se genera un sentido de seguridad y legitimidad en las acciones tomadas; esto no solo mejora la motivación y en consecuencia el desempeño del equipo, sino que también fortalece la reputación de la empresa ante sus clientes y socios.

El dato cobra valor cuando evoluciona en un **ecosistema adecuado**, cuando es susceptible de ser correlacionado con determinadas temáticas de interés. Por lo tanto, la cantidad, calidad e integración de los datos determinarán su valor.

Su aprovechamiento estratégico deriva de la integración de todas estas fuentes trabajadas por los mejores expertos en seguridad y las más innovadoras tecnologías aplicadas. Desde el iSOC los datos se emplean para dar respuesta inmediata operativa y estratégica, desde el modelo de seguridad híbrida son transformados en inteligencia, que permite anticipar y mitigar riesgos, aprovechando la experiencia para generar un procesamiento de alto nivel de complejidad. Así, nos lleva a **la acción presente y futura, gestionando la incertidumbre** y adelantándonos a los desafíos de seguridad.

Esta es la clave del cambio de paradigma de seguridad que vivimos: la convergencia tecnológica y el uso inteligente de los datos en el ***iSOC*** nos permiten anticipar los cambios, **acompañando al mundo en su trasformación.**

Funciones y elementos centrales del SOC

Fuente: Prosegur Research, 2025.

HOME

04

Datos para una **seguridad de confianza**

04 DATOS PARA UNA SEGURIDAD DE CONFIANZA

Vivimos en una era donde **la generación de datos es incesante** y están transformando nuestro mundo de maneras profundas, alterando no solo nuestras sociedades, sino también nuestra propia naturaleza como seres humanos. Si miramos hacia el pasado, podemos encontrar paralelismos interesantes con **la forma en que la tecnología y la información han sido recibidas y comprendidas** a lo largo de la historia. A principios del siglo XX, algunos expertos creían que el teléfono, al eliminar la necesidad de contacto personal, podría llevar al aislamiento social. Incluso mucho antes, en 1818, la novela Frankenstein de Mary Shelley nos advertía sobre los peligros de utilizar la tecnología para jugar a ser Dios, desdibujando las líneas entre lo humano y lo no humano.

Y si retrocedemos aún más, encontramos en el *Fedro* de Platón, alrededor del 370 a. C., una reflexión de Sócrates sobre la escritura, sugiriendo que esta podría ser perjudicial para la memoria humana, ya que, una vez escrito algo, ya no sentiríamos la necesidad de recordarlo. Estas preocupaciones históricas nos invitan a reflexionar sobre las competencias que necesitaremos en el presente y el futuro cercanos.

En este contexto, **la conexión es crucial para la integración**, necesitando modelos de comprensión del mundo como es la seguridad híbrida y el iSOC, cerebro del mismo, que están profundamente vinculado a la cultura del dato. Esta cultura exige una comprensión compartida y un **compromiso colectivo** para aprovechar al máximo el poder de los datos, sin caer en la trampa de la parálisis por análisis.

HOME

En nuestro caso, Prosegur Security trabaja con más de un millón de dispositivos conectados, y más de **160.000 expertos que gestionan de forma estratégica más de 1.5 millones de eventos y datos de seguridad al año.**

La sobrecarga de datos puede ser paralizante, pero esta realidad también nos convoca a la acción. Para superar esta parálisis, todos debemos contribuir activamente, la colaboración y la cooperación es lo que promueve la civilización del mundo, como dice Luis Klein con su famosa frase **"cuanto más avanza la integración, mayor es el beneficio común."**

En Prosegur Research sabemos que esto implica generar **confianza entre las personas, tener la determinación de impulsar cambios y colaborar para integrar** diferentes perspectivas y conocimientos. Todo esto se logra cuando existe coherencia en los proyectos e ideas, y cuando todos *hablamos el mismo idioma,* es decir, compartimos términos y definiciones comunes y consensuadas, lo que requiere además de reflexión mucho diálogo, esto es, contexto adecuado y contacto de calidad, con ello logramos una **integración inteligente** que nos permita hacer del mundo un lugar más seguro.

PROSEGUR
SECURITY

Garantizamos la seguridad de las personas,
las empresas y la sociedad en su conjunto.

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com