PROSEGUR RESEARCH

Hybrid Security Series

Las personas en **seguridad híbrida**

2024

PROSEGUR
SECURITY

Este documento es **interactivo**

HOME

01

Las personas como prioridad

HOME

01
Las personas como prioridad

02
Las competencias de los expertos en seguridad

03
Los profesionales de la seguridad híbrida

04
El liderazgo innovador desde la experiencia

01

LAS PERSONAS COMO PRIORIDAD

Las personas son las grandes protagonistas de 2024, como ya advertimos desde **Prosegur Research,** y **de nosotros depende entender los grandes cambios que se aproximan;** adaptando, anticipando y aprovechando serán los gerundios que marcarán la diferencia.

> “Si hay algo en nosotros verdaderamente divino, es la voluntad. Por ella afirmamos la personalidad, templamos el carácter, desafiamos la adversidad, reconstruimos el cerebro y nos superamos diariamente.
>
> **Santiago Ramón y Cajal**

Desde una visión sistémica, y entendiendo los impactos y la interdependencia del mundo global, **Donella Meadows** nos da **14 consejos interesantes para operar en un “mundo de sistemas”.** En esta publicación vamos a explicar el contexto en el que debemos recibirlos bajo la transformación empresarial que estamos viviendo, y también el entorno específico de seguridad, de creciente complejidad, donde estos consejos pueden resultar críticos.

Gráfico 1
Consejos de Donella Meadows para un mundo sistémico

1. Pilla el ritmo
2. Aprende a escuchar la sabiduría del sistema
3. Airea y refresca tus modelos mentales
4. Sé humilde y en constante aprendizaje
5. Honra y protege la información
6. Localiza la responsabilidad en el sistema
7. Crea políticas de feedback para sistemas de retroalimentación
8. Presta atención a lo importante, no solo a lo cuantificable
9. Busca el bien del conjunto
10. Amplía horizontes temporales
11. Amplía horizontes de pensamiento
12. Amplía horizontes del cuidado
13. Celebra la complejidad
14. Aférrate a la meta de la bondad

Fuente: Prosegur Research, 2024 basado en Donella Meadows, 2024.

En contraposición a la obsesión por el control y la predicción, Meadows explica que **los sistemas no se pueden controlar, pero sí (re)diseñar; en otras palabras, bailar con ellos.** Vivir en un mundo de sistemas requiere, además de la habilidad de calcular, la capacidad para distinguir lo verdadero de lo falso, la racionalidad, la imaginación o la ética, entre otras.

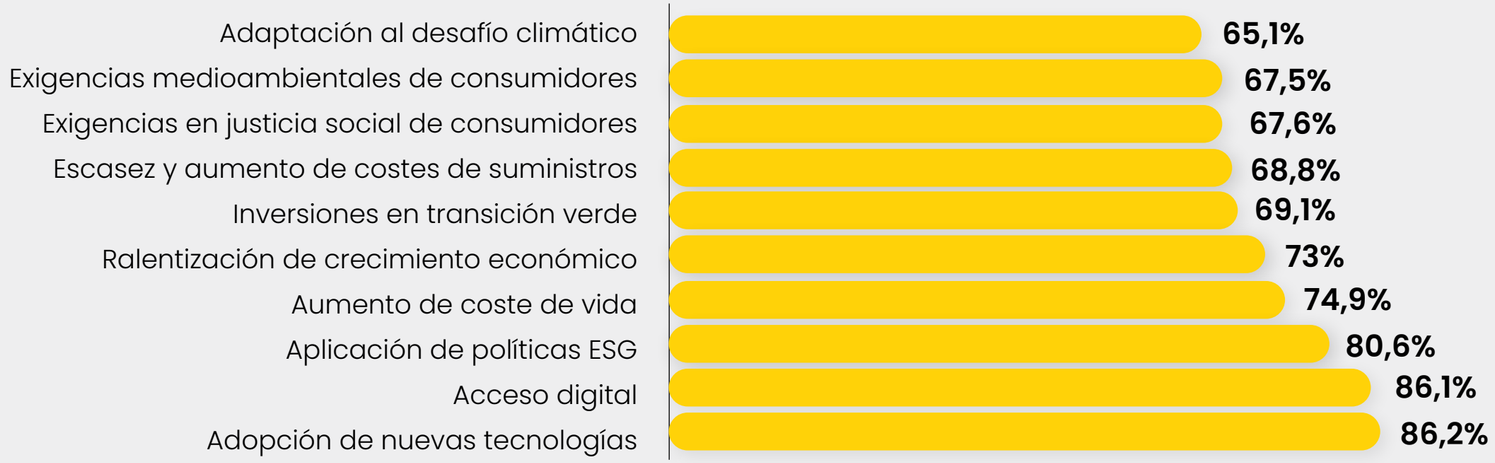
A Habilidades para un mundo en cambio

La constante transformación del entorno en el que nos encontramos inmersos requiere una capacidad de **adaptación continua a los cambios** que se producen a todos los niveles, desde los tecnológicos o climáticos hasta los económicos y políticos. La incertidumbre generalizada está propiciando **tensión y preocupación crecientes en los trabajadores,** con una demanda en relación con su bienestar, unas condiciones de vida dignas y un propósito laboral hacia un objetivo común, que se ha visto reflejado en fenómenos recientes como la **Gran Renuncia.**

En este sentido, drivers como la tecnología, las variables demográficas o las condiciones socioeconómicas están teniendo un impacto profundo en la forma en que se lleva a cabo el trabajo, reconfigurando a nivel global el mercado laboral.

- Según Adecco, **uno de cada dos trabajadores quiere cambiar de empleo** buscando un mayor salario, si bien hasta el 44% aceptaría permanecer en su organización si se apuesta por la **progresión laboral** y el **reskilling** de habilidades.
- Según el **Future of Jobs Report** del World Economic Forum (WEF), hasta el 60% de todos los empleados necesitarán revisar y **aprender nuevas habilidades y conocimientos** para 2027 en el proceso conocido como **reskilling.**

Gráfico 2
TOP-10 drivers para la transformación empresarial según % de opinión



Fuente: Prosegur Research, 2024 basado en ***WEF***

Ya en el año 2019 la Organización para la Cooperación y el Desarrollo Económicos (OCDE) señaló que **en los próximos 15 años hasta el 32% de todos los trabajos del mundo cambiarían radicalmente** debido a las nuevas tecnologías, lo que hace necesario una readaptación y reconfiguración de las habilidades de los trabajadores. Sin embargo, estudios de Boston Consulting Group (BCG) indican que solo el 24% de las organizaciones muestran una clara conexión entre la estrategia corporativa y los esfuerzos en reskilling, a pesar de que casi el 70% de los empleados desean aprender nuevas habilidades y competencias para seguir siendo competitivos. Así, desde el Future for Work Institute destacan la necesidad de incorporar nuevas **prácticas de gestión de equipos basadas en habilidades** como eje para el futuro del trabajo.

Con todo, los datos nos orientan hacia un **futuro optimista:** el WEF defiende que las tecnologías para sectores tan variados como la agricultura, el comercio electrónico, la ciberseguridad o la robótica serán positivas para el mercado laboral durante los próximos cinco años.

Así, son multitud las variables que afectan de forma directa o indirecta a la reconfiguración de la fuerza de trabajo global. A modo de ejemplo, el WEF argumenta que **las tendencias económicas y geopolíticas han creado resultados divergentes** en los mercados laborales de diferentes regiones geográficas: mientras que los **países de renta alta** experimentan **mercados laborales competitivos,** los **países de renta baja y media** se enfrentan a un **desempleo mayor** que antes de la pandemia de COVID-19, que en lugares como Sudáfrica se sitúa en más del 30%.

Adicionalmente, desde The Future of Skills se apuntan **siete megatendencias** que condicionarán el futuro del trabajo y las habilidades humanas necesarias para 2030:

Progreso tecnológico

La digitalización, la automatización de empleos manuales por máquinas o la mayor conectividad son algunas de las áreas que están transformando la actividad empresarial de multitud de organizaciones. Según el **Digital Leadership Report 2021,** el 60% de las compañías han mudado sus operaciones centrales a la nube. Además, los datos de PricewaterhouseCoopers (PwC) apuntan que casi el 40% de los empleados están preocupados por el **riesgo de la eliminación de puestos de trabajo** debido a la automatización de procesos, si bien el 73% considera que la tecnología nunca podrá reemplazar las capacidades humanas. Por ello, durante los próximos años el progreso tecnológico moldeará el mercado laboral, atrayendo nuevo talento en sectores y conocimientos punteros como el cloud computing, las plataformas colaborativas o el análisis de datos.

Globalización

La creciente interdependencia de los mercados y las compañías durante las últimas décadas ha permitido reducir costes, generar empleo y compartir conocimientos y productos entre diversos países. Sin embargo, en los últimos años se está observando un cierto retroceso en esta materia, con algunos discursos proteccionistas y la imposición de diferentes medidas como los aranceles o el reshoring de empresas a los países de origen, lo que está suponiendo en parte un freno a la globalización, particularmente en sectores clave como el tecnológico.

Demografía

El envejecimiento de la población y la caída en la tasa de natalidad en países mayormente occidentales está generando una brecha generacional con comportamientos muy variados en materias de consumo y empleabilidad, como la búsqueda de propósito en generaciones Millennial o la Z, ocasionando tensiones sociales adicionales a diferentes niveles, como las inversiones necesarias en infraestructuras, pensiones o asistencia sanitaria, por ejemplo. Todo ello puede derivar en la necesidad de reorientar los mercados laborales hacia países que en los próximos años o décadas experimenten una explosión demográfica con población joven en edad de trabajar, especialmente en Asia y África.

Sostenibilidad

Los efectos del desafío climático pueden generar severos impactos en sectores como la agricultura, el turismo o la energía, entre otros, por lo que los trabajos de la llamada “economía verde” son vulnerables a los efectos de los comportamientos de los consumidores y las acciones políticas que se lleven a cabo en esta materia. Asimismo, efectos derivados como la inseguridad alimentaria podrían exacerbar problemas estructurales como la pobreza, acrecentando conflictos geopolíticos, económicos y sociales entre diferentes Estados y afectando en última instancia a la economía mundial y al mercado laboral.

Urbanización

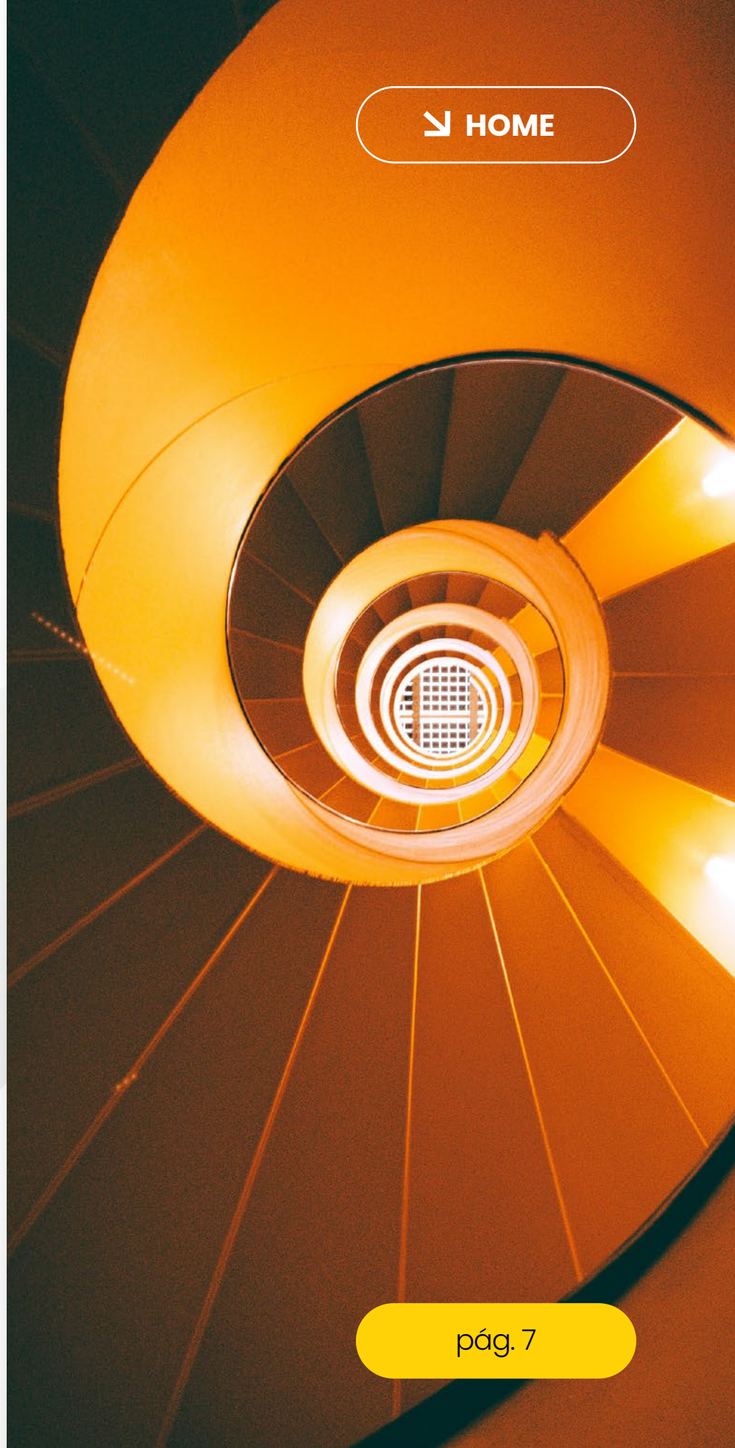
Mientras que en la actualidad se estima que el 50% de la población mundial vive en grandes urbes, para 2050 se prevé que la cifra alcance el 70%. La atracción de las industrias y la concentración de oportunidades profesionales en las grandes ciudades son dos tendencias significativas en el mercado laboral, si bien los posibles cambios en las políticas fiscales, los desafíos climáticos, la violencia urbana, la inversión necesaria en infraestructuras y servicios públicos y las consecuentes ratios de deuda pública pueden configurarse como fuentes de conflicto durante las próximas décadas.

Disparidad creciente

La progresiva diferencia entre los ingresos y la riqueza constituye uno de los mayores desafíos para las sociedades, lo que está provocando una disminución del poder adquisitivo, una progresiva erosión de la clase media y un desplazamiento en la distribución de la renta hacia los extremos superior e inferior. De este modo, la educación, la inversión pública y la acción política pueden impactar en el mercado laboral durante los próximos años, sin descartar posibles fuentes de conflicto como la inestabilidad social, la polarización o la desconfianza hacia los gobiernos.

Incertidumbre política

La inestabilidad política puede afectar negativamente a sectores estratégicos de multitud de Estados, especialmente en los que las acciones políticas impactan de manera directa, como la defensa, la construcción, la sanidad o la energía. Por ello, la incertidumbre puede generar repercusiones en el mercado laboral, aumentando la competitividad entre países para la atracción de inversión o la reasignación de recursos hacia las empresas con mayor productividad.



HOME

Todo lo anteriormente expuesto puede ocasionar **multitud de escenarios de futuro** en la materia que nos ocupa, de acuerdo con las tendencias hasta ahora apuntadas evolucionen y configuren los mercados laborales de todo el mundo. En este sentido, PwC señala **cuatro posibles escenarios de futuro para el trabajo en 2030:**

Mundo rojo

Marcadas por la innovación, los nichos de mercado y la ausencia de reglas, las empresas con mayor capacidad de innovación y se caractericen por la agilidad, la rapidez y la personalización de productos tendrían más probabilidades de éxito, si bien este escenario presenta serios desafíos organizacionales como la necesidad de innovación constante o la competencia empresarial por la atracción de talento en aptitudes críticas.

Mundo azul

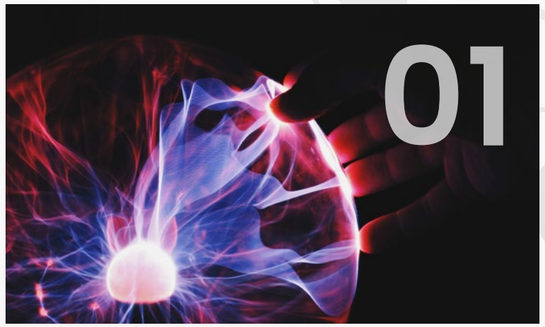
Las organizaciones multinacionales y la elección del consumidor serían los ejes de futuro en un mercado altamente capitalista, por lo que la empleabilidad y la permanencia del trabajador en las compañías dependería de su éxito y su relevancia, además de existir amenazas adicionales como la fusión de empresas o los ciberataques.

Mundo verde

La sostenibilidad convierte las palabras en hechos, priorizando la concienciación en materia ecológica en el mercado laboral. Los estándares éticos favorecerían la lealtad de los trabajadores hacia las empresas con un firme propósito verde, además de caracterizarse por la flexibilidad laboral y la confianza entre empleado y empleador. Por ello, la construcción de imagen de marca, la comunicación, la prevención de amenazas y el compliance serían algunas de las áreas con mayor relevancia para las empresas.

Mundo amarillo

Los empleados y las compañías trabajarían conjuntamente a favor del bienestar social y la justicia, por lo que la lealtad y el compromiso laboral no se orienta hacia la marca, sino hacia el sentimiento compartido de luchar por una misma causa. La ética, la transparencia y la acción político-social de las organizaciones serían algunos de los desafíos prioritarios de estas.



pág. 8

HOME

B Las competencias del futuro

Las habilidades necesarias en la actualidad están cambiando de forma veloz. Aún cuando las **habilidades técnicas** continúan siendo relevantes, las **habilidades más puramente humanas** como la comunicación, la colaboración y la capacidad analítica están adquiriendo especial protagonismo. La interacción con los nuevos desarrollos tecnológicos y la capacidad de aprender nuevos conocimientos se han convertido en habilidades fundamentales en un **entorno laboral en constante evolución.**

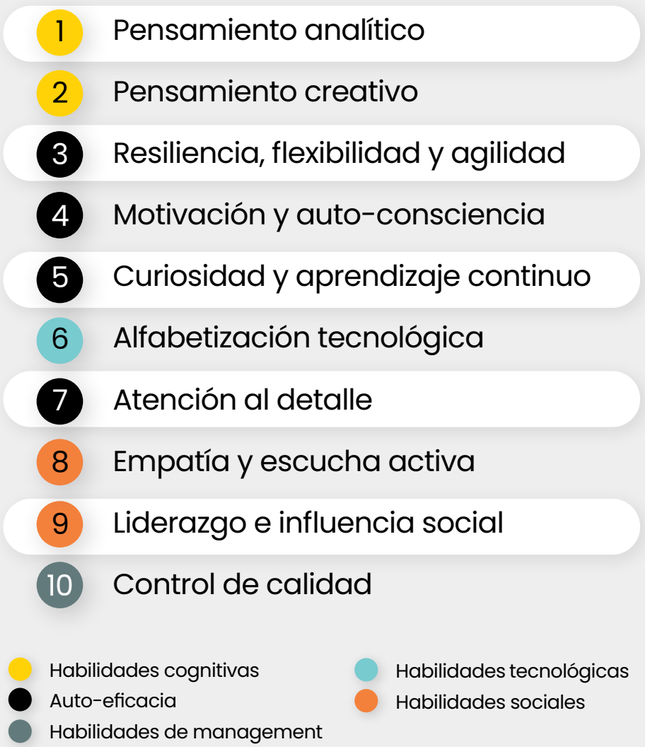
Según el WEF, algunos de los trabajos con peores expectativas para el futuro se relacionan con las tareas repetitivas como con las administrativas, mientras que los especialistas en sostenibilidad, los analistas de seguridad, los analistas de inteligencia empresarial o los ingenieros de energías renovables serán algunos de los trabajos con **mayor crecimiento en el corto y medio plazo.**

Sin embargo, se deben tener en cuenta las variables sociales ante el análisis del futuro mercado laboral, puesto que **la demografía como eje de futuro** revela resultados dispares. Algunos datos muestran que la automatización de empleos en países como Sudáfrica podría derivar en la **destrucción de más de tres millones de trabajo actuales** para 2030.

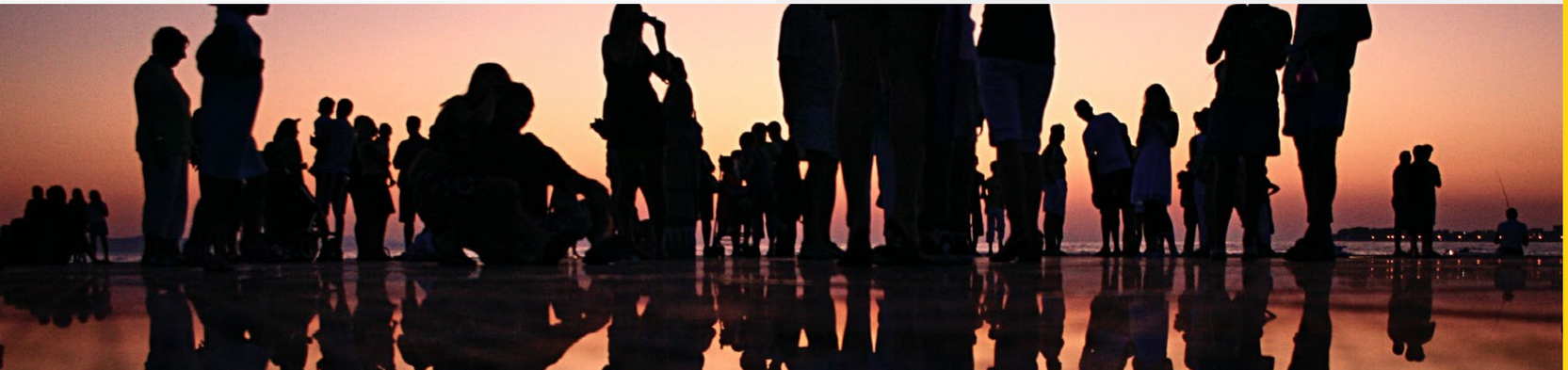
Ante este panorama, diferentes compañías e instituciones internacionales están estudiando las habilidades que marcarán la diferencia de valor en los trabajadores, que generalmente deben competir en **mercados tensionados, saturados, con una alta competitividad para un mismo puesto y, en ocasiones, con una sobrecualificación para la tarea a desempeñar.**

El Future of Jobs Report de 2023 del WEF destaca una serie de habilidades necesarias y que marcarán un valor diferencial competitivo en el trabajador durante los próximos años:

Gráfico 3
TOP-10 habilidades profesionales para el futuro



Fuente: Prosegur Research, 2024 basado en ***WEF***



Por su parte, desde la Organización para la Cooperación y el Desarrollo Económicos (OCDE) señalan que existen ***tres grupos de habilidades esenciales para el trabajo en el futuro:***

A

Habilidades cognitivas y meta-cognitivas, que involucran procesos mentales como la capacidad aritmética, el lenguaje, el conocimiento y otras aptitudes verbales y no-verbales como la creatividad o el pensamiento crítico.

B

Habilidades sociales y emocionales, que permiten manifestar comportamientos y emociones para cultivar relaciones con los demás, incluyendo algunas como la empatía o la colaboración.

C

Habilidades prácticas y físicas, que se relacionan con la capacidad de operar con herramientas y operaciones como las tecnologías de la información y la comunicación.

02

Las competencias de los **expertos en seguridad**

HOME

01
Las personas como prioridad

02
Las competencias de los expertos en seguridad

03
Los profesionales de la seguridad híbrida

04
El liderazgo innovador desde la experiencia

HOME

02

LAS COMPETENCIAS DE LOS EXPERTOS EN SEGURIDAD

Desde Prosegur Research entendemos que el **mundo híbrido** en el que vivimos necesita de diferentes conocimientos: no podemos vivir en el presente con las herramientas del pasado. Las competencias humanas son absolutamente fundamentales e insustituibles, por lo que se debe **buscar el empoderamiento de los trabajadores potenciando sus habilidades mediante la palanca de cambio que constituye la tecnología.**

La clave radica en la alineación entre los recursos humanos, dotados de conocimiento y experiencia, con los medios tecnológicos adecuados, con el objetivo de adaptarse ante los cambios constantes del entorno. En palabras de Xavier Marcet, las máquinas se pueden sincronizar, pero no pueden sentir la complicidad, y en la actualidad resulta necesario construir complicidades en entornos corporativos que no anulen la empatía, la paciencia, el respeto o la generosidad que caracteriza a los equipos de personas que trabajan en sintonía y por un objetivo compartido.

Así pues, **en Prosegur Research creemos que existen cuatro categorías principales de habilidades, conocimientos, aptitudes y actitudes** que mejor preparan al trabajador para los cambios en el mercado laboral que se aproximan en el futuro y que mejor muestran los **pilares de la denominada seguridad híbrida:**

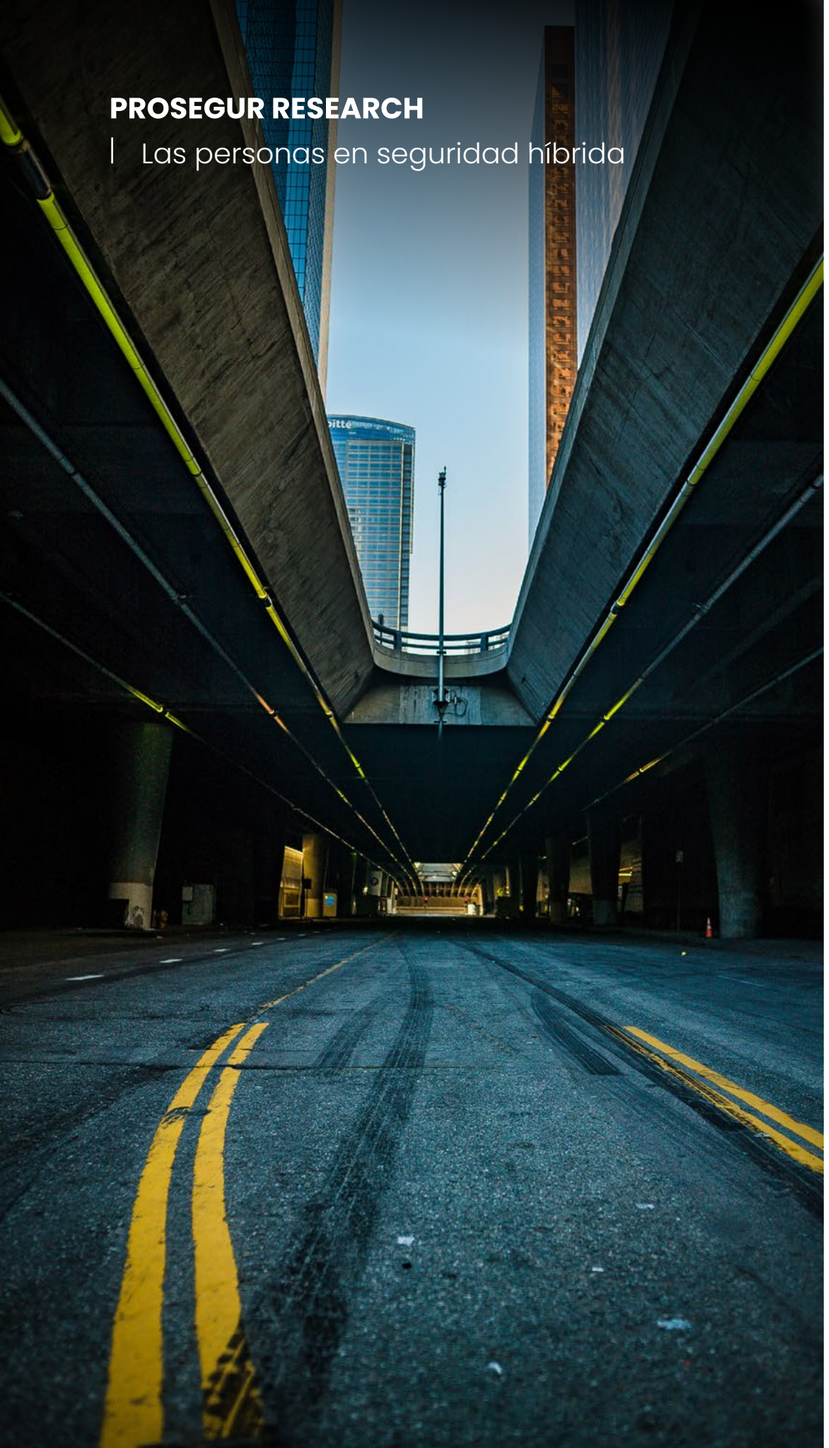
Competencias digitales
Vinculadas al manejo de las tecnologías de la organización: inteligencia artificial (IA), realidad virtual (RV), Blockchain, etc.

Expertos en seguridad
Profesionales con amplio conocimiento y experiencia internacional en gestión de riesgos y seguridad, en entornos conflictivos.

Autogestión
Para trabajar en un entorno volátil y de cambio continuo: la resiliencia, la tolerancia al estrés y la flexibilidad.

Competencias humanas
Como la resolución de problemas complejos, el pensamiento crítico, la creatividad, la influencia social, etc.

pág. 12



HOME

1 Competencias en seguridad

La volatilidad constante de los mercados financieros, la geopolítica o la inestabilidad social de multitud de países son algunas de las variables que afectan diariamente a la continuidad de negocio de las organizaciones, independientemente del sector al que pertenezcan, lo que puede derivar en grandes pérdidas económicas o en graves perjuicios para la imagen de la marca. De tal forma, se requieren profesionales con amplio conocimiento y experiencia en gestión de riesgos y seguridad que adapte lo que ocurre al marco empresarial en el que opera, entienda la transversalidad de los procesos y analice con una visión sistémica la realidad cambiante abaracando cuestiones como las siguientes:

Componente político
Involucra todos los aspectos relacionados con las decisiones políticas y la geopolítica que pueden afectar directa o indirectamente a las expectativas económicas de una empresa, así como su imagen o reputación, con la posibilidad de que disminuya el valor de la misma. De esta manera, la incertidumbre regulatoria, los marcos legales vigentes, la desinformación o los conflictos interestatales deben ser una materia de especial interés para cualquier experto en seguridad.

Componente económico
La economía influye en todas las decisiones diarias de cualquier compañía, por lo que el riesgo económico, entendido como la posibilidad de generar pérdidas monetarias o de inversión que obstaculicen el cumplimiento de la línea estratégica, debe estar presente en cualquier análisis de riesgos, en relación con la inflación, el precio de los activos, el déficit fiscal, la interdependencia económica o las disrupciones en la cadena de suministros.

Componente social
Se vincula con la posibilidad de generar climas de descontento, polarización, incertidumbre o conflictividad por parte de la ciudadanía

o colectivos civiles. Así, el activismo social, la polarización, las manifestaciones o la conflictividad laboral pueden impactar de manera directa sobre el patrimonio, la reputación o la imagen de marca de las organizaciones.

Componente ambiental

Las empresas no son independientes del entorno físico en el que operan, por lo que los expertos deben considerar aquellas variables con posibilidad de afectación directa e indirecta a las infraestructuras, a los trabajadores o a la propia actividad empresarial, como las enfermedades, las pandemias, los accidentes laborales o los eventos climáticos extremos.

Componente de seguridad física

Las amenazas físicas nunca deben infravalorarse, puesto que pueden generar daños sobre activos tangibles o intangibles de la organización. Por este motivo, el expertise sobre la delincuencia común en el territorio en el que opera la compañía, los impactos del crimen organizado, el vandalismo, la intrusión, las estafas, los secuestros, las agresiones o las consecuencias de posibles atentados terroristas se configuran como elementos de crucial relevancia para cualquier análisis de riesgos.

2 Competencias digitales

Relacionadas con el manejo de las tecnologías en la organización, son fundamentales para desempeñar correctamente la labor profesional. Según Qlik y The Future Labs, la **alfabetización de datos** será la habilidad más demandada en los trabajadores en 2030. De esta forma, el trabajador necesita conocer las aplicaciones de los **desarrollos más punteros y disruptivos,** como las tecnologías de inmersión virtual, la inteligencia artificial, la computación cuántica, el blockchain, la robótica o el Internet de las Cosas, entre otras.

Componente digital

El traslado de la conducta humana al ámbito digital conlleva comprender las diferencias y similitudes y entender el impacto del cambiante entorno digital en todos los ámbitos de la empresa, y especialmente el de la seguridad. El uso incorrecto y/o malintencionado de las tecnologías puede derivar en disrupciones en la actividad empresarial o en posibles vulnerabilidades de las infraestructuras. Por tanto, conocer variables como la digitalización, el espionaje industrial, los ciberataques, las aplicaciones criminales de la robótica o los drones, las aplicaciones de la inteligencia artificial en materia de suplantaciones de identidad o los riesgos en el cifrado de información por los avances en la computación cuántica es vital para garantizar el correcto desempeño de cualquier compañía.

Componente tecnológico

Los cambios técnicos siguen su curso, y estar al día en las **tecnologías más innovadoras** requiere inevitablemente unos conocimientos y competencias denominadas “duras”. Entender no solo el uso, sino también el diseño y la implementación de las tecnologías adquiere un protagonismo creciente en los expertos en seguridad: tecnologías consolidadas como Internet de las cosas, nube o cloud, robótica e inteligencia artificial, tecnologías en expansión como los sistemas biométricos, el blockchain, la realidad aumentada o el 5G, así como potenciales tecnologías disruptivas como las impresoras 3D, realidades mixtas o la computación cuántica marcarán, todas ellas, el futuro de la seguridad, que sin duda tendrá un importante componente tecnológico.

3 Competencias humanas

Con el propósito de desempeñar trabajos en entornos cambiantes y puestos de trabajo multifuncionales, se debe contar con diversas capacidades puramente humanas y que pueden ser el valor diferencial en un trabajador:

- **Pensamiento analítico e integrador**
  Los retos híbridos exigen de los empleados la habilidad de analizar el entorno de forma ágil y desagregar los problemas en diversas partes para que, apoyados por la tecnología más puntera, identifiquen las soluciones integradas y adaptadas a las necesidades de cada cliente y situación.

- **Resolución de problemas complejos**
  Resolver problemas para los que todavía no hay solución es algo intrínsecamente humano, y los expertos empoderados por la tecnología lo realizan cada día para abordar la compleja realidad y afrontar los desafíos híbridos que requieren soluciones únicas.

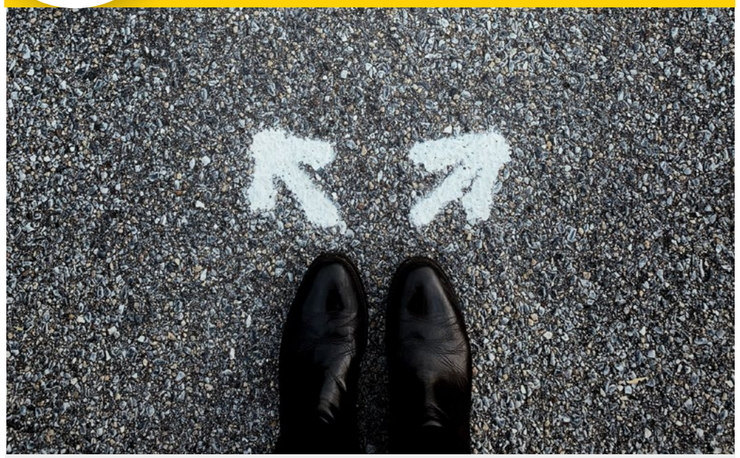
- **Pensamiento crítico e innovador**
  Los profesionales de la seguridad híbrida analizan la información de cualquier canal con imparcialidad, honestidad y objetividad para garantizar la mejor protección de personas, activos y negocios.

- **Creatividad y generación de ideas**
  La tecnología es la gran aliada de los expertos en seguridad. Cuando aplicamos la creatividad humana para desarrollar novedosos procesos, identificar nuevas fórmulas de mejora y respuesta ante incidentes y se potencia la eficiencia de servicios, manteniendo el máximo nivel de seguridad son iniciativas constantes.

- **Empatía**
  Los expertos conocen las necesidades de empresas y personas porque se posicionan en su lugar y gracias a ello son capaces de identificar las soluciones de seguridad adecuadas a cada entorno físico o digital en el que operan.

HOME

4 Competencias en autogestión

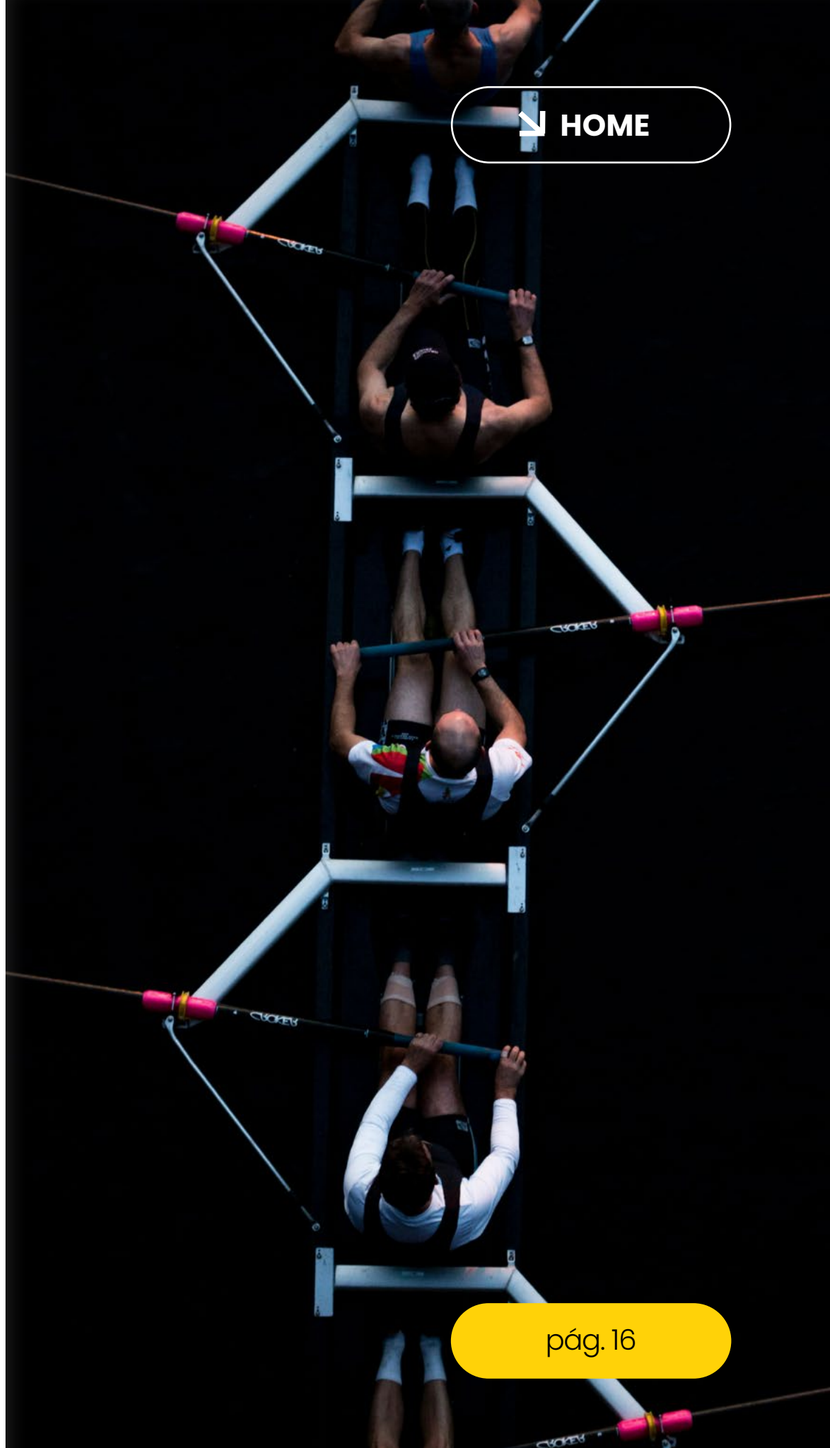


Las habilidades de autogestión y liderazgo resultan necesarias ante el turbulento entorno que nos rodea. El mundo requiere adaptación, flexibilidad, gestión a la frustración y, en definitiva, resiliencia para transformar los retos y desafíos en oportunidades:

- **Liderazgo y trabajo en equipo**
  Los mejores expertos en seguridad híbrida lideran equipos y generan influencia social en las personas para ser capaces de absorber todo el potencial tecnológico a su disposición. Responder de forma conjunta y coordinada por parte de todos los actores y herramientas involucrados en cada servicio es esencial para ofrecer una seguridad integral en entornos híbridos.

- **Flexibilidad y resiliencia**
  En seguridad, los expertos aprenden a trabajar bajo presión, gestionar sus emociones y adaptarse a los constantes cambios del entorno, por lo que los modelos mentales ágiles son indispensables para aprender de cada nuevo avance tecnológico y ponerlo a disposición de los clientes.

- **Aprendizaje activo y estrategias de aprendizaje**
  La disrupción es constante en los actuales entornos híbridos, por lo que los expertos en seguridad están aprendiendo permanentemente y adoptan distintas estrategias de aprendizaje según el contexto, aplicando las herramientas digitales pertinentes en cada situación.



03

Los profesionales de la seguridad híbrida

HOME

01
Las personas como prioridad

02
Las competencias de los expertos en seguridad

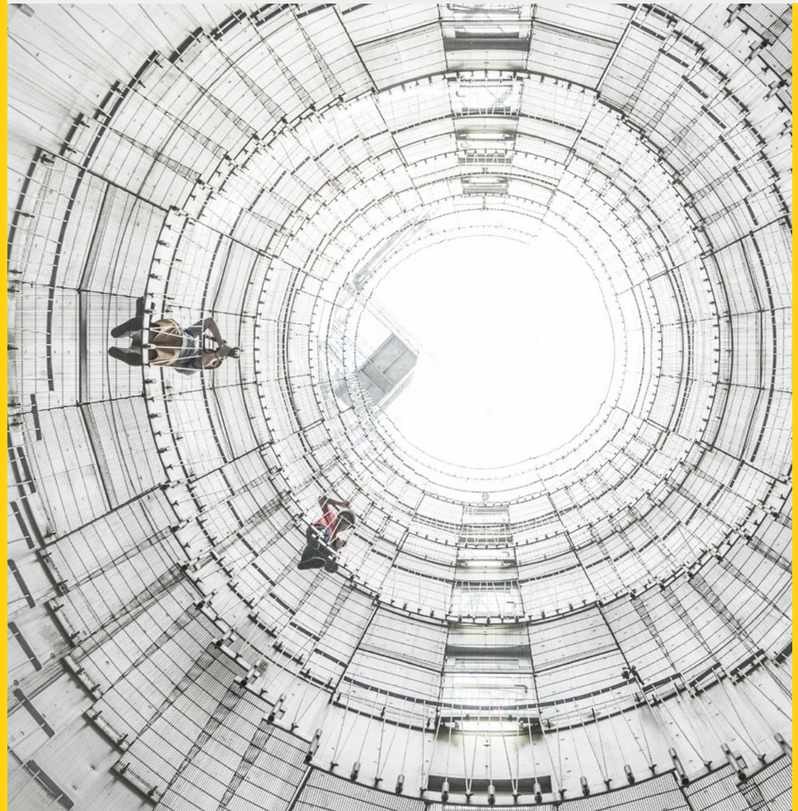
03
Los profesionales de la seguridad híbrida

04
El liderazgo innovador desde la experiencia

03

LOS PROFESIONALES DE LA SEGURIDAD HÍBRIDA

La contribución de las personas en términos de **comprensión del contexto y su capacidad para innovar** son aspectos clave desde una perspectiva estratégica, especialmente en un mundo de complejidad creciente como el actual, y en un **contexto de seguridad ampliada** que demandará, sin duda, nuevas competencias específicamente **dentro del sector.**



> Nos movemos hacia un mundo en el que los riesgos tradicionales no solo persisten, sino que crecen con una complejidad adicional. Las amenazas surgen de fuentes cada vez más inesperadas y difusas, y el concepto de Seguridad se amplía para incluir otras cuestiones no contempladas anteriormente.

Fernando Abós, CEO de Prosegur Security

HOME

Si bien la tecnología juega un papel crucial en el mundo actual, y los datos adquieren un carácter estratégico para un servicio adecuado, lo cierto es que **el factor humano es esencial para el éxito.** Competencias como el pensamiento crítico y creativo y la adaptabilidad son fundamentales. Tanto el conocimiento técnico como las habilidades humanas son indispensables, ya que una empresa con tecnología de vanguardia, pero sin personal capacitado en seguridad, no puede enfrentar los rápidos cambios y riesgos actuales. **Las personas, son, en definitiva, el eje central de la seguridad híbrida,** quienes ejecutan las labores, toman las decisiones y, en el día a día, los máximos responsables de los servicios.

Recordemos las inspiradoras palabras del **Teniente General Gan** sobre cómo elegir a un candidato para una expedición al polo norte: asumir nuestros errores sin buscar otros culpables, aceptar los errores de los demás sin rencor y tener capacidad de juntarse con otras personas para cambiar el mundo. Si nos fijamos, todos los criterios hacen referencia a la forma de trabajar, dando un peso extraordinario a las habilidades sociales. En el mundo de la seguridad esto se vuelve aún más crítico, pues **trabajar en equipo es indispensable** cuando damos respuestas a incidentes con multitud de personas implicadas en los servicios: vigilantes, analistas, operadores, etc. Veamos el papel de algunos de ellos.

VIGILANTE CONECTADO

El complejo entorno actual, caracterizado por la imprevisibilidad y la hibridación de amenazas, requiere un enfoque sistémico en la prestación de servicios de vigilancia. Así, el vigilante conectado a un iSOC ve potenciadas sus capacidades de respuesta gracias a una amplia gama de datos y tecnologías a su disposición, retroalimentando continuamente el flujo de información entre las partes.

Principales labores

- Vigilancia y patrullaje, tanto estático como dinámico.
- Protección y/o transporte de valores.
- Respuesta a emergencias o señales de alarma.
- Interposición de denuncias ante ilícitos.
- Recopilación de datos en tiempo real.
- Apoyo en labores de búsqueda y rescate de personas desaparecidas.
- Detección de sustancias no permitidas u objetos peligrosos.
- Control de accesos e identidad.
- Gestión de masas y flujos de personas.
- Colaboración con Fuerzas y Cuerpos de Seguridad del Estado.

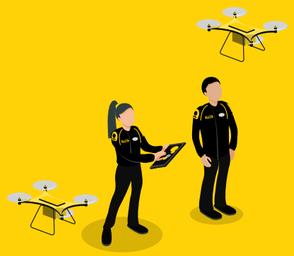
Tecnologías de empoderamiento

- Software de grabación y gestión de incidentes.
- Comunicación: smartphones y dispositivos como las radios de dos vías.
- Gestión de vídeo y acceso remoto a cámaras.
- Dispositivos de seguridad personal.
- Detección de intrusiones: alarmas, escaneo o sensores.
- Tecnología biométrica, de videovigilancia y GPS.

Competencias destacadas

- Competencias de seguridad: prevención y análisis de riesgos.
- Competencias tecnológicas: utilización de sistemas de vigilancia y comunicación para la seguridad.
- Competencias humanas: comunicación, empatía y situational awarenes.
- Competencias de autogestión: flexibilidad y resiliencia.

HOME
pág. 20



OPERADOR DE DRON

Un operador o vigilante empoderado mediante la tecnología de drones aporta una mejora a la eficiencia operativa al ser capaz de cubrir más terreno o superficie en un menor periodo de tiempo. Además, el incremento en la capacidad de respuesta o el alcance de la vigilancia aporta una diferenciación competitiva en términos empresariales, lo que mejora en última instancia la reputación de la compañía.

Principales labores

- Vigilancia y patrullaje aéreo (instalaciones deportivas, industriales, eventos, etc.).
- Vigilancia de perímetros en zonas de difícil acceso, tanto estática como dinámica.
- Respuesta a emergencias.
- Recopilación de datos en tiempo real.
- Apoyo en labores de búsqueda y rescate de personas desaparecidas.
- Vigilancia de infraestructuras críticas o sensibles.
- Automatización de rondas de vigilancia.
- Protección medioambiental como los incendios forestales.
- Detección de anomalías por la utilización de sensores (térmicos, presión, etc.).

Tecnologías de empoderamiento

- Plataformas de gestión de Operaciones de Drones desde centros de control.
- Coordinación de Operaciones entre centro de control y Piloto.
- Planificación de vuelos recurrentes.
- Implantación de capa IA.
- Monitorización y grabación de video en streaming desde SOCs.
- Control de horas de vuelo de Pilotos y Drones.
- Herramientas para el control de señales técnicas, mantenimiento y gestión de incidencias.

Competencias destacadas

- Competencias de seguridad: conocimiento en normativas sobre drones y capacidad en vigilancia aérea.
- Competencias tecnológicas: experiencia en operación y mantenimiento de drones.
- Competencias humanas: pensamiento analítico y situational awareness.
- Competencias de autogestión: flexibilidad y aprendizaje activo.

HOME

OPERADOR DE iSOC

A menudo conocido como guardián digital o TIER 1, el operador de un iSOC se configura como uno de los componentes de mayor relevancia para la correcta operatividad de las labores del centro de seguridad y profesionales derivados, como los vigilantes conectados y los operadores de drones. Así, su función se enmarca en la actuación por evento, seguimiento de indicadores y conductas en tiempo real para coordinar la respuesta ante incidentes, ya que típicamente son la primera fase de reacción ante un incidente de seguridad.

La rápida evolución en el ecosistema de la seguridad, tanto en los cambios que se producen en los incidentes de seguridad – creación de nuevos modus operandi para cometer hurtos en establecimientos, por ejemplo – como en el desarrollo tecnológico, exigen a los operadores del iSOC un aprendizaje activo en nuevas competencias de seguridad y tecnológicas.

Principales labores

- Monitorización en tiempo real de eventos, conductas y señales de seguridad.
- Triaje inicial de incidentes de seguridad.
- Respuesta inmediata ante funciones o incidentes básicos de seguridad.
- Comunicación con equipos especializados o vigilantes en terreno.

Tecnologías de empoderamiento

- Plataformas para la gestión y almacenamiento de contenido visual.
- Utilización de algoritmos de análisis visual avanzados y técnicas de inteligencia artificial para comprender y extraer información de vídeos.
- Sistemas para la coordinación y manejo eficiente de situaciones problemáticas.
- Herramientas y sistemas diseñados para identificar y prevenir accesos no autorizados o actividades maliciosas.
- Tecnologías para asegurar el cumplimiento normativo y gestionar posibles vulnerabilidades en sistemas y redes.

Competencias destacadas

Con el objetivo de garantizar un correcto pensamiento analítico ante cada evento que se produzca para garantizar la continuidad de negocio.

- Competencias de seguridad: conocimiento y capacidad en ciberseguridad y análisis de riesgos.
- Competencias tecnológicas: conocimiento y capacidad en ciberseguridad.
- Competencias humanas: comunicación y pensamiento analítico.
- Competencias de autogestión: trabajo en equipo y aprendizaje activo.

HOME

ANALISTA DE DATOS

En la actual era de los datos, el analista de datos se configura como un rol fundamental para la correcta operatividad de cualquier gran compañía, puesto que mediante técnicas avanzadas de recopilación y análisis se exploran y evalúan grandes conjuntos de datos con el objetivo de avanzar en la maratón del dato y la cadena del conocimiento –aquella en la cual los datos se transforman en información, que deriva en conocimiento para dar lugar a inteligencia–.

Principales labores

- Análisis de datos e indicadores para identificar tendencias y patrones de (in)seguridad.
- Recopilación e integración de información proveniente de diversos canales.
- Diseño, limpieza, preprocesado y modelado de datos para la elaboración de bases y dashboards.
- Identificación de patrones, tendencias y correlaciones entre los grandes volúmenes de información mediante técnicas de análisis y minería de datos.
- Desarrollo de modelos predictivos basados en datos cuantitativos y datos históricos.
- Identificación de indicadores de compromiso (IoC).
- Optimización de recursos y procesos corporativos.

Tecnologías de empoderamiento

- Uso de diversos lenguajes de programación para analizar y consultar datos en bases relacionales y no relacionales.
- Implementación de tecnologías para procesar y gestionar grandes volúmenes de datos mediante algoritmos y machine learning.
- Almacenamiento de información en sistemas adaptados para manejar estructuras flexibles de datos.
- Representación visual de datos mediante herramientas especializadas.
- Automatización de procesos y secuencias de trabajo para mejorar la eficiencia operativa.
- Integración de sistemas y transformación de datos para garantizar la interoperabilidad entre diferentes plataformas y formatos.

Competencias destacadas

- Competencias de seguridad: análisis de riesgos y privacidad.
- Competencias tecnológicas: dominio de herramientas, bases de datos, análisis y visualización.
- Competencias humanas: pensamiento crítico.
- Competencias de autogestión: aprendizaje activo.

HOME

INGENIERO DE INNOVACIÓN

La constante evolución y convergencia tecnológica deriva en la necesidad de mantener flujos de innovación en servicios de seguridad para cada cliente, con medidas hiper-personalizadas y adaptadas a cada necesidad en esta materia. Un ingeniero de innovación, con conocimientos transversales a multitud de departamentos,aporta una visión holística del panorama empresarial, siendo capaz de anticipar tendencias diversas y subirse a la cresta de la ola del progreso, fomentando una cultura de innovación que marque la diferencia respecto a los principales competidores.

Principales labores

- Colaboración y desarrollo de líneas innovadoras de productos de seguridad.
- Identificación de oportunidades de negocio.
- Manejo de la comunicación interna y externa.
- Formación interna sobre nuevos productos.
- Estrategia inicial de puesta de mercado.
- Investigación y análisis en tendencias de mercado y líneas tecnológicas.
- Implementar mejoras en la operatividad de la organización.
- Validación técnica, de producto y de negocio de las nuevas soluciones.
- Asesoramiento técnico en materia de innovación.
- Fomento de cultura empresarial basada en el progreso tecnológico.

Tecnologías de empoderamiento

- Utilización de tecnologías y herramientas de comunicación para facilitar la interacción y colaboración entre equipos.
- Implementación de sistemas de inteligencia artificial y visión por computadora para realizar tareas avanzadas de análisis y reconocimiento.
- Aplicación de tecnologías de robótica y drones para el desarrollo y control de dispositivos autónomos.
- Uso de sensores y plataformas de adquisición de datos para recopilar información del entorno.
- Implementación de sistemas de videovigilancia y biometría para la seguridad y autenticación de usuarios.
- Integración de tecnologías de GPS y realidad aumentada para mejorar la ubicación y la experiencia de usuario.

Competencias destacadas

- Competencias de seguridad: conocimientos y capacidades en gestión de riesgos y amenazas emergentes.
- Competencias tecnológicas: conocimiento en desarrollos emergentes y tendencias de mercado.
- Competencias humanas: curiosidad y capacidad de aprendizaje. Empatía y resiliencia. Habilidades de comunicación y persuasión, visión, liderazgo y empoderamiento de equipos.
- Competencias de autogestión: liderazgo y aprendizaje activo.

HOME

ANALISTA DE INTELIGENCIA

El analista de inteligencia aporta valor a toda la cadena empresarial, puesto que su función, siguiendo el clásico ciclo de inteligencia, se vincula con la recopilación de información, el análisis y evaluación de la misma para, finalmente, producir inteligencia accionable, es decir, que facilite la toma de decisiones. El analista de inteligencia se caracteriza por la capacidad para la anticipación de amenazas y eventos que impacten a diferentes niveles de una organización (personas, patrimonio, activos, infraestructuras, reputación o continuidad de negocio). Para un analista de inteligencia, especialmente en los campos de la seguridad, el crimen organizado, el terrorismo o el análisis de riesgos, es crucial contar con una variedad de herramientas y software que le permitan recopilar, analizar y presentar datos e información de manera efectiva y segura.

Principales labores

- Análisis de datos e indicadores para identificar tendencias y patrones de (in)seguridad.
- Recopilación e integración de información proveniente de diversas fuentes.
- Actualización o mantenimiento de bases de datos y dashboard a disposición del cliente.
- Preparación de informes y presentaciones que apoyen la toma de decisiones empresarial.
- Colaboración con equipos de respuesta a incidentes.

Tecnologías de empoderamiento

- Recopilación y extracción de datos: utilización de diversas fuentes abiertas y técnicas de web scraping para obtener información relevante.
- Análisis y visualización de datos: destacando los grandes volúmenes de datos y manejo de paquetes de análisis estadísticos mediante IA y machine learning.
- Herramientas de ciberinteligencia: empleo de software especializado en análisis forense digital y pruebas de penetración para proteger sistemas y redes.
- Gestión y análisis de información geoespacial: utilización de herramientas para trabajar con datos espaciales, cartografía e imágenes satelitales.
- Monitorización de redes sociales y análisis de comunidades: herramientas y softwares de social listening (SL) y social network analysis (SNA).
- Colaboración y gestión de proyectos: utilización de plataformas para organizar y comunicar eficazmente en proyectos y tareas.

Competencias destacadas

- Competencias de seguridad: análisis de riesgos, amenazas y vulnerabilidades.
- Competencias tecnológicas: dominio de herramientas de análisis de datos y fuentes de información diversas.
- Competencias humanas: pensamiento crítico y creatividad.
- Competencias de autogestión: trabajo en equipo, aprendizaje activo y flexibilidad.

HOME

pág. 25

PREVENTA Y COMERCIAL

El valor estratégico de un técnico preventa y comercial para la seguridad híbrida radica en su capacidad para mantener una visión sistémica de la organización y las necesidades de cada cliente, generando relaciones de confianza y apoyar la línea estratégica de la corporación. Tanto para mantener la operatividad de la compañía como para impulsar mejoras a largo plazo esta labor es fundamental.

Principales labores

- Adaptar los servicios de seguridad a las necesidades de cada cliente.
- Apoyo en la línea estratégica de la compañía.
- Investigación y análisis en tendencias de mercado.
- Análisis de necesidades y/o mejoras en procesos y servicios de seguridad.
- Implementar mejoras en la operatividad de la organización.
- Identificación de oportunidades de negocio.
- Generación de ingresos y desarrollo de relaciones de confianza con stakeholders.
- Participación en negociaciones y licitaciones.

Tecnologías de empoderamiento

- Plataformas para la gestión de clientes (CRM) para administrar y organizar las interacciones con los mismos, así como para gestionar información relacionada con ventas y marketing.
- Entornos de pruebas y simulaciones para realizar demostraciones y pruebas de sistemas en un entorno controlado antes de implementar cambios o lanzar productos al mercado.
- Herramientas para la creación y presentación de documentos técnicos.
- Sistemas para gestionar relaciones, colaboración y comunicación: permiten facilitar la interacción y colaboración entre equipos internos y externos.
- Recursos para obtener inteligencia de ventas y análisis competitivo.

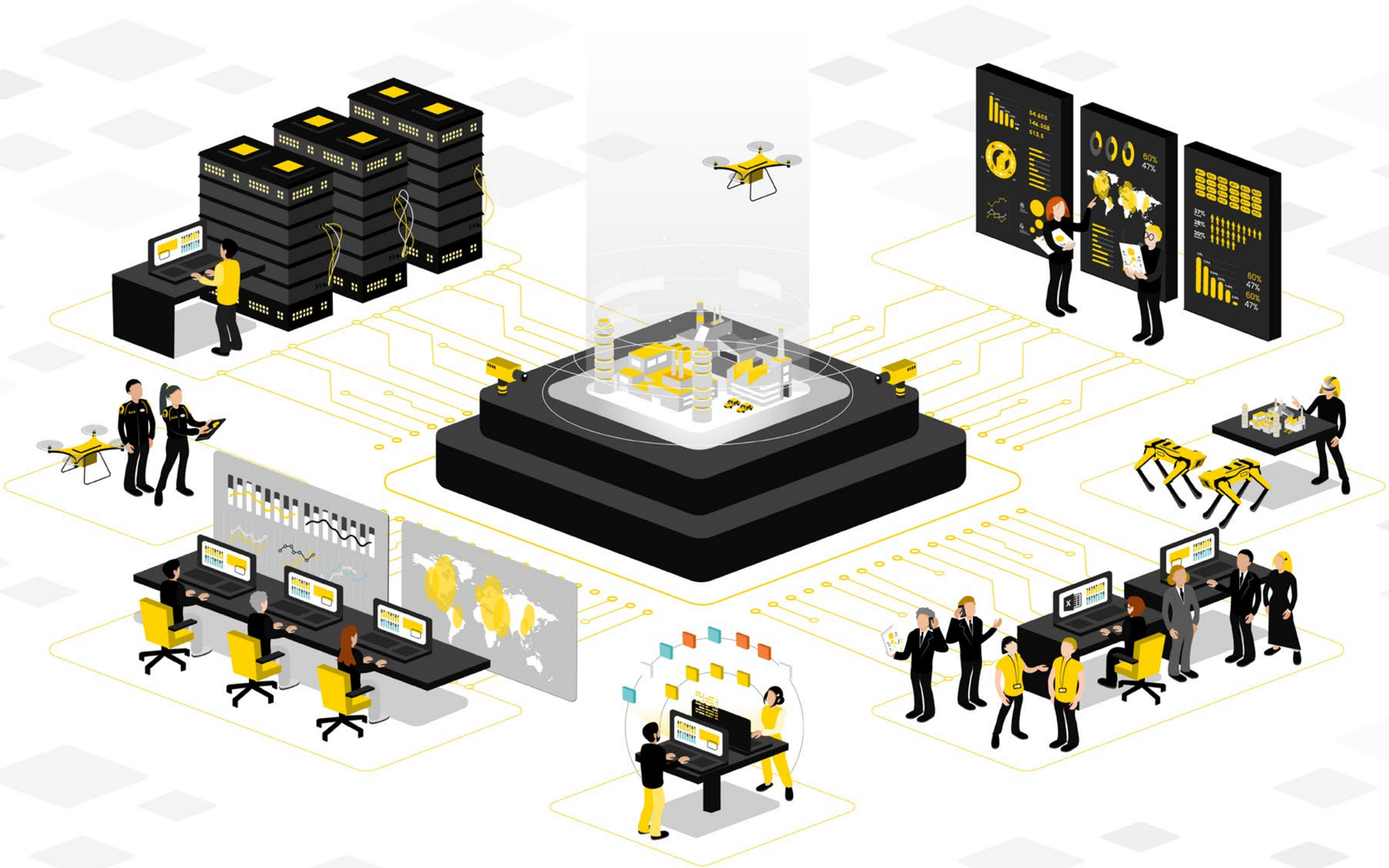
Competencias destacadas

- Competencias de seguridad: conocimiento en nuevos productos y servicios en el sector.
- Competencias tecnológicas: experiencia con herramientas de gestión de proyectos y clientes.
- Competencias humanas: negociación, comunicación y empatía.
- Competencias de autogestión: liderazgo y resiliencia.

HOME

Cuando hablamos de personas en seguridad híbrida, no se trata de un grupo o un puesto de trabajo, sino de **equipos de expertos con distintas competencias que se integran** para potenciar el factor humano de manera cohesionada con las tecnologías y los datos.

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.**



04

El liderazgo innovador **desde la experiencia**

HOME

01
Las personas como prioridad

02
Las competencias de los expertos en seguridad

03
Los profesionales de la seguridad híbrida

04
El liderazgo innovador desde la experiencia

04 EL LIDERAZGO INNOVADOR DESDE LA EXPERIENCIA

En Prosegur Research sabemos que son los equipos de expertos quienes llevan a las empresas al éxito, en su apuesta decidida por el propósito de lo que hacen.

El motor del mundo son las personas. Con ellas se transforman vidas y negocios, se hace un buen o mal uso de la tecnología y de los datos, y son quienes verdaderamente generan mejoras en la eficiencia y eficacia de todo tipo de servicios.

En el camino hacia el liderazgo innovador, el **factor humano** debe ser el centro de toda la organización porque es lo que aporta el ***mindset*** **o mentalidad de crecimiento,** desde donde evolucionar hacia formas y procesos con mayor agilidad, eficiencia y sostenibilidad. Una empresa será tan innovadora como lo sea el conjunto de sus empleados. Y como un sistema que se retroalimenta, recordando a Meadows, las **organizaciones con propósito y cultura de innovación atraerán a las personas con el mayor talento,** creatividad y capacidad de trabajo en equipo.

Desde el modelo de seguridad híbrida, el propósito y la cultura alinean sus tres elementos esenciales: personas, tecnologías y datos. Siendo la tecnología la gran palanca de cambio, el factor humano es quien aprovecha al máximo las tecnologías y datos en un entorno en constante evolución. Además, la contribución de los expertos se extiende más allá, aportando **inteligencia contextual y capacidad innovadora** a toda la cadena de valor de la organización.

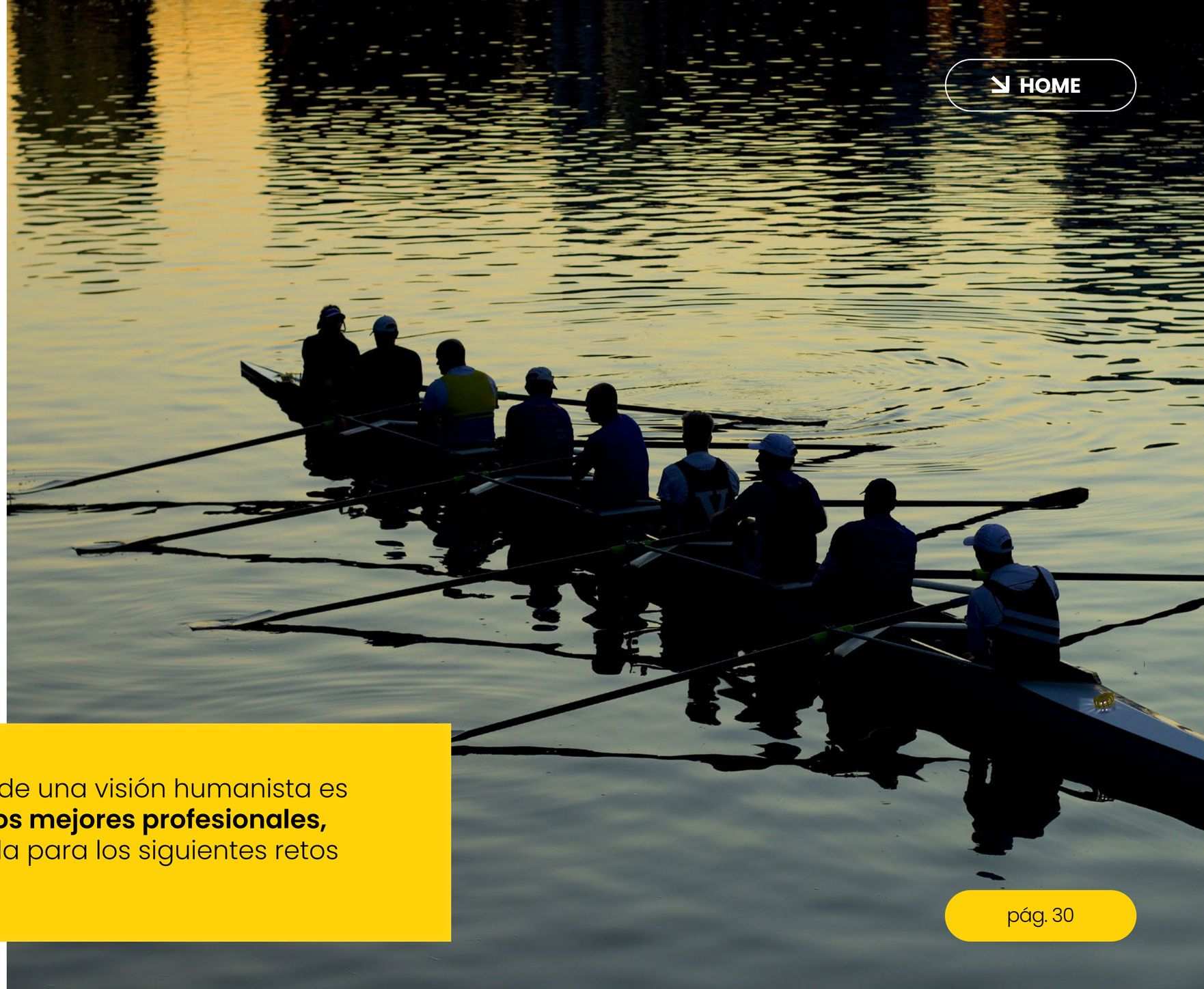
HOME

La seguridad híbrida se compone de **personas empoderadas** por la **tecnología** más innovadora que les permite hacer un uso estratégico de los **datos.**

HOME

Por este motivo, la **seguridad híbrida contempla las personas como prioridad,** de forma que la atracción y fidelización del talento son compromisos irrenunciables. Estos se pueden materializar en muy diversas acciones sobre sus empleados como programas de **formación continua y específica,** iniciativas de **diversidad** y **empoderamiento** o fomento de una buena comunicación interna, así como priorizando sus actividades desde **pilares humanistas.**

Prosegur, como empresa líder de seguridad global presente en los cinco continentes, cuenta con más de 170.000 empleados que **apuestan cada día por hacer del mundo un lugar más seguro,** posicionando a Prosegur como la **segunda mayor empleadora** de España. Para ello, como empresa internacional, **reinvierte más del 70% de su beneficio bruto en las personas,** principalmente en retribución del talento humano, que es donde radica la clave de su liderazgo innovador.



Invertir en liderazgo a largo plazo desde una visión humanista es lo que permite alcanzar el **éxito con los mejores profesionales,** que no es más que el punto de partida para los siguientes retos de futuro que afrontaremos juntos.

PROSEGUR
SECURITY

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

research@prosegur.com

www.prosegurresearch.com