PROSEGUR RESEARCH

Seguridad Híbrida

PROSEGUR

Índice | Seguridad Híbrida

Los libros en los que nos hemos basado para construir este modelo

Este documento es interactivo

El mundo en cambio

De la actual incertidumbre
A las 7 claves de futuro

El mundo en cambio

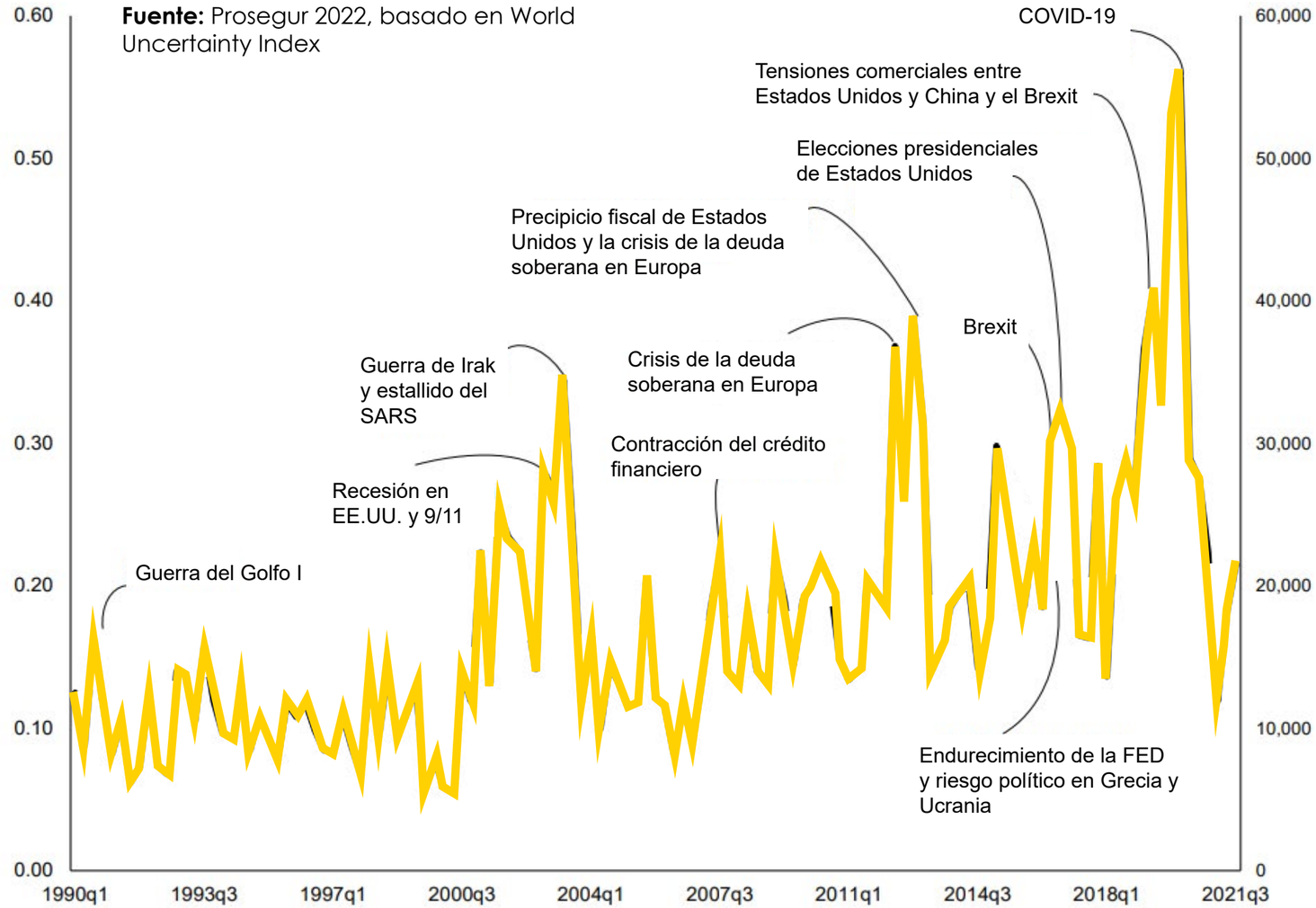
1.1. De la actual incertidumbre

Como señaló el ensayista y poeta francés, Paul Valery, **el futuro ya no es lo que era.** Con cada acción presente se abren nuevas alternativas y escenarios, pues el futuro se va construyendo; y si no se hace con estrategia, las olas en la playa pueden convertirse en auténticos tsunamis.

La desaparición de sectores económicos completos, las personas cambiando de trabajo en masa (Great Resignation), la obsolescencia del conocimiento y la exponencial reducción de tiempo en los ciclos de vida de bienes y servicios son ejemplos de cambio invadiendo nuestro presente y acercando el futuro con rapidez.

Índice de incertidumbre mundial

Fuente: Prosegur 2022, basado en World Uncertainty Index



El mundo en cambio

1.1. De la actual incertidumbre

1 

Ransomware

2 

Disrupciones de extremismos políticos

3 

Pandemias y crisis sanitarias

4 

Eventos climáticos extremos

5 

Crisis en la cadena de suministros

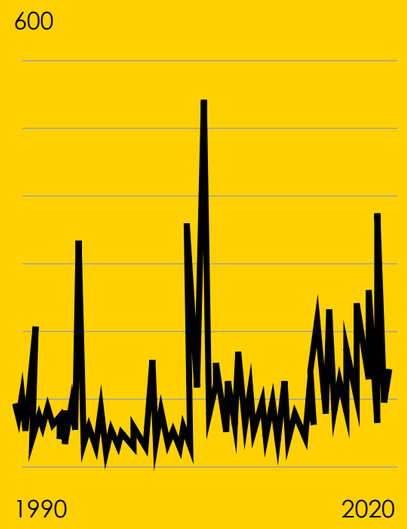
6 

Conflictos geopolíticos de alto impacto

Paralelamente una serie de eventos extremos están desestabilizando el mundo: los ciberataques masivos de ransomware, extremismos, afectaciones críticas a la cadena de suministros, eventos climáticos extremos, pandemias y conflictos como el de Ucrania nos sitúan en un entorno donde la constante es el cambio.

Los índices de incertidumbre están en niveles máximos, y desconocemos del todo las amenazas, y cómo, cuándo y dónde se van a materializar en la próxima ocasión.

Junta de la Reserva Federal, Índice de Riesgo Geopolítico



Empresas sujetas a una cibervulneración al año, %

Desastres naturales por año, número

Fuente: Prosegur 2022, basado en Mckinsey, 2021

El mundo en cambio

1.2. A las 7 claves de futuro

En este contexto, Prosegur propone estudiar las tendencias del mundo a través de 7 claves de futuro que permiten ordenar el análisis y la monitorización de estos cambios. Es fundamental estudiar e interpretar los hechos y los datos en el momento actual, considerado el interregno: nos encontramos continuamente nuevas tendencias mientras no terminan de morir las viejas, algunas desaparecen y otras incluso se recuperan con más fuerza que en tiempos atrás. Nos ubicamos en un periodo de latencia donde las tendencias transforman ágilmente nuestro mundo: reestructurando sociedad, reconfigurando espacios políticos, incluso haciendo aparecer o desaparecer sectores económicos completos. Es precisamente **en este caótico interregno donde surgen las oportunidades:** frente a las rivalidades, las emergencias, los vacíos de poder y las crisis, comprender las transformaciones nos permite un enfoque nuevo, bajo el que personas, estados y empresas pueden renovarse por completo. En el sector de la seguridad, entender lo que ocurre en el mundo se vuelve un asunto crítico, y transformarse en conjunción con la sociedad no es optativo: solo formando parte del cambio podremos adaptarnos a las nuevas necesidades de personas y empresas.

En el documento ***7 claves de futuro*** se detalla esta tendencia hacia la incertidumbre de la denominada “nueva normalidad”. Así, no podemos llegar a conocer con total exactitud la naturaleza de las amenazas, ni dónde, cuándo o cómo se podrán materializar. La situación de Ucrania supone un ejemplo como conflicto de poder difuso, con los múltiples impactos que ha tenido - y seguirá teniendo - en materia de seguridad, económica, política y social, entre otras. Además, nuevos riesgos ecológicos como lo fue el inicio de la COVID-19 en el año 2020 impactan de manera directa en otras áreas como el empowerment, priorizando el bienestar y el individualismo frente a otras corrientes como el colectivismo. Unido, además, a la creciente inflación y dificultades económicas que se están produciendo a nivel global, la polarización social se postula como una de las principales variables para el mantenimiento de la estabilidad estatal, con otros efectos como la ***desinformación y el desorden de la información.***

Fuente: Prosegur, 2022

La seguridad evoluciona con la sociedad

Ampliando los campos que abarca

Enfrentando amenazas híbridas

Desafiando riesgos sistémicos

02

La seguridad evoluciona con la sociedad

2.1. Ampliando los campos que abarca

La seguridad está evolucionando junto la sociedad en un **contexto de grandes cambios[1].** La creciente incertidumbre nos sitúa en un entorno de enormes desafíos para particulares y empresas[2], y lógicamente vemos como los riesgos tradicionales también evolucionan.

Así, los nuevos riesgos convierten a la **seguridad** en un **concepto evolutivo** y **cada vez más amplio.**

Así, por ejemplo, se incorporan en la gestión de la seguridad

- Ataques a la cadena de suministros que afecten a la continuidad de negocio
- Ciberataques que afecten a la reputación corporativa
- Ataques a infraestructuras críticas o sensibles
- Inteligencia para operar en zonas geográficas y sectores económicos
- Robo de datos e información que afecten a la propiedad industrial

El concepto de seguridad ha amplificado sus horizontes en la medida en que los Estados de bienestar se han desarrollado y los ciudadanos han accedido a mayores niveles de bienestar. Tener cubiertas, en la medida posible, necesidades de carácter primario lleva **a incrementar los niveles de exigencia y demanda de seguridad en áreas tradicionales y emergentes.**

De una seguridad centrada en la protección de personas y activos o bienes, se ha pasado a cubrir áreas como la seguridad económica, medioambiental, alimentaria, legal, de datos, de la información o la tecnológica.

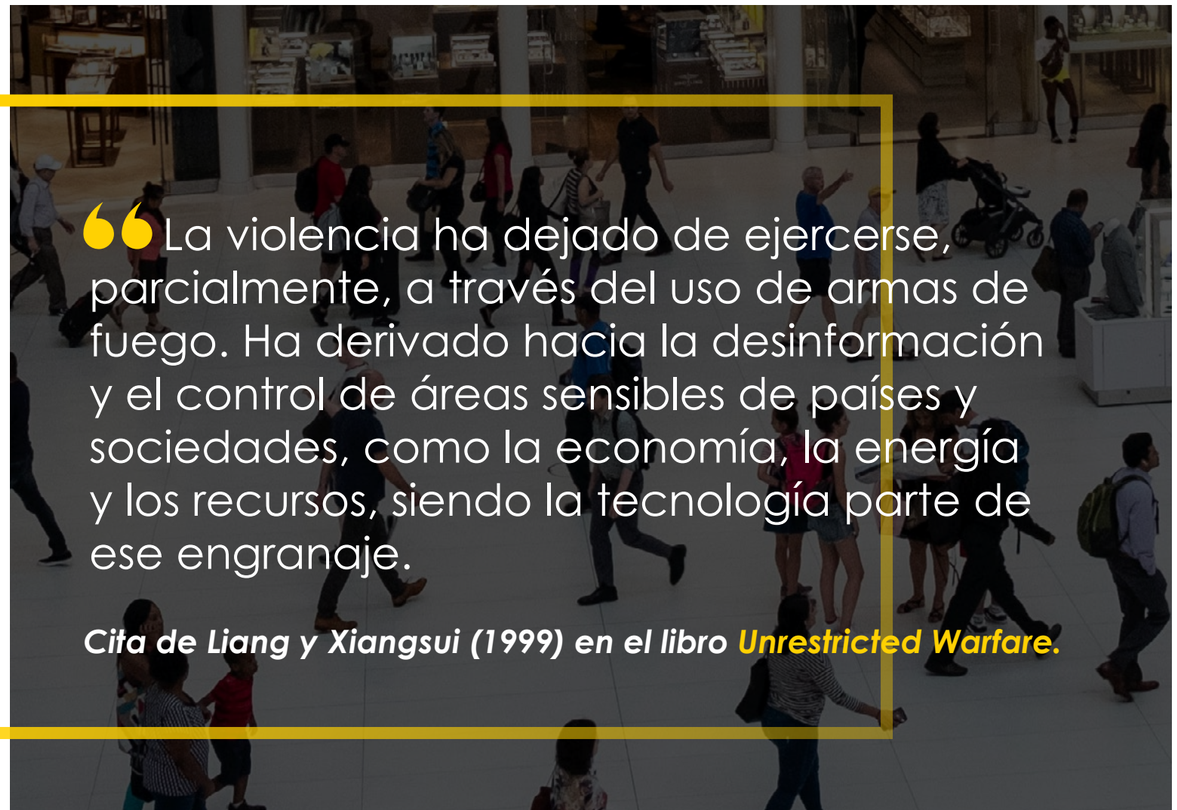
El daño a las sociedades y las empresas no sólo se manifiesta a través de la violencia física directa, que sigue existiendo sin lugar a dudas. Surgen **nuevos riesgos** cada vez más difusos, inesperados y disruptivos, frecuentemente con un claro componente tecnológico[3].

[1] Lo que sociológicamente se ha llegado a denominar ***Modernidad líquida.***
[2] A modo de ejemplo, se puede citar el ***Manual para vivir en la era de la incertidumbre.***
[3] Una lectura de interés sobre el tema es ***The future goes faster than you think.***

La seguridad evoluciona con la sociedad

2.2. Enfrentando amenazas híbridas

La seguridad del mundo actual debe ser capaz de anticipar esos riesgos[4] de una forma inteligente y ágil, teniendo en cuenta la importante diversidad de amenazas desde distintos ámbitos, en ocasiones fruto de la hibridación de distintos entornos y actores. Esto implica trabajar la **prospectiva corporativa,** adquiriendo habilidades y capacidades para detectar los patrones de cambio (acelerado exponencialmente, discontinuo e interdependiente), interpretar los impactos en la organización y proponer cursos de acción a largo plazo.



> “La violencia ha dejado de ejercerse, parcialmente, a través del uso de armas de fuego. Ha derivado hacia la desinformación y el control de áreas sensibles de países y sociedades, como la economía, la energía y los recursos, siendo la tecnología parte de ese engranaje.
>
> ***Cita de Liang y Xiangsui (1999) en el libro Unrestricted Warfare.***

Por ello, debemos ser conscientes de que nos enfrentamos a las **amenazas híbridas.** El uso de drones por parte de organizaciones criminales y terroristas, el empleo de armas 3D para ataques extremistas, el crowdsourcing criminal mediante robos masivos de tarjetas de crédito, el empleo de un Centro de Operaciones de Seguridad (SOC, por sus siglas en inglés) para un ataque terrrorista ponen de manifiesto que esta hibridación ya es una realidad.

Por último, transversalmente la tecnología empodera todo tipo de procesos y conductas, dando lugar al surgimiento de nuevas herramientas como las impresoras 3D y, consecuentemente, nuevas oportunidades para el crimen, como el atentado producido en Halle (Alemania) en 2019.

En esta era digital, donde las tecnologías son las claras protagonistas[5] del crecimiento y en la que se ha demostrado que su desarrollo es más rápido del que cabría esperar, presentando así una gran exponencialidad acelerada[6], se requiere un **mindset de crecimiento** asumiendo la no-linealidad[7]: solo las personas que aprendan a aprovechar los cambios y a impulsarse gracias al desarrollo tecnológico marcarán esa diferencia.

---

[4] La importancia de anticipar estos cambios se desprende del libro ***Corporate Foresight.***
[5] Tal y como se explica en ***The Digital Future.***
[6] Se recomienda la lectura ***Exponential.***
[7] Para profundizar más, se puede reflexionar con ***Mil años de historia no lineal.***

La seguridad evoluciona con la sociedad

2.3. Desafiando riesgos sistémicos

Esta era tecnológica caracterizada por los cambios disruptivos y frecuentes implica necesariamente un esfuerzo en conocer todos los actores y fuerzas que dirigen el cambio, alejándonos del clásico presentismo que sobrevalora la relevancia de los factores actuales en los cálculos futuros. Ya no se trata únicamente de los componentes financieros, sino que se deben tener en cuenta, además, los factores sociales, medioambientales[8], políticos, geoeconómicos[9] y tecnológicos, entre otros, tanto a corto, medio y largo plazo.

Todo lo mencionado hace destacar el concepto de **riesgo sistémico:** cualquier circunstancia, en cualquier lugar, es susceptible de generar impactos en cascada en naciones, industrias y sectores. Un conflicto como el de Ucrania afecta a la actividad de las empresas, a las previsiones globales de crecimiento, a aumentar la inflación mundial, produce una crisis alimentaria susceptible de derivar en descontento social y nuevas “primaveras” (manifestaciones, huelgas, etc.), genera oportunidades para nuevas formas de criminalidad, etc.

Ello redunda en la necesidad de situar el foco en la **inteligencia contextual,** es decir, pivotar de una gestión de riesgos a una inteligencia de riesgos, ya que cualquier hecho, independientemente del lugar en el que se produzca, es susceptible de generar nuevas oportunidades para las sociedades, los gobiernos y, por supuesto, las redes criminales.

02

[8] Como podemos identificar entre los riesgos más destacados según el ***WEF (2022)***.
[9] Para profundizar, se recomienda leer ***The Fat Tail.***

Nuestra visión: Seguridad Híbrida

El modelo de personas, datos y tecnologías

El iSOC como cerebro

La base: organización con propósito y cultura

3.1. Nuestro modelo de seguridad para un mundo híbrido

Fuente: Prosegur, 2022

En este mundo cambiante de amenazas híbridas y reconfiguración de los parámetros de seguridad **nace el término que Prosegur acuña como Seguridad Híbrida,** para dar soluciones de seguridad “as a service”:

- Que **se adaptan continuamente** a cada cliente y su entorno.
- Ejecutadas por **expertos profesionales** con la **tecnología** más **innovadora.**
- Potenciadas por un **modelo global de datos e inteligencia.**
- Que permite **anticipar y mitigar riesgos** respondiendo de la forma más **eficiente.**
- Que agrega **un valor diferencial** al negocio del cliente.

Por todo ello, Prosegur propone el modelo que da respuesta a la seguridad híbrida, en el que las **personas expertas en seguridad son empoderadas mediante tecnologías eficientes y conectadas que aprovechan los datos de forma inteligente;** todo esto solo es posible con la base adecuada: una organización con propósito y cultura, capaz de alinear estos tres elementos esenciales, mediante un SOC Inteligente o iSOC.

El iSOC es el cerebro desde el cual se activan los procesos que interrelacionan personas, tecnologías y datos permitiendo la toma de decisiones, eficiente y ágil, que responda a los cambios disruptivos del mundo actual.

Nuestra visión

3.1.1. Las personas como prioridad

Lo verdaderamente clave radica en la perfecta alineación entre los recursos humanos[10], dotados de experiencia y conocimiento, los medios tecnológicos y los datos, que se organizan con el propósito común de proteger de forma más individualizada a las personas y los negocios.

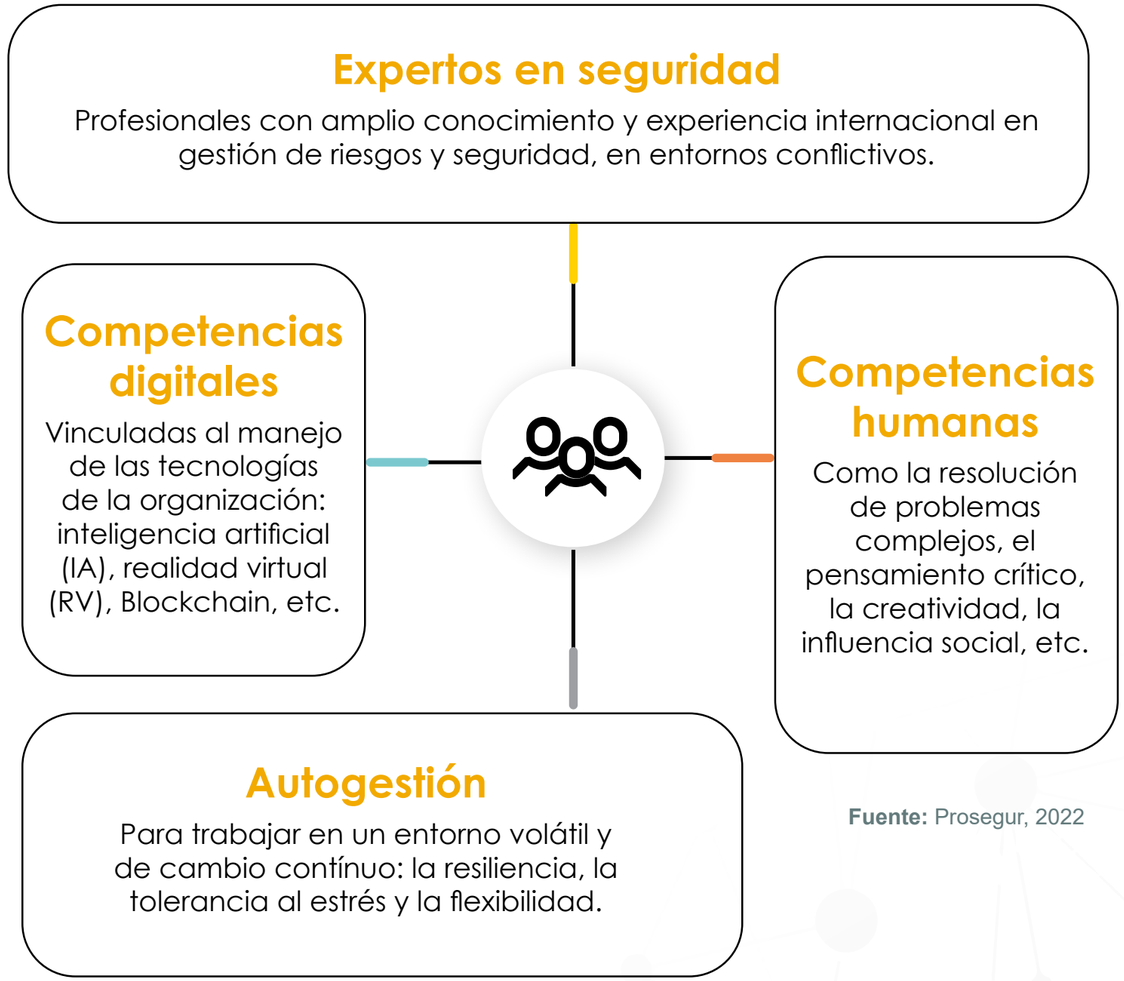
En este sentido, si bien la tecnología es la palanca de cambio, el **factor humano es la esencia del éxito de la seguridad híbrida,** gracias a aptitudes como el pensamiento crítico o la flexibilidad. Tanto su expertise como sus competencias humanas son insustituibles, pues una empresa con la mejor tecnología, pero sin personas expertas en seguridad sería incapaz adaptarse a los vertiginosos ritmos de cambio que generan riesgos actuales[11].

Su aportación en términos de inteligencia contextual nos permite entender el entorno y su inteligencia transformativa aporta capacidad de innovación al modelo completo; estos aspectos son fundamentales desde una perspectiva estratégica.

Eso es lo que la organización busca: empoderar personas con las tecnologías disruptivas. Estos profesionales deben ser expertos en seguridad, además de contar con soft skills humanas, especialmente la capacidad de autogestión, y hard skills vinculadas a competencias digitales.

[10] Una reflexión más profunda sobre el futuro del trabajo en entornos cambiantes se encuentra en ***El trabajo ya no es lo que era.***

[11] Para explorar más sobre las personas en el sector tecnológico se recomienda la lectura ***Más platón y menos tech.***



Fuente: Prosegur, 2022

Nuestra visión

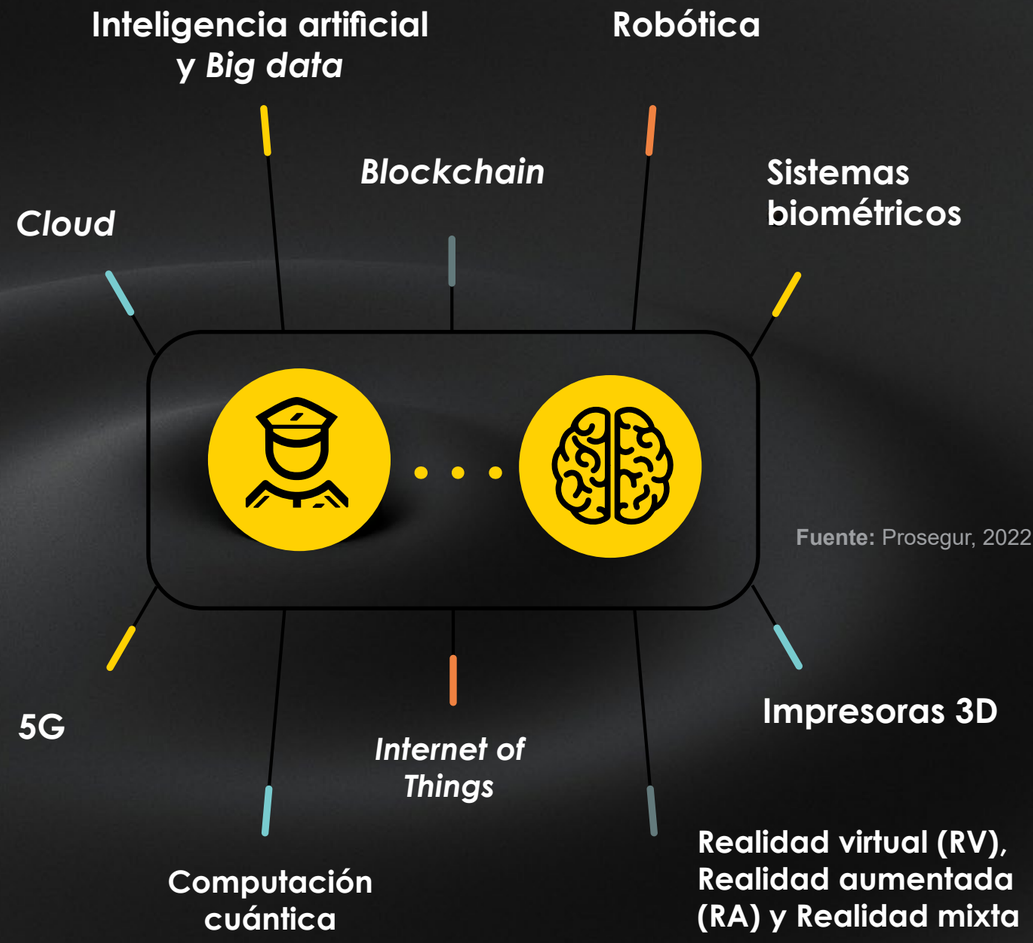
3.1.2. Las tecnologías como medio

La tecnología se configura como el gran game changer de futuro y, sin lugar a dudas, será una de las fuentes principales para el surgimiento de **nuevos riesgos y amenazas**, pero también de **oportunidades** de negocio y **potenciales mejoras** de servicios y productos[12].
Nos apoyamos en tecnologías que estén claramente testadas y sean eficientes, lejos de los hype tecnológicos habituales:

- Tecnologías que actúan en entorno físico tanto para ejecutar tareas como para enviar información a nuestro SOC: cámaras, sensores, drones, alarmas, redes y sistemas, robótica, etc.
- Tecnologías utilizadas en nuestro SOC para tratamiento y análisis de la información y apoyo a la toma de decisiones: inteligencia artificial, machine learning, data science, procesamiento de lenguaje natural, modelos GIS, cloud computing, simuladores virtuales y en 3D.
- Desarrollos propios para conectar los mundos físicos y digitales, y para interactuar con los inputs de fuentes de información y con los receptores finales del producto final (Genzai, Pops y Connect).

Son disruptivas porque irrumpen bruscamente como fuerzas productivas dado su **crecimiento exponencial,**[13] y son **convergentes** porque se complementan (enabling) y potencian entre sí, acelerando aún más el desarrollo tecnológico[14].

Cuando los procesos cuantitativos acelerados alcanzan cierto ritmo, se genera un salto, un cambio cualitativo que impacta en la sociedad. Esta es la verdadera **fuerza transformadora de la tecnología.**



Fuente: Prosegur, 2022

[12] Es interesante el concepto y libro ***Antifragile.***
[13] Un ejemplo de exponencialidad es el tiempo de uso según la generación de conectividad móvil: con el 3G se tardaba 45 minutos en descargar una película en HD, con el 4G se tarda 21 segundos y con el 5G menos tiempo que en leer esta frase (Diamandis y Kotler, 2021).
[14] Por ejemplo, el desarrollo de nuevos medicamentos se acelera no únicamente por el avance exponencial de la biotecnología, sino por la aplicación de la inteligencia artificial y la informática cuántica. También los avances en la construcción de drones derivan de la combinación de machine learning, nuevos materiales e impresión 3D.

Nuestra visión

3.1.3. Los datos como valor añadido

Tratar y trabajar datos no es tarea sencilla, pero sin duda es una oportunidad[15] para marcar la diferencia con un valor añadido en el mercado[16]. Se trata de analizar de forma estratégica[17] para detectar alertas tempranas y señales débiles[18] aportando visión prospectiva que permita la adopción de respuestas adecuadas en tiempo y forma a cada incidente y generar, a la vez, **ecosistemas que interactúen de forma inteligente** para proteger personas y empresas en entornos cambiantes.

El manejo de elevados volúmenes de datos permite establecer **visiones globales y periféricas.** Es una capacidad a desarrollar en los **niveles estratégicos,** basado en una monitorización activa del entorno, con objeto de detectar amenazas y oportunidades para las organizaciones. Y adoptar estas visiones es lo que nos permite adelantarnos a las ***innovaciones criminales***[19].

[15] Sobre información y datos se recomienda la lectura de ***Factfulness.***
[16] Los datos se emplean para establecer los riesgos e identificar las amenazas, pero serán siempre sistemas de apoyo a la decisión de los expertos en seguridad.
[17] Profundiza sobre una auténtica visión estratégica el libro ***Good Strategy, Bad Strategy.***
[18] Se trata de una observación o pieza de información que aparenta no tener conexión o relación, pero que puede ser un reconocido como un posible patrón si se observa desde otro punto de vista o se conecta con otras piezas de información. La detección de señales débiles se realiza a través de escanear el entorno (Environmental scanning), con capacidades como la visión periférica y una orientación prospectiva; tal y como refiere Ansoff en su estudio sobre ***Managing Strategic Surprise by Response to Weak Signals.***
[19] Por ejemplo, conocer los robos que se producen en una determinada tienda en un punto concreto del país puede proporcionar información útil, pero administrar la información de la totalidad de los robos que se producen en todas las tiendas de un determinado grupo empresarial en todo el territorio nacional proporciona inteligencia de negocio hasta ahora desconocida. Así es como podemos anticipar riesgos y reforzar la seguridad que personas y empresas necesitan en la actualidad.

Nuestra visión
3.2. El iSOC como cerebro

Esta transformación e hibridación del mundo crea nuevos desafíos y oportunidades a la seguridad de personas y negocios. Consecuentemente, los Security Operations Centers (SOC) evolucionan también.

En este contexto[20], nuestro modelo se basa en los iSOC, Centros de Operaciones de Seguridad con una “i” diferencial: con información de gran valor, de carácter internacional, con capacidad integradora que aporta innovación desde una visión inteligente. Todos se coordinan de forma global. Los iSOC engloban la integración de personas, datos y tecnologías de manera inteligente, estratégica y prospectiva. Ello nos permite aprovechar la experiencia para generar un procesamiento de alto nivel de complejidad, más similar al humano que nunca.

En el modelo de seguridad híbrida, las soluciones se gestan en el iSOC mediante **estrategias operativas sofisticadas** basadas en el funcionamiento cerebral[21]: el iSOC es el cerebro del modelo. Nos permite conocer de forma muy ágil y ajustada a la realidad lo que ocurre en el mundo, y hacerlo además de forma preventiva y automatizada para impulsar la eficiencia en las respuestas. Esto se logra focalizando los esfuerzos en las siguientes tareas:

- Favorecer la configuración de un iSOC **global y unificado** que contribuya de forma ágil y eficiente al modelo de seguridad híbrida garantizando la seguridad de personas y empresas trabajando datos globales.
- Cubrir las necesidades de seguridad adaptado a los requerimientos de las empresas y las personas afectadas, **customizando las soluciones** sin perder capacidad de automatización de procesos estratégicos de mejora para generar respuestas inteligentes.
- Favorecer el análisis de datos respetando la privacidad y **dando coherencia a la gestión integral** de todas las organizaciones y personas, un SOC del mundo que integre las incidencias del presente para proteger un futuro común.

[20] Tradicionalmente, los SOCs han trabajado en formato de reacción ante incidentes a partir de las capacidades de monitorización según la información disponible. Lo cierto es que a partir del siglo XXI viró hacia un enfoque de seguimiento reactivo con cierta capacidad de análisis de vulnerabilidad del entorno. Posteriormente se reorientó hacia un enfoque proactivo aplicando inteligencia al estudio de amenazas. Finalmente, la inclusión de procesos automatizados permite la inclusión de evaluaciones de riesgo externo más complejas y un cierto grado de orquestación. Para leer un breve pero más específico repaso de los SOCs se puede leer a ***ISACA, 2021.***

[21] Porque aprender es un ejercicio de valentía y perseverancia, sirva como explicación del funcionamiento cerebral el libro ***Atrévete a saber.***

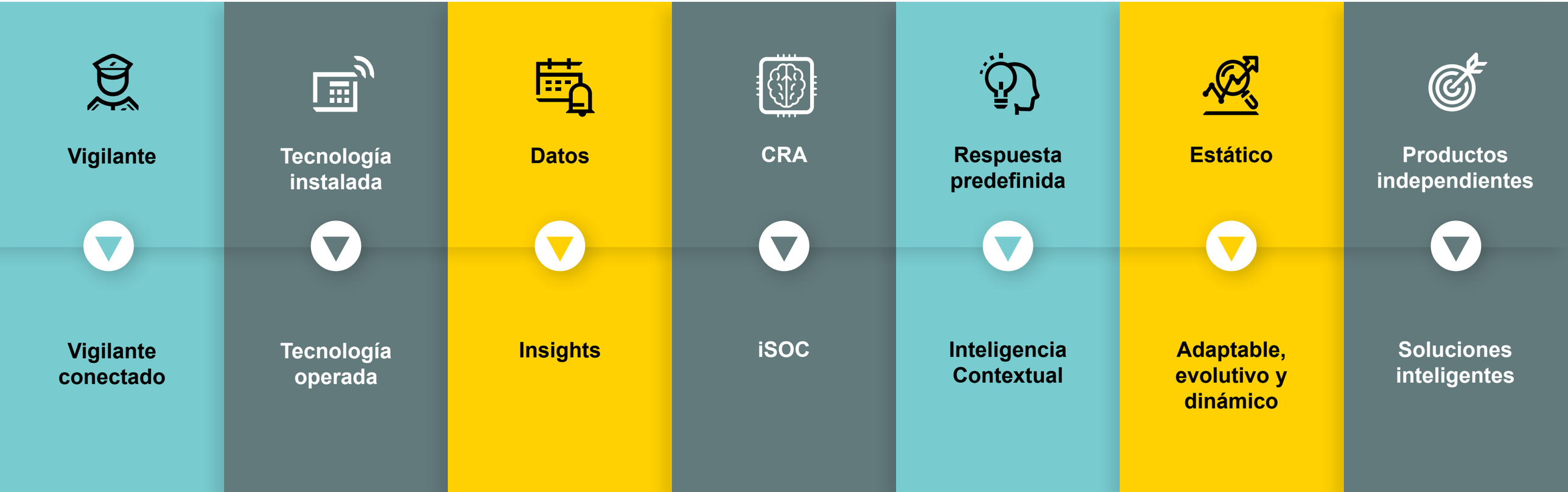
Nuestra visión

3.2. El iSOC como cerebro

Si ubicamos el iSOC en una corporación con visión periférica y prospectiva, en un modelo preparado para amenazas híbridas y entornos cambiantes, este cerebro deberá pensar en clave de futuro.

Así, un SOC preparado para el futuro, al que toda organización debe aspirar, tiene que ser revolucionario y transformador, preparando para el cambio a cada elemento del modelo de seguridad híbrida.

Siendo capaz de transformar las personas, la tecnología y los datos, vértices de su propio modelo, en expertos conectados, tecnología operada y vinculada y en insights que aporten **valor añadido en la toma de decisiones.** Esto es lo que deriva en una auténtica transformación de su cerebro, de un centro de gestión de respuestas a un iSOC, que trabaje con inteligencia contextual mediante un enfoque adaptable, evolución y dinámico; así, para cada problema de cada persona o negocio será capaz de encontrar una solución integral, inteligente y única.



Nuestra visión

3.3. La base: organización con propósito y cultura

Para triangular de forma certera personas, tecnologías y datos es esencial una organización capaz de ofrecer **soluciones de seguridad *"as a service"*** y que se adapte continuamente a los entornos de personas y negocios.

- Ejecutadas por expertos profesionales empoderados con tecnología innovadora.
- Potenciadas por un modelo global de datos e inteligencia que permite anticipar y mitigar riesgos.
- Respondiendo de la forma más eficiente y agregando valor al negocio.

Aquellos negocios que hayan desarrollado funciones de seguridad tradicional abarcando sus diversas formas y asumiendo la complejidad de los riesgos durante un prolongado período de tiempo contarán con una ventaja competitiva: **el valor diferencial de aportar una dilatada experiencia** a los procesos de innovación. Contar con un importante know-how en seguridad centrado en proteger personas, hogares, negocios y activos es la esencia de la empresa híbrida, pues es el inexcusable punto de partida para la transformación digital de sus servicios.

La base del modelo de seguridad híbrida es la organización inteligente[22]: una empresa que aporta su cultura de organización y su propósito de proteger personas y negocios y que a su vez aprende del entorno de manera expansiva.

[22] Sobre cómo es una organización inteligente se recomienda el libro ***La quinta disciplina.***

Liderar entornos híbridos

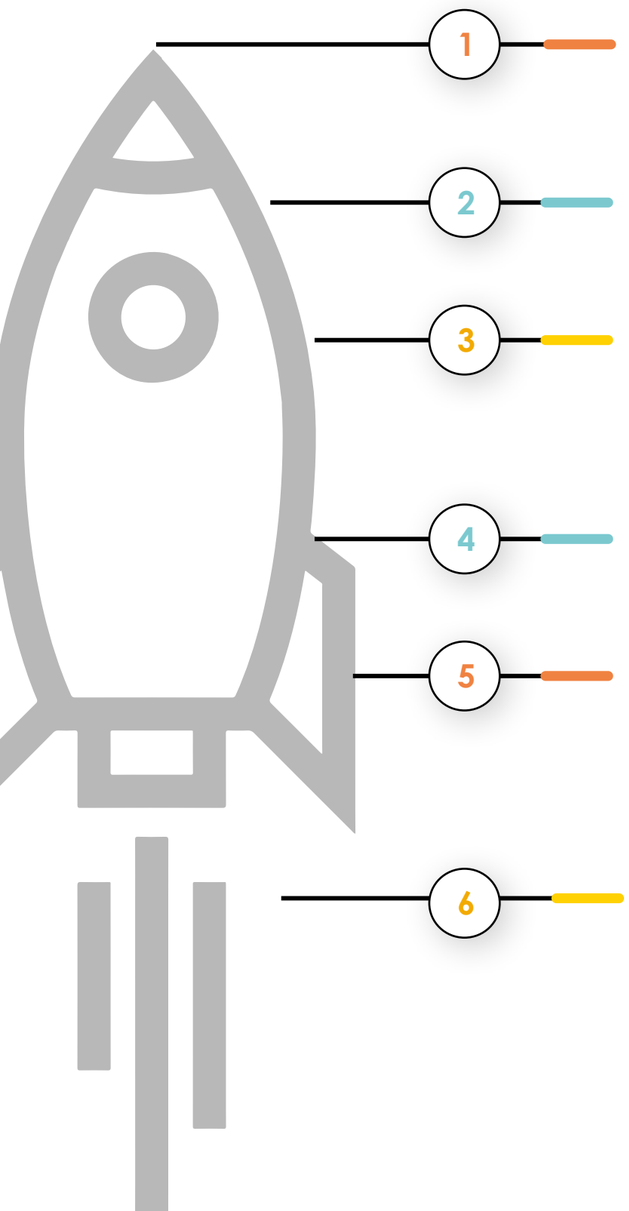
Tips para la acción

04

Liderar entornos híbridos

4.1. Tips para la acción

El liderazgo creativo[23], valiente y sereno **marcará la diferencia** en los entornos disruptivos, y será clave en la seguridad híbrida. A continuación, exponemos unas tips para la acción.



Despegar desde la experiencia en seguridad. Se requiere una gran experiencia para garantizar la seguridad de personas y negocios en los nuevos entornos físicos, digitales e híbridos. Precisamente esta es la **base robusta** sobre la que se pueden introducir los potentes procesos de innovación que generen auténticos resultados de **mejora y adaptación al contexto disruptivo** actual.

De la transformación a la aceleración digital. Debemos orientar las mejoras en seguridad de forma progresiva y exponencial aprovechando la **convergencia de las tecnologías y el talento de las personas;** esto a su vez genera una inercia de innovación cada vez más capacitada y ágil, y bien implementada permite **anticipar** nuevos cambios.

Buenos compañeros de viaje. Colaborar con otros actores es esencial para **ampliar perspectivas y capacidades,** y dar así una protección más adecuada, incluso adelantándonos a necesidades futuras: se requieren socios estratégicos tanto para la adquisición de tecnologías punteras, como para la detección de necesidades del entorno; también para el aprendizaje orientado a la mejora de los servicios y la implementación de servicios efectivos de seguridad híbrida.

El viaje será largo o no será. La innovación es para organizaciones valientes: el éxito que de ella deriva es consecuencia de una **apuesta decidida** por el auténtico cambio, asumiendo que la seguridad es algo dinámico. Se requiere tiempo, visión, inversión inteligente y perseverancia en la implantación de procesos para la seguridad híbrida.

Las personas marcan el camino. Una solución única para una persona única es la esencia de la seguridad híbrida. Para ello, es vital la capacidad de customización mediante procesos ágiles cuya clave radica precisamente en el factor humano: **competencias excepcionalmente humanas** como la creatividad, el liderazgo o la flexibilidad componen el mecanismo perfecto para complementar con tecnología: personas expertas en seguridad **empoderadas** por las tecnologías más innovadoras.

El destino es mejorar. La tecnología es un medio y la innovación hacia lo híbrido una fórmula que tiene el **fin de mejorar,** por lo que el espíritu de perfeccionamiento en seguridad híbrida deriva ineludiblemente en cultivar el **cambio constante**.

---

[23] Se recomienda ampliar esta idea con la lectura de ***Leassons in creative leadership.***

Los libros en los que nos hemos basado para construir este modelo

Los libros en los que nos hemos basado para construir este modelo

- Modernidad líquida
- Mil años de historia no lineal
- *Good Strategy, Bad Strategy*
- Manual para vivir en la era de la incertidumbre
- *The Fat Tail*
- *Managing Strategic Surprise by Response to Weak Signals*
- *The future goes faster than you think*
- El trabajo ya no es lo que era
- Atrévete a saber
- *Corporate Foresight*
- Más platón y menos *tech*
- La quinta disciplina
- *The Digital Future*
- *Antifragile*
- *Leassons in creative leadership*
- *Exponential*
- *Factfulness*
- El *shock* del futuro

Human capabilities that make technology work. Technological capabilities that make people smarter.

PROSEGUR **RESEARCH**

research@prosegur.com
www.prosegurresearch.com

PROSEGUR