PROSEGUR RESEARCH

Hybrid Security Series

Los SOC del futuro: hacia la integración **inteligente**

2023

PROSEGUR
SECURITY

PROSEGUR RESEARCH

Los SOC del futuro:
Hacia la integración inteligente

Este documento es **interactivo**

HOME

HOME

01

Contexto actual: dinamismo y oportunidad

01

CONTEXTO ACTUAL: DINAMISMO Y OPORTUNIDAD

Tras una pandemia global, conflictos bélicos y crisis económicas, políticas y sociales de diversa índole ha quedado patente que **el escenario en el que vivimos es complejo, con cambios disruptivos y nuevas amenazas de carácter híbrido** que se unen a las tradicionales, generando novedosas disrupciones a todos los niveles imaginables. A este respecto, la Agencia de la Unión Europea para la Ciberseguridad (ENISA) ha señalado, en su **horizonte 2030,** que las amenazas híbridas pueden suponer una multitud de potenciales actores y amenazas, con impactos derivados para las organizaciones y, en última instancia, la sociedad. Actualmente cualquier circunstancia, no importa el momento o el lugar, puede generar impactos sistémicos en cascada en compañías, industrias e incluso naciones con potencial desestabilizador muy amplio. **Este dinamismo genera nuevos desafíos y oportunidades** para las empresas, por lo que el sector de la seguridad no es una excepción ante el desarrollo global.

Ante este reto no **se puede vivir en el presente empleando los medios del pasado;** tampoco es suficiente adaptarse para sobrevivir y esperar a la siguiente ola de cambio: se requiere una visión innovadora para crear futuro junto con los avances de la sociedad.

Antes bastaba con percibir que algo estaba pasando para actuar de forma reactiva, con gran agilidad y coordinación ante cualquier alteración del entorno, ahora se requiere cierta capacidad de anticipación, como un *situational awareness* mejorado. El presente es solo lo que separa el pasado del futuro y en el momento actual es bueno reflexionar, escuchar y mirar donde no se ha puesto el foco antes para valorar nuevas formas de evolución y mejora. En este contexto, el científico botánico Stephano Mancuso destaca la increíble sofisticación con la que las plantas perciben el entorno que les rodea, con una sensibilidad de varios órdenes de magnitud superior a los animales. Esa extraordinaria capacidad de percepción les sirve para comprender si algo está cambiando en su entorno con mucha antelación. Y esto es precisamente lo que demanda el sector de la seguridad: **de reaccionar a anticipar, de la coordinación a la integración, del pasado al futuro.** Mejorar nuestras habilidades para entender algo tan esencial como es nuestro ecosistema requiere una revisión de nuestras formas de operar, nuestras fuentes y metodologías, y sobre todo de cómo vemos el futuro.

Solo entendiendo la evolución en las necesidades de seguridad de un mundo en cambio podremos anticipar las amenazas y mitigar los riesgos con una visión de sostenibilidad. Asumir este importante reto conlleva una profunda transformación, y en el sector de la seguridad, **uno de los elementos de mayor evolución en términos de seguridad es sin duda el Security Operation Center (SOC).**

HOME

02

Los SOC:
el cerebro a revisión

02

LOS SOC: EL CEREBRO A REVISIÓN

2.1.
Aproximación al concepto

El centro de operaciones de seguridad, o SOC por sus siglas en inglés, es una infraestructura en la que se centralizan las funciones de seguridad de una compañía para ofrecer servicios remotos a otras organizaciones basándose en una serie de **funciones y procesos básicos para los que necesita de tecnología avanzada precisa:** en primer lugar, soluciones de captura de datos en tiempo real sobre incidentes de seguridad concretos, que a continuación fluyen hacia los equipos de seguridad con el objetivo de formular decisiones críticas que den la respuesta más adecuada para cada situación y contexto de seguridad. Para ello, deben existir **plataformas tecnológicas dentro del SOC** que reciban y visualicen la información de manera constante. Tras una evaluación de la situación por parte de los profesionales presentes en el SOC, llamados operadores, una serie de acciones de mitigación serán activadas si se considera oportuno, las cuales se introducen en flujos de trabajo repetibles y medibles, para cuyo seguimiento se necesitan sistemas de gestión de incidentes.

Según **ENISA,** se deben diferenciar los centros de operaciones de seguridad (SOC) de los equipos de respuesta a incidentes de seguridad informática (CSIRT): mientras que el SOC ofrece servicios de detección y respuesta incidentes mediante la monitorización de información, el CSIRT se encarga de todos los aspectos

HOME

HOME

relacionados con los ciberincidentes, incluyendo la gestión de vulnerabilidades o la protección de servicios y operaciones centrales, entre otros.

Debido a la multitud de tareas, variables y fuentes que monitorizar y actividades empresariales que vigilar existen **diferentes tipos de SOC,** que se adaptan a las necesidades de cada compañía y proceso operativo concreto.

Es importante señalar que no todas las organizaciones cuentan con SOCs para poder gestionar sus operaciones y responder ante incidentes críticos, siendo una actividad empresarial usualmente subcontratada. De hecho, según algunos datos de Gartner, **para 2025 el 90% de todos los SOC estarán gestionados al menos parcialmente de forma externa** por proveedores de seguridad especializados, lo que se encuadra en la oferta de servicios de seguridad conocida como **Security-as-a-Service (SaaS).**

Atendiendo a la tipología de *Gartner,* se pueden distinguir diversas categorías principales:

1. **SOC virtual.** Sin instalaciones físicas asociadas, su componente es meramente reactivo a modo de respuesta ante incidentes.

2. **SOC especializado.** Se aportan infraestructuras físicas especializadas, con equipos cualificados para llevar a cabo las tareas a realizar.

3. **SOC distribuido.** Se suele asociar a proveedores de servicios de seguridad (MSSP, por sus siglas en inglés), juntando equipos dedicados y semi-dedicados a una determinada operación.

4. **SOC de coordinación.** Su función es coordinar otros SOCs y equipos, tratando de aportar expertise sobre una determinada tarea, por lo que no se asocia a operaciones rutinarias**.**

5. **SOC multifunción.** Con el objetivo de reducir costes, se aportan infraestructuras y equipos especializados en diferentes tareas.

2.2.
Evolución histórica

Los SOC se han adaptado, al igual que el sector de la seguridad, a los cambios del entorno y las necesidades operativas y de continuidad de negocio de las organizaciones. Históricamente se ha vinculado el SOC a los servicios de ciberseguridad, con el auge de las operaciones en el ciberespacio y la nube:

Figura 1
Antecedentes y evolución histórica de los Centros de Operaciones de Seguridad (SOC)
Fuente: Prosegur Research, 2023

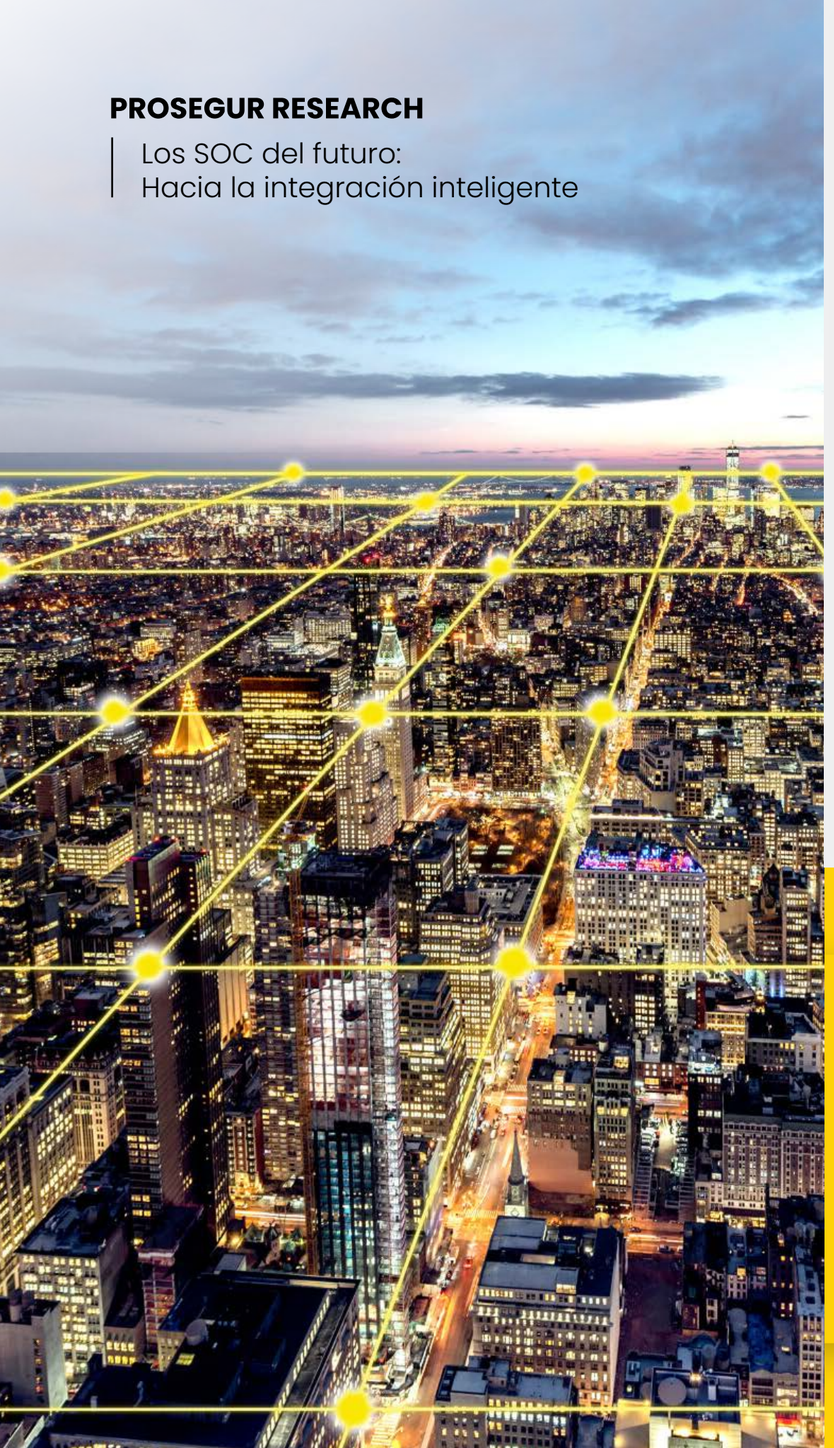
Conocidos como Network Operations Center (NOC), se asocian con el control de comunicaciones y códigos maliciosos tras el incremento de las redes informáticas y los activos digitales, si bien inicialmente su uso se vinculaba al ámbito público en zonas de conflicto. Se realiza el visionado incidentes físicos a través de cámaras localmente mediante el “Centro de Control”.

Se popularizan los servicios de carácter eminentemente reactivo de la mano de las grandes corporaciones multinacionales como las financieras, con el objetivo de detectar y responder ante intrusiones y amenazas de todo tipo, desde virus hasta incidentes físicos.

El NOC evoluciona y se popularizan los SOC hacia la detección de intrusos, las alertas de seguridad y protocolos de respuesta a incidentes. Se avanza en una mayor integración de los Centros de Control, ganando efectividad en la respuesta de incidentes.

Debido a la irrupción de la ciberseguridad como añadido de seguridad física a gran escala se incorpora un marcado componente de innovación tecnológica, avanzando hacia la proactividad, la monitorización de múltiples fuentes de información en tiempo real, la seguridad en la nube y la escalabilidad.

Desde finales de la década de 2010, los SOC están apostando por la proactividad y la monitorización basada en la automatización, inteligencia artificial y el big data, pasando de modelos reactivos a estratégicos, con multitud de sistemas integrados (SCADA, CRM, DLP, etc.), por lo que la protección de los servicios de seguridad y el SOC se configuran como parte fundamental de la estrategia empresarial.



Así, la evolución pasa irremediablemente de la detección y protección de activos hasta la **protección a múltiples niveles de todos los sistemas centrales y críticos de una organización.** La gran variedad de actores y de potenciales amenazas conlleva la necesidad de realizar reflexiones sobre los riesgos a los que se enfrenta una compañía en la actualidad y configurar consecuentemente los procesos de negocio que necesitan especial protección y monitorización. Esta tendencia se puede ver reflejada en los datos sobre el valor de mercado global de los SOC, que, según Allied Market Research, se situaba en 2021 en los más de cuatro mil millones de dólares, mientras que está previsto que alcance los ***diez mil millones de dólares para 2031.***

[1] Según ***DATAMINR.*** Key Considerations When Building a SOC.

2.3.
Características tradicionales

Todo SOC se basa en tres funciones fundamentales – preparación, monitorización y respuesta – para asegurar su correcto funcionamiento:

↘ HOME

1. **Respuesta inmediada a eventos críticos** y **preparación de su adecuada gestión**, mediante la concreción de un plan de continuidad de negocio, apoyado en protocolos y tecnologías fácilmente accionables en caso de eventos inesperados que afecten a las operaciones del negocio.

2. Es importante recopilar y **monitorizar** eventos mediante datos en tiempo real de diversas fuentes con el fin de activar las alertas relevantes en caso de que sea necesario actuar, entre las que se incluyen sistemas, redes y aplicaciones de los que dispone la organización, así como otras actividades que requieren de la presencia de vigilancia, como la gestión de identidades y accesos para asegurar la debida autorización a recursos críticos y/o lugares restringidos.

3. La existencia de protocolos avanzados, el entrenamiento de los equipos y sistemas de seguridad y el desarrollo de canales de notificación en masa son necesarios para ofrecer una **respuesta** adecuada ante un evento crítico con el fin de minimizar su impacto en el funcionamiento de la organización[1].

Paralelamente, **el SOC lleva a cabo una serie de procesos para asegurar un correcto flujo de trabajo,** como el análisis de vulnerabilidades de todos los sistemas, activos y operaciones a proteger; la investigación de los incidentes y análisis forense, con el objetivo de recopilar evidencias y tratar de prevenir futuras amenazas; y la optimización y mejora continuada de todos los procesos y procedimientos.

De esta forma, la gestión y resiliencia de los procesos de negocio se puede mejorar a través de los SOC gracias a la detección y la monitorización en tiempo real, la gestión de respuesta a incidentes, la evaluación y mitigación de riesgos, los planes de continuidad, el entrenamiento y la sensibilización. Así, los SOC tienen un **enorme potencial en el ámbito del business continuity,** que a su vez es una ventaja competitiva fundamental y refuerza la reputación de marca.

Como consecuencia, los SOC se configuran como un elemento de especial interés para la externalización y subcontratación de funciones de seguridad para multitud de compañías.

Figura 2
Funciones y elementos centrales del SOC

Fuente: Prosegur Research, 2023

03

El iSOC: liderando la transformación del sector

HOME

01
Contexto actual: dinamismo y oportunidad

02
Los SOC: el cerebro a revisión

03
El iSOC: liderando la transformación del sector

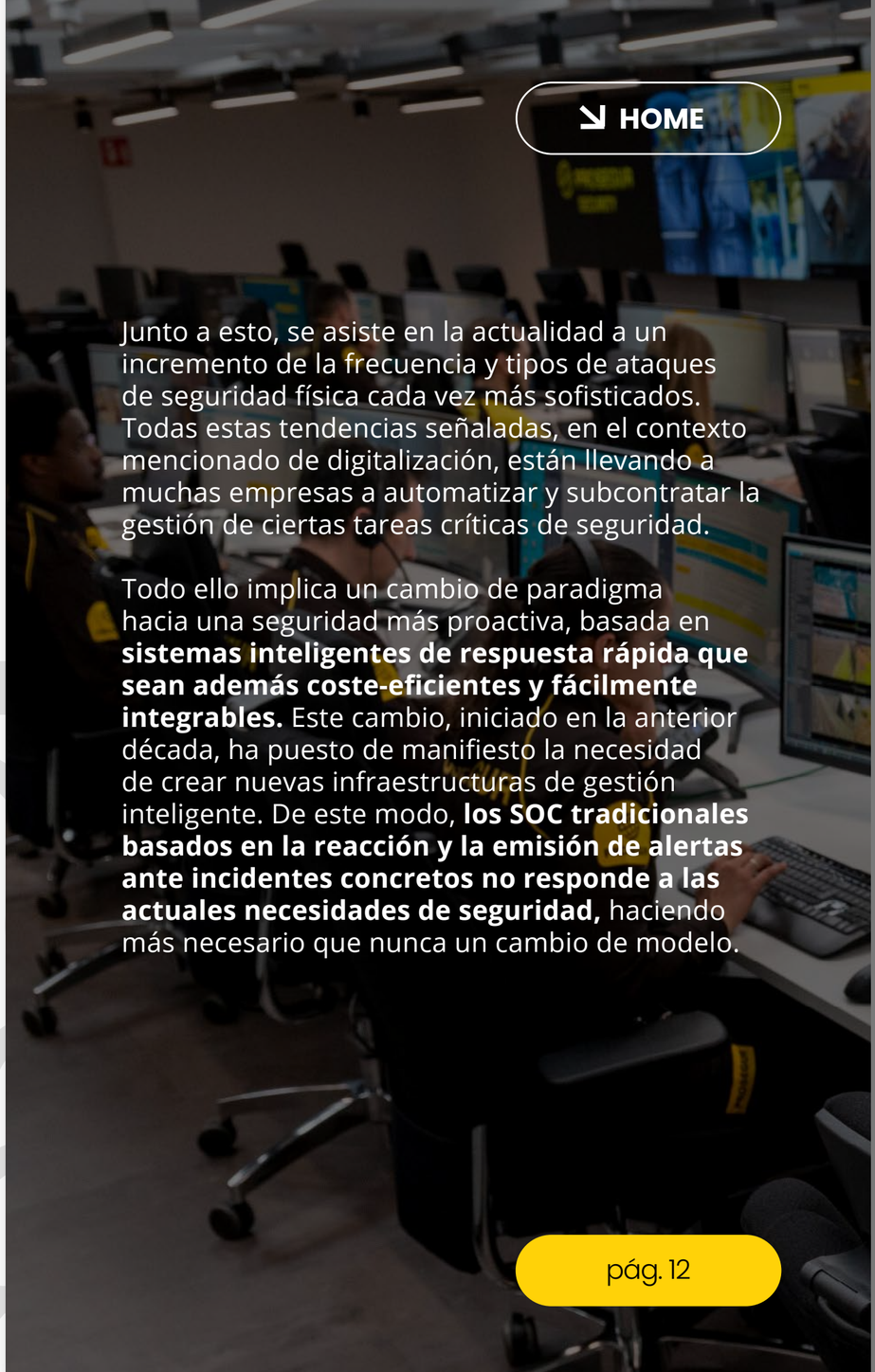
04
Aprender: la clave en la era del cambio

EL ISOC: LIDERANDO LA TRANSFORMACIÓN DEL SECTOR

3.1.
El futuro ya está aquí: por qué ya no basta con el SOC tradicional

En las últimas décadas se ha asistido a un crecimiento exponencial en la utilización de los desarrollos tecnológicos. Consecuentemente, **el mundo está cada vez más digitalizado y con ello el sector de la seguridad física,** por lo que las operaciones de seguridad dependen cada vez más de soluciones tecnológicas avanzadas, lo que Prosegur acuñó como **seguridad híbrida.** Todos los cambios en el ecosistema de la información empresarial, con el auge de plataformas, sistemas y nubes virtuales orientan hacia la acción más que hacia la reacción. Ya no es tiempo de dar respuesta a incidentes, sino que se trata de **crear procedimientos de gestión basados en la prevención proactiva** para los mismos.

Además, la **ampliación de la seguridad a todos los niveles,** incorporando a la gestión empresarial aspectos como la protección de los activos digitales, la reputación corporativa, el patrimonio, la incertidumbre jurídica o los efectos medioambientales en el entorno hace necesario revisar los protocolos, sistemas y servicios que se pueden ofrecer desde un SOC. Así pues, las tecnologías avanzadas de monitorización remota, el Internet de las Cosas y la interconectividad, la inteligencia artificial, los sensores, los robots o los drones, entre otras, son algunas de las soluciones cada vez más frecuentes en escenarios de seguridad.



HOME

Junto a esto, se asiste en la actualidad a un incremento de la frecuencia y tipos de ataques de seguridad física cada vez más sofisticados. Todas estas tendencias señaladas, en el contexto mencionado de digitalización, están llevando a muchas empresas a automatizar y subcontratar la gestión de ciertas tareas críticas de seguridad.

Todo ello implica un cambio de paradigma hacia una seguridad más proactiva, basada en **sistemas inteligentes de respuesta rápida que sean además coste-eficientes y fácilmente integrables.** Este cambio, iniciado en la anterior década, ha puesto de manifiesto la necesidad de crear nuevas infraestructuras de gestión inteligente. De este modo, **los SOC tradicionales basados en la reacción y la emisión de alertas ante incidentes concretos no responde a las actuales necesidades de seguridad,** haciendo más necesario que nunca un cambio de modelo.

3.2.
Del pasado SOC al presente y futuro iSOC

Para asegurar la continuidad de negocio es necesario identificar y cuantificar los procesos empresariales críticos, analizando para cada uno de ellos algunas medidas relevantes como tiempos críticos de operación en cada proceso, nivel de probabilidad de ataque, impacto operacional (económico, legal, comercial, reputacional) de potenciales interrupciones en cada unidad o tiempo de recuperación en caso de disrupción, entre otros.

Todo ello hace necesario que los SOC tengan una "i" diferencial: información de gran valor, de carácter internacional y con capacidad integradora e innovación desde una perspectiva inteligente. En un iSOC los datos masivos son transformados en inteligencia, que permite anticipar y mitigar riesgos, además de adoptar decisiones tanto internas como de los clientes que mejoren sus procesos productivos, aprovechando la experiencia para generar un procesamiento de alto nivel de complejidad, más similar al humano que nunca. Es así porque el análisis avanzado de datos va mucho más allá de la seguridad:

Proporciona las **claves para la protección de personas y bienes,** por ejemplo si las bandas organizadas desarrollan nuevos tipos de asaltos, qué productos o instalaciones son los nuevos objetivos, las zonas más calientes o los movimientos sospechosos en los perímetros, entre otros muchos.

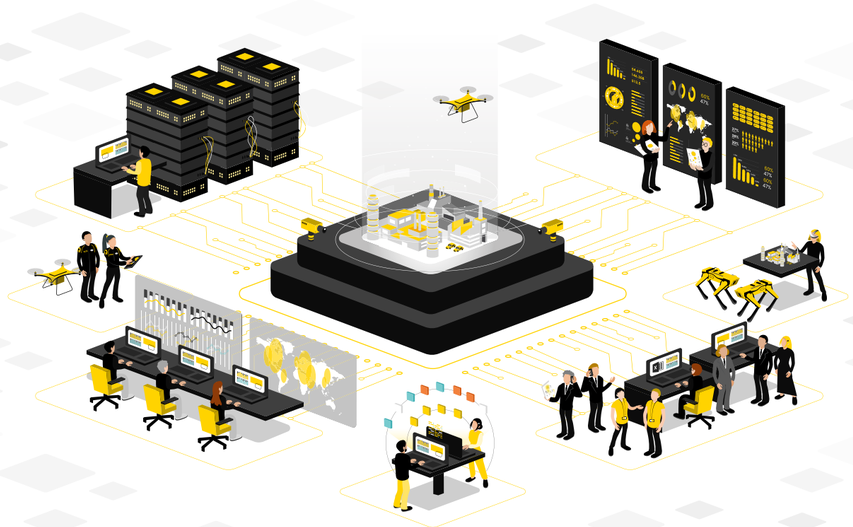
Genera cuadros de mando a disposición de los clientes que les permiten mejorar su gestión corporativa: por ejemplo, sobre el seguimiento de medidas de seguridad laboral o de gestión medioambiental, del sistema logístico para evitar fraudes o accidentes o la respuesta del público a diferentes estrategias de venta, por nombrar solo algunas.

Cubre las necesidades de seguridad adaptadas a los requerimientos de cada sector, servicio, cliente o personas afectadas, **customizando las soluciones** pero sin la pérdida de capacidad de automatización de procesos y de mejora continua.

En resumen, cimentado sobre la base de la ***seguridad híbrida,*** **en el iSOC las soluciones se gestan mediante estrategias operativas sofisticadas basadas en el funcionamiento cerebral.** Así, el iSOC es el cerebro del modelo, permitiendo conocer de forma muy ágil y ajustada a la realidad lo que ocurre en el mundo y hacerlo, además, de forma anticipada para impulsar la eficiencia en las respuestas.

HOME

> "A diferencia de los SOC tradicionales, que trabajan en el presente, los iSOC están orientados al futuro."
>
> **Fernando Abós, CEO de Prosegur Security.**



3.3.
Qué aporta el iSOC

En los últimos años las crecientes amenazas de seguridad física, cibernética y reputacional, entre otras, están impactando en la continuidad de negocio de las organizaciones y con ello causando graves pérdidas económicas y dañando su imagen corporativa, a pesar de que según los estudios de Ontic **el 55% de los directivos no son conscientes de las amenazas de seguridad física sobre su organización ni de su impacto en la continuidad de negocio.** No obstante, progresivamente las compañías están empezando a ver la seguridad no como una fuente de costes, sino como un activo organizacional valioso.

Por otro lado, la reciente aceleración de la innovación tecnológica y la conectividad implica que sea más fácil y más barato contratar o desarrollar servicios de seguridad, no solo para las funciones tradicionales, sino también para la monitorización de cualquier proceso organizacional del día a día a gran escala. Así, se debe considerar que, si bien el diseño de servicios de seguridad desde un iSOC depende de los objetivos y el perfil de riesgo de cada organización, siempre se basa en **información en tiempo real para tomar decisiones informadas, en analítica de datos y en análisis de amenazas** de cara a diseñar acciones de mitigación apropiadas, creando sinergias de comunicación y apoyo entre diversos equipos y aprovechando sistemas tecnológicos integrados.

Por tanto, a la hora de asegurar procesos de negocio es importante adoptar una **gestión proactiva de riesgos** que aspire a crear resiliencia organizacional, integrando todos los aspectos relevantes dentro de una política de seguridad general holística ante amenazas híbridas. Ahora bien, existen amenazas de difícil gestión, como los ataques con arma de fuego, el riesgo de secuestro a directivos o la combinación de amenazas tradicionales con nuevos componentes tecnológicos, lo que necesariamente deriva en la relevancia de la integración de nuevas tecnologías en los iSOC y en la constante mejora todos los procesos y operativas que lo componen.

Si el iSOC es el centro neurálgico de las operaciones, integrar de forma adecuada e innovadora todos sus elementos – personas, tecnología y datos –, comprender el ***valor estratégico del dato*** en la actualidad y estar al día con las **últimas innovaciones tecnológicas en el sector** se vuelve un asunto crítico.

HOME

Todo ello hace que el valor del iSOC redunde en su capacidad de anticipación de amenazas, pues está diseñado para evolucionar de forma constante como respuesta a un mundo en cambio y aprendiendo de su propia experiencia: aprovechando el know-how de los expertos que trabajan allí, innovando constantemente en sus herramientas tecnológicas y haciendo un uso estratégico de los datos, tanto internos como externos, generando inteligencia accionable para tomar decisiones estratégicas, gestionando la incertidumbre y adelantándose a los desafíos de seguridad.

Las grandes cantidades de volúmenes de datos y su difícil gestión para **obtener insights accionables** para las empresas en la actualidad se configura como un importante reto para las compañías. Para ello, se deben contar con los últimos desarrollos tecnológicos en materia de seguridad e integrar la información de manera estratégica para aprovechar el valor de los datos. Es por este motivo que un SOC se convierte en un auténtico iSOC cuando el nivel de **integración de todos sus elementos** es el máximo y responde a una forma de trabajar y de ver el servicio de la seguridad como un traje a medida. Los datos que la tecnología y la experiencia humana transforman en conocimientos son, pues, el principal activo: todo el equipo, hasta el último vigilante, está en permanente contacto con la información o los técnicos del iSOC para definir la respuesta adecuada ante cualquier incidente.

El iSOC debe estar preparado para el presente y el futuro y, por lo tanto, tiene que ser revolucionario y transformador y preparar para el cambio a cada elemento del modelo de seguridad híbrida. Más allá de las tres fases tradicionales (preparación, monitorización y respuesta), **la incorporación de sistemas tecnológicos en el iSOC facilita y capacita diferentes funciones de seguridad:**

Ingesta de datos de múltiples fuentes a gran escala

1. y que permiten a los expertos la elaboración de insights accionables, es decir, la posibilidad de llevar a la práctica el resultado del flujo de trabajo.

Detección de eventos de seguridad de forma rápida y precisa

2. normalmente mediante el uso de analítica con machine learning y computer vision.

Anticipación de eventos de seguridad

3. con el objetivo de dirigir de forma proactiva la atención humana y facilitar el proceso de respuesta apropiado.

Automatización de tareas rutinarias

4. permitiendo acelerar las principales funciones diarias realizadas dentro del SOC, como la detección y contención de amenazas.

Organización de los datos

5. para conectar todos los elementos dentro del SOC entre sí y con elementos externos para fortalecer la preparación ante la evolución constante de amenazas.

Recomendación de acciones

6. individuales o protocolos concretos adaptado a cada uno de los operadores y clientes.

Investigación y priorización de incidentes

7. para asegurar una respuesta rápida y eficaz. Mediante la gestión de alertas de riesgos se puede reducir el “ruido” de las alarmas falsas o irrelevantes y mediante analítica de datos se puede también automatizar la recolección y agrupación de incidentes para facilitar la respuesta.

Colaboración y comunicación en tiempo real

8. de forma integral y coordinada mediante soluciones basadas en datos que prioricen la información estratégica.

HOME

Gestión de incidentes

9. para lo cual los equipos humanos del SOC deben contar con protocolos, documentación, comunicación directa e información detallada facilitada por sistemas avanzados, como analítica de vídeos en tiempo real.

Reporting

10. mediante herramientas que faciliten el control de procesos de seguridad y permitan medir su eficacia de forma constante y rápida sin recurrir a diversas plataformas, lo que resulta especialmente útil en tareas de compliance y en la consecución de objetivos empresariales.

HOME

3.4.
Los tres ejes del iSOC: personas, tecnologías y datos

Como se ha visto, el iSOC se configura como el auténtico paradigma de la integración inteligente de la seguridad a todos los niveles, integrando información cualitativa y cuantitativa en tiempo real obtenida de una enorme diversidad de fuentes tanto internas como externas: humanas (HUMINT), públicas (OSINT) y tecnológicas (TECHINT).

Gracias a esto, la visión holística de lo operativo aporta inteligencia contextual a la perspectiva estratégica, y desde una sofisticada estrategia se pueden tomar las mejores decisiones operativas y para la continuidad de negocio. Esto, a su vez, supone también la integración de safety y security, pues permite atender tanto riesgos derivados de eventos fortuitos (accidentes, desastres naturales o daños ambientales) o de actos negligentes como aquellos de naturaleza intencionada (como robos, intrusiones, vandalismo y agresiones, entre otros).

En consecuencia, el iSOC se enmarca como cerebro de la seguridad híbrida, permitiendo la materialización de sus elementos interrelacionados: expertos en seguridad empoderados con tecnologías innovadoras que hacen un uso estratégico de los datos, y pasando de un plano conceptual a la práctica del mundo real.

El modelo de seguridad híbrida se aplica de forma diaria y cotidiana en el iSOC mediante las personas, las tecnologías y los datos de sus clientes, pues protegerlos es su auténtica razón de ser. Por eso, el iSOC es el cerebro en el cual se recibe, procesa y analiza toda la información y datos de valor para ofrecer soluciones de seguridad innovadoras y eficientes.

Por este motivo, el paso del SOC al iSOC en el marco de la seguridad híbrida es un proceso de transformación en el presente que mira al futuro: no se trata de plantear como será el iSOC en el mañana, sino analizar el mundo desde el iSOC del futuro, que anticipe riesgos y amenazas y que nos permita dar respuesta hoy.

Nuestro modelo de seguridad para un **mundo híbrido**

Fuente: Prosegur Research, 2023.

HOME

A Personas

La integración y la incorporación de las nuevas tecnologías a múltiples industrias está suponiendo que las habilidades necesarias ya en la actualidad están cambiando de forma veloz. Ello no quiere decir que las aptitudes técnicas hayan dejado de tener valor, sino que las competencias digitales y las habilidades más puramente humanas están adquiriendo especial protagonismo. De esta manera, la interacción con nuevos desarrollos tecnológicos, la capacidad de aprender nuevos conocimientos y la autogestión o la resiliencia se han convertido en habilidades fundamentales en un **entorno laboral en constante evolución**, como lo puede ser el sector de la seguridad y las novedades que requieren los iSOC. Así, desde Prosegur estamos convencidos de que para operar en este mundo **las competencias humanas son absolutamente fundamentales e insustituibles,** por lo que se debe buscar el empoderamiento de las habilidades de los profesionales mediante la palanca de cambio que constituye la tecnología.

Competencias digitales

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

Competencias humanas

Como la resolución de problemas complejos, el pensamiento crítico, la creatividad, la influencia social, 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 contínuo: la resiliencia, la tolerancia al estrés y la flexibilidad.

pág. 17

B Tecnología

Sabiendo que los sistemas tecnológicos juegan un papel fundamental en el iSOC actual, es realmente importante diseñar e implementar un iSOC considerando en detalle todos sus elementos siempre desde una perspectiva de **interoperabilidad e interconectividad.** Para ello, el iSOC se basa en tecnologías que estén claramente testadas y sean eficientes, lejos de los hype tecnológicos habituales:

Tecnologías que actúa en el **entorno físico** tanto para ejecutar tareas como para enviar información: cámaras, sensores, drones, alarmas, redes y sistemas, robótica, etc.

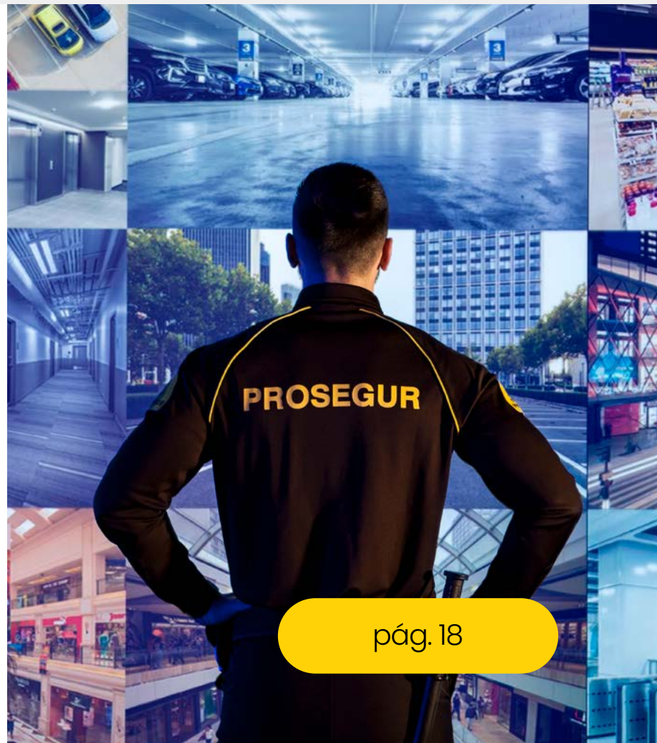
Tecnologías utilizadas para el tratamiento y **análisis de información y el apoyo en la toma de decisiones:** inteligencia artificial, machine learning, procesamiento del lenguaje natural, simuladores virtuales, modelos GIS, cloud computing, etc.

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: Genzai, POPS, Connect.

- **GENZAI** una plataforma que gestiona las cámaras de videovigilancia como dispositivos IoT (Internet de las Cosas) procesando así imágenes y datos con un algoritmo de inteligencia artificial avanzada. Así, el iSOC cuenta con tecnología inteligente conectada, lo que nos permite tener una comprensión amplificada del entorno a través de GENZAI. La automatización y protección autónoma que caracteriza a esta herramienta permite anticipar y mitigar riesgos a través de la integración de todas las tecnologías desplegadas en cada servicio.

- **POPS** es la aplicación con la que cada vigilante registra la información relevante de las novedades e incidencias que se producen en las instalaciones del cliente, permitiendo un registro en tiempo real y adaptado a los requerimientos del mismo, lo que dota a cada profesional de un mayor conocimiento de las necesidades del negocio de cada compañía. Contar con profesionales expertos conectados en todo momento gracias a POPS nos permite capturar datos contextualizados y categorizados para una respuesta más eficiente y efectiva. Además, sus habilidades y capacidades se ven potenciadas por la tecnología y la información, para tomar las mejores decisiones ante todo tipo de incidentes.

- **CONNECT** es la plataforma que permite al cliente la visualización de todo tipo de datos en tiempo real sobre lo que ocurre en su negocio. Además, Prosegur Connect se adapta a cada cliente, personalizando novedades, tareas y registros en función de sus necesidades. Emplear la información de manera estratégica para anticipar y adaptar los posibles sucesos para distribuir adecuadamente los recursos aporta un valor extraordinario para el negocio de cada cliente de forma única y exclusiva.



HOME

C Datos

El aprovechamiento estratégico de los datos deriva de la integración de todas estas fuentes trabajadas por los mejores expertos en seguridad y las más innovadoras tecnologías aplicadas.

Dentro del iSOC existen multitud de sistemas integrados, muchos de ellos accesibles de forma individual por cada analista u operador, quien está conectado normalmente a una serie de sistemas corporativos y de seguridad, además de recibir insights de una serie de fuentes en tiempo real, tener acceso a diversas redes de comunicación internas y externas, a numerosas herramientas de seguridad y soluciones de emergencia y apoyo.

Combinar la tecnología punta y la excelencia profesional para un procesamiento inteligente de datos es lo que nos permite gestionar in situ y a distancia los servicios de seguridad y los procesos empresariales de nuestros clientes. Los datos masivos son transformados en inteligencia, que permite anticipar y mitigar riesgos y un flujo constante de retroalimentación entre lo operativo y lo estratégico que facilita la mejor toma de decisiones tanto internas como de nuestros clientes.

En resumen, **el iSOC se configura como el paradigma de la integración de fuentes muy diversas, dando lugar a este concepto de la seguridad híbrida**. Así, los datos de entrada (inputs) de vigilantes, sensores, alarmas y cámaras, por nombrar solo algunos, son captados a través de numerosos dispositivos, para después ser procesados y poder ofrecerse (outputs) mediante nuestras plataformas únicas (POPS, Genzai y Connect) en forma de dashboards, acciones de mitigación, informes, alertas o recomendaciones, mejorando la inteligencia competitiva, los productos y los servicios.

04

Aprender: la clave en la era del cambio

HOME

APRENDER: LA CLAVE EN LA ERA DEL CAMBIO

Como en el iSOC, la diversidad y el dinamismo deben ser parte de toda la compañía donde se enmarca, de forma acompasada con la evolución de la sociedad y el entorno donde opera. Esta visión integrada e inteligente en el mundo permite dar paso a una nueva era de impulso a **la honestidad, el trabajo en red y el talento:** un salto a lo auténtico, dando respuesta desde su razón de ser. Lo que define a una organización no es su nivel de innovación tecnológica, su tamaño en empleados y facturación o sus modernas oficinas, es su propósito: ser capaz de identificarse más con el hacia dónde va que con el desde dónde viene.

Como dice **Mariana Mazzucato,** el mayor problema actualmente es la inercia; desde Prosegur Research estamos convencidos de que el desafiante futuro que se presenta, desbordado de cambios e incertidumbres, solo se podrá afrontar con un auténtico carácter de **aprendizaje sistémico,** siguiendo el interesante enfoque de **Donella Meadows** para cultivar resultados positivos. Trasladar esto el ámbito empresarial no es sencillo; en palabras de **Enrique Dans,** "algunas empresas están locas por hacer lo que hacían y se la van a pegar; otras asumen que es un aprendizaje y que el talento irá allí donde le den libertad", y podemos añadir, esa libertad nacerá de la **transparencia, la flexibilidad y la diversidad** que emane de la cultura empresarial.

Transparencia en las organizaciones para abandonar la adicción de ir en automático; pedir y rendir cuentas para compartir los avances y también las potenciales mejoras, resistir la tentación de buscar certezas, asumiendo los actuales tiempos de incertidumbre.

Flexibilidad para ir más allá del papel, superar las constricciones de las directrices e incorporar pequeños cambios de forma sistemática y grandes cambios cuando sean disruptivos; reservar espacios para pensar y tiempos para actuar.

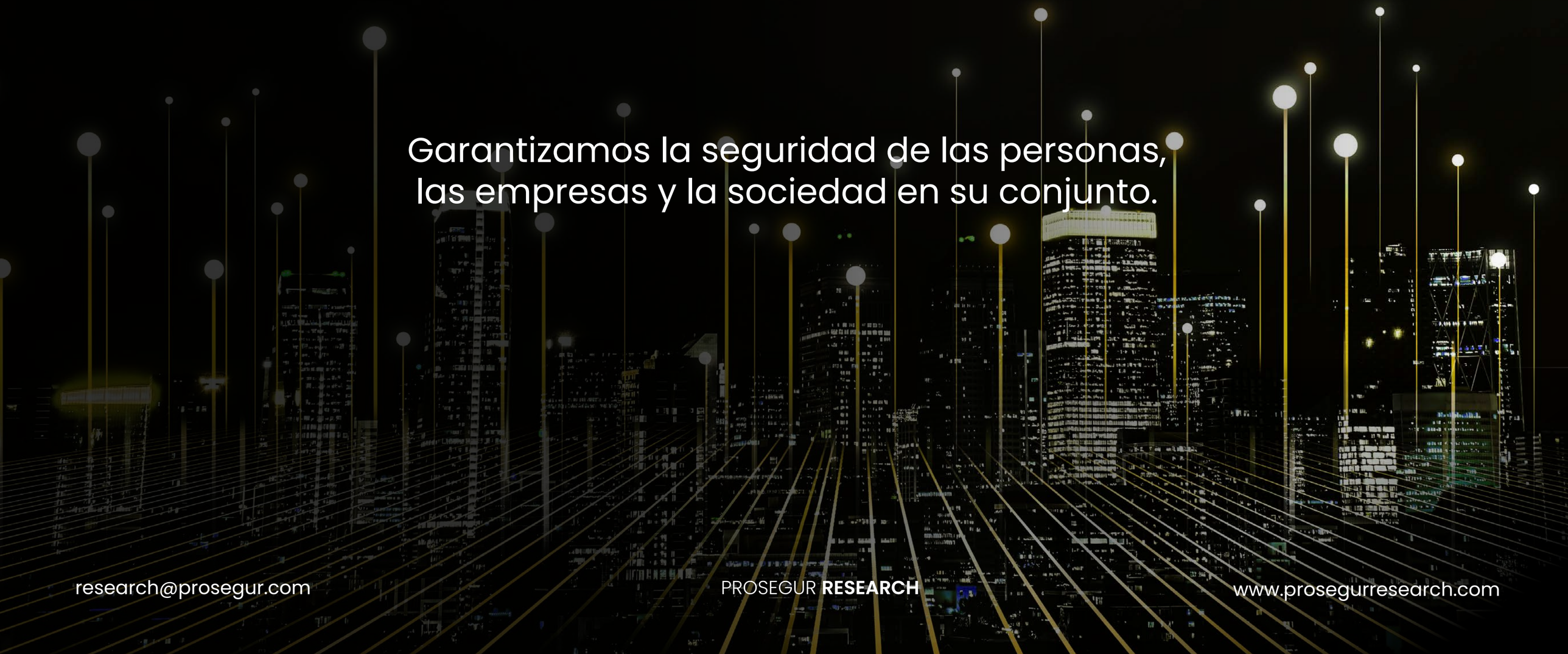
Diversidad en equipos, pero también para abandonar la monogamia ideológica, exponernos a otros enfoques y practicar la promiscuidad en materia de aprendizaje, debemos ser capaces de relacionar disciplinas aparentemente no afines y tener el valor de analizar nuestras propias capacidades, de ver lo que nos falta y e incorporarlo de manera natural.

El auténtico reto para las organizaciones será absolver todo este aprendizaje en primera persona y transformarlo en algo útil para toda la estructura, generando entornos propicios de cadenas de transmisión de cambio; lo que ***Xavier Marcet*** denomina "un ecosistema de aprendizaje potente". Por ello, el paradigma de la integración inteligente es algo que supera el concepto de iSOC, solo aquellas empresas que entiendan su importancia y abracen la **innovación como mentalidad de cambio con base en el aprendizaje formarán parte del futuro.**

Libros que nos han inspirado

- Misión economía
- Designing and Builing Security Operations Center
- AI 2041: Ten Visions for Our Future
- Thinking in Systems
- Link: How Decision Intelligence Connects Data, Actions, and Outcomes for a Better World
- The coming wave
- Todo va a cambiar: tecnología y evolución: adaptarse o desaparecer
- The future of national intelligence
- Next Gen Securlty Operations Center: From Concept to Reality
- Management humanista
- How to research trends
- Modern Security Operations Center

PROSEGUR
SECURITY



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

research@prosegur.com

PROSEGUR **RESEARCH**

www.prosegurresearch.com