evolutio
Empowering secure AI

Google Cloud

Del SOC tradicional al SOC agéntico

Cómo Evolutio y Google Cloud transforman las operaciones de seguridad

Índice

Introducción El tiempo de respuesta se ha convertido en la variable crítica

01 Defender cuando el atacante opera a velocidad de máquina

02 Por qué el SOC tradicional ha alcanzado su límite

03 De la automatización tradicional al SOC agéntico

04 La arquitectura del SOC agéntico

05 Siete sistemas coordinados y tres desarrollos diferenciales de Evolutio

06 Evolutio y Google Cloud. Un partnership que potencia el SOC agéntico

07 Un incidente de principio a fin

08 Control humano confianza y soberanía

09 Del rendimiento técnico al impacto empresarial

10 Cómo empezar. Del primer caso de uso a la autonomía progresiva

11 Conclusiones

Introducción

El **tiempo de respuesta** se ha convertido en la variable crítica

Los **centros de operaciones de seguridad** se diseñaron para recoger señales, correlacionarlas y trasladar los casos relevantes a un equipo de analistas. Ese modelo sigue siendo necesario, **pero ya no resulta suficiente** para un entorno en el que los atacantes automatizan tareas, comparten accesos en segundos y explotan vulnerabilidades antes de que exista un parche.

La presión no procede únicamente del **volumen de alertas**. El volumen de alertas es solo una parte del problema. Cada investigación exige consultar telemetría, inventarios, identidades, inteligencia de amenazas, tickets anteriores y procedimientos internos.

El analista debe reconstruir lo ocurrido y decidir qué hacer **con información repartida entre sistemas** que no siempre comparten contexto. Cuando cada paso depende de trabajo manual, el tiempo se acumula precisamente donde el atacante busca avanzar con mayor rapidez.

La **Inteligencia Artificial permite delegar parte de ese trabajo** a agentes especializados. Estos agentes pueden reunir evidencias, formular hipótesis, consultar fuentes y preparar una respuesta.

Para **convertir esa capacidad en un servicio de seguridad**, necesitan límites, fuentes autorizadas, trazabilidad y conocimiento del entorno protegido.

La cuestión no consiste en automatizar todo, sino en asignar a cada tarea el nivel de autonomía adecuado.

La clave no es automatizarlo todo: es dar a cada tarea el nivel de autonomía adecuado, con contexto, límites y trazabilidad.

El objetivo de este documento es desarrollar el modelo de SOC agéntico de Evolutio.

La base tecnológica es **Google Security Operations**, una plataforma cloud-native que unifica SIEM y SOAR, complementada por **Gemini** y por la inteligencia de **Google Threat Intelligence**, **Mandiant** y **VirusTotal**.

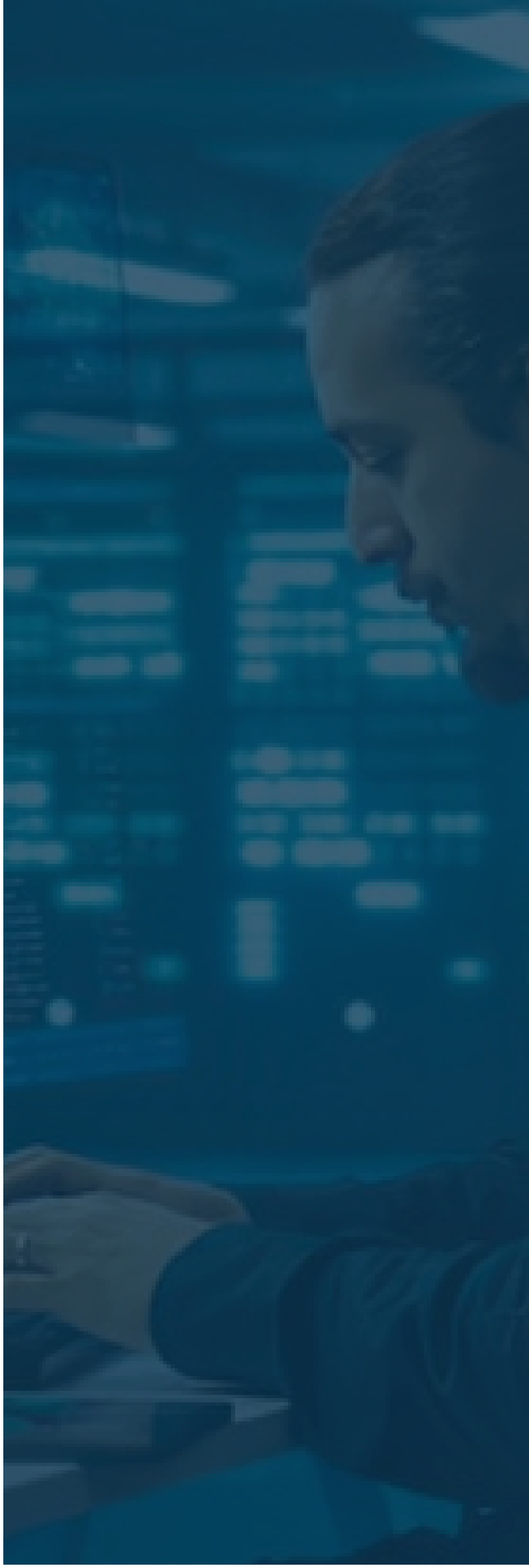
Evolutio integra esas capacidades en una arquitectura de siete sistemas, con tres desarrollos propios:

- Contextualización
- Inteligencia
- Management

Contextualización y **Management** constituyen el núcleo que conecta la capacidad general de los modelos con el conocimiento y los procesos de cada cliente; **Inteligencia** añade vigilancia externa y búsqueda proactiva para anticipar amenazas y mejorar la cobertura defensiva.

A lo largo de este documento seguiremos un caso concreto: **una transferencia inusual de datos hacia un dominio externo**. Puede ser un proceso autorizado o el inicio de una exfiltración. Veremos por qué a un SOC tradicional le cuesta saberlo a tiempo y cómo lo resuelve, paso a paso, el modelo agéntico.

El modelo ya funciona en el SOC de Evolutio. **Ha recibido el premio al Mejor Proyecto de IA en los Premios Byte TI 2026** y, en las operaciones medidas, **ha reducido hasta un 50% el tiempo de triaje y hasta un 40% el tiempo medio de resolución**.



01 Defender cuando el atacante opera **a velocidad de máquina**

De las horas a los segundos

Mandiant ha observado un cambio significativo en la colaboración entre grupos criminales. En las investigaciones recogidas en **M-Trends 2026**, la mediana entre el acceso inicial de un grupo y el traspaso a un segundo actor **cayó de más de ocho horas en 2022 a 22 segundos en 2025**.



El SOC debe valorar las señales tempranas antes de que el atacante convierta un acceso inicial en una operación de mayor impacto.

Este dato no mide movimiento lateral dentro de una red. Mide la **velocidad** con la que un acceso puede pasar de un actor especializado en obtenerlo a otro preparado para explotarlo.

La consecuencia operativa es directa. **Una infección que parece limitada puede ser la primera fase de una operación de ransomware o extorsión.** El SOC necesita valorar las señales tempranas antes de que el segundo actor despliegue herramientas, escale privilegios o afecte a los sistemas de recuperación.

Explotación acelerada de vulnerabilidades

Los **exploits** fueron el vector inicial **más frecuente por sexto año consecutivo** en las investigaciones de Mandiant y representaron el 32% de los casos analizados en 2025. El tiempo medio estimado entre la disponibilidad de una corrección y la explotación **cayó hasta menos siete días**. Un valor negativo indica que, de media, la explotación comenzó antes de que hubiera un parche disponible.

El panorama de acceso inicial no se limita a las vulnerabilidades. M-Trends 2026 situó el **vishing** en el 11% de las infecciones observadas. El compromiso previo representó el 10% de las intrusiones globales y alcanzó el 30% en las operaciones de ransomware. Esta combinación obliga al SOC a correlacionar explotación técnica, abuso de identidades y señales de ingeniería social.

La gestión de vulnerabilidades y la operación del SOC deben trabajar como un ciclo conectado. Cuando la inteligencia confirma explotación activa, el equipo no puede esperar a que termine el proceso ordinario de parcheado. Debe identificar los activos expuestos, reforzar la vigilancia, desplegar medidas compensatorias y buscar evidencias de actividad.

La IA amplía la capacidad del atacante

Google Threat Intelligence Group ha documentado una transición desde el uso de modelos como asistentes hacia su incorporación en flujos ofensivos más amplios. Los actores los utilizan para reconocimiento, ingeniería social, investigación de vulnerabilidades y desarrollo de malware. En 2026, **GTIG** y **Mandiant** observaron además el uso de marcos agénticos de pruebas de penetración en intrusiones reales.

La mayoría de los incidentes sigue aprovechando fallos conocidos: credenciales, configuraciones débiles, exposición de servicios y falta de visibilidad. **La IA no elimina esos fundamentos; reduce el esfuerzo necesario para explotarlos y permite coordinar más tareas en menos tiempo.** El defensor necesita una capacidad equivalente para analizar señales, correlacionar evidencias y contener actividad sin depender de una secuencia enteramente manual.

Persistencia y falta de visibilidad

La velocidad no es la única estrategia del adversario. M-Trends 2026 situó la permanencia mediana global en 14 días, frente a 11 días el año anterior. Los casos de espionaje y determinadas operaciones con identidades legítimas elevaron ese valor. El patrón muestra **dos extremos que el SOC debe cubrir**: ataques que progresan en segundos y accesos que buscan permanecer ocultos durante meses.

Los puntos ciegos ya no se limitan al endpoint. Dispositivos perimetrales, hipervisores, servicios SaaS, identidades no humanas y herramientas administrativas pueden quedar fuera de la telemetría habitual.

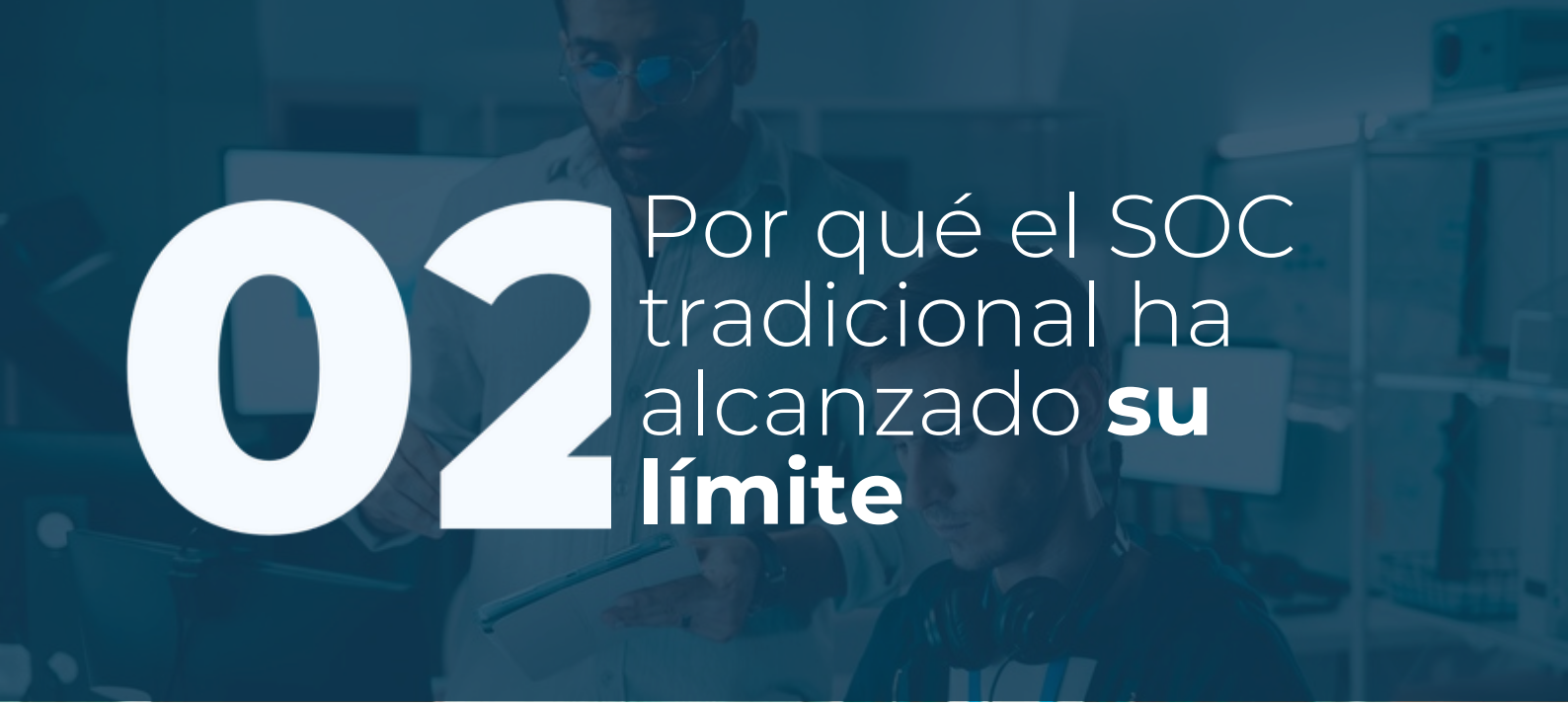
Detectar comportamientos anómalos exige correlacionar actividad a lo largo del tiempo y formular búsquedas proactivas que no dependan de una alerta previa.

Europa y España

El **ENISA Threat Landscape 2026** confirma que el **ransomware** continúa siendo el incidente con mayor impacto a corto plazo en la Unión Europea. El 73% de las organizaciones afectadas en los incidentes analizados eran **entidades esenciales** o importantes según la definición de NIS2. **La Administración Pública fue el sector más atacado**, con el 32% de los casos.

En España, **INCIBE gestionó 122.223 incidentes de ciberseguridad durante 2025**, un 26% más que el año anterior. El balance incluyó **401 incidentes en operadores esenciales e importantes**, con banca, transporte y energía entre los sectores representados. Estos datos sitúan la modernización del SOC en un contexto **especialmente relevante para grandes empresas y Administraciones Públicas**.

NIS2 exige a las entidades afectadas una alerta temprana **en un máximo de 24 horas** desde que conocen un incidente significativo y una notificación en un máximo de 72 horas. Cumplir esos plazos requiere identificar, contextualizar y documentar con rapidez. **La automatización agéntica puede acelerar esas tareas**, pero la responsabilidad, la clasificación del incidente y la decisión de notificar siguen necesitando gobierno humano y jurídico.



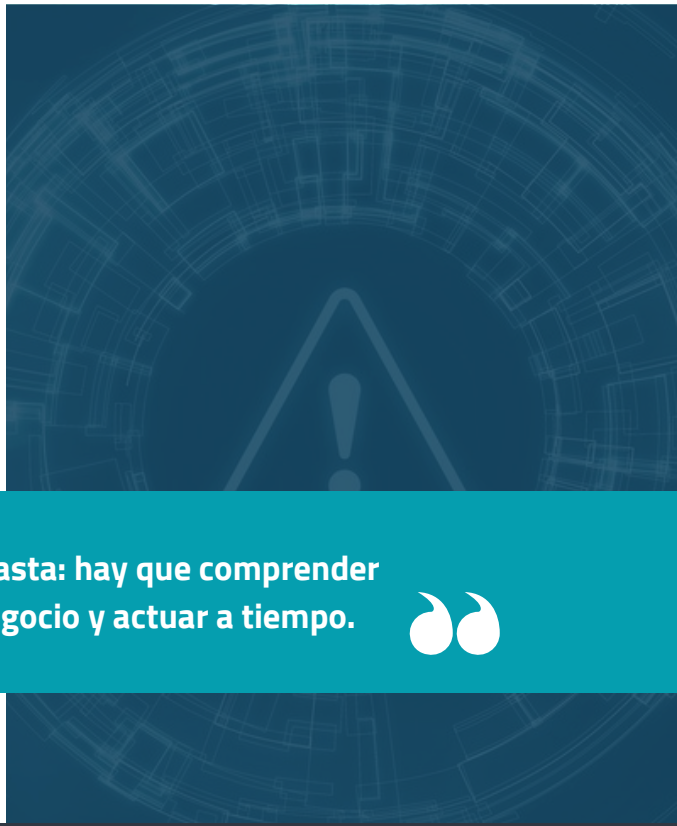
02 Por qué el SOC tradicional ha alcanzado **su límite**

Más alertas más datos y más complejidad

El SOC actual recibe señales de endpoints, identidades, redes, aplicaciones, entornos cloud y servicios de terceros. La dificultad no consiste solo en almacenar esa telemetría. **El equipo debe relacionar eventos de tecnologías diferentes y decidir cuáles representan un riesgo real para el negocio.**

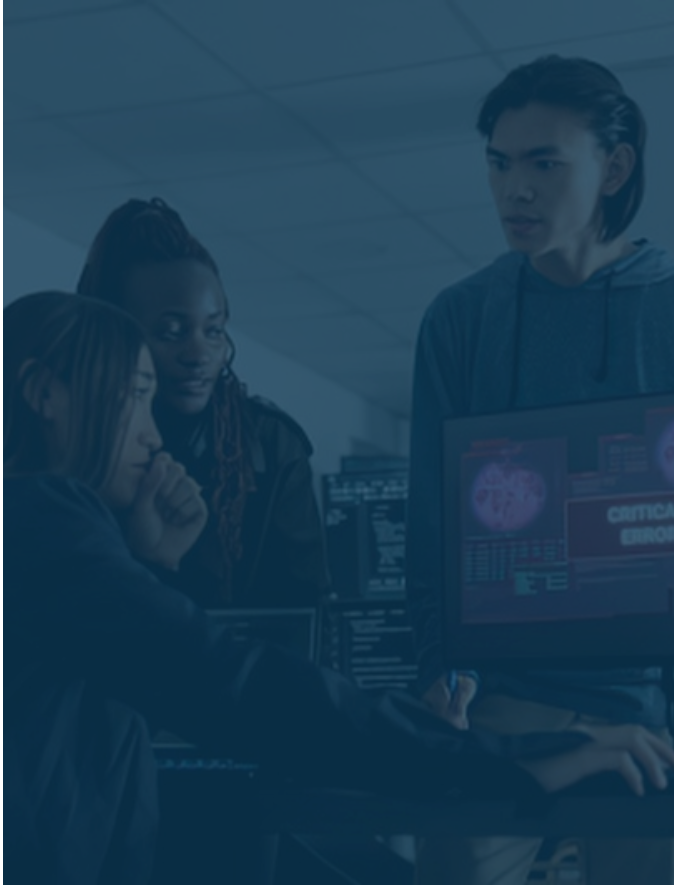
Una alerta aislada rara vez aporta toda la respuesta. Para interpretarla hay que conocer el usuario implicado, la función del activo, sus vulnerabilidades, los cambios autorizados y la actividad previa.

Cuando esa información permanece repartida entre herramientas, **la investigación empieza con una búsqueda manual de contexto.**



Detectar una alerta no basta: hay que comprender qué significa para el negocio y actuar a tiempo.

La investigación manual no escala



Cada consulta manual añade espera. El analista abre varias consolas, copia indicadores, reconstruye una cronología y documenta el resultado.

El proceso puede ser correcto y, aun así, llegar tarde. La consecuencia es una cola de alertas en la que los casos **compiten por una capacidad experta limitada**. Una alerta como la transferencia de datos de nuestro caso **puede quedarse esperando turno mientras el atacante avanza.**

Google indica que su **agente de Triaje e Investigación** puede reducir un análisis manual típico **de 30 minutos a 60 segundos**. La cifra describe la capacidad comunicada por Google, no un resultado medido en las **operaciones de Evolutio**. Su valor está en mostrar **qué parte del trabajo inicial puede comprimirse** cuando la plataforma reúne evidencias y entrega un veredicto explicado.

Escasez y dependencia del conocimiento individual

Las operaciones de seguridad necesitan especialistas capaces de **interpretar** técnicas de ataque, **comprender** el entorno del cliente **y tomar decisiones bajo presión**. Ese conocimiento suele concentrarse en analistas concretos.

Cuando los procedimientos no capturan cómo se consulta y utiliza el contexto, **resulta difícil mantener una calidad homogénea** entre turnos y equipos.

Los agentes pueden convertir parte de ese conocimiento en **instrucciones, conectores y políticas reutilizables**.

No sustituyen el criterio profesional. **Preparan el caso para que el analista dedique más tiempo a valorar el riesgo, decidir excepciones y dirigir la respuesta.**

Los límites de las reglas y la automatización rígida

Las **reglas** y los **playbooks** siguen siendo fundamentales cuando el patrón y la respuesta están bien definidos.

Su **limitación** aparece cuando el caso exige elegir qué fuente consultar, interpretar un resultado ambiguo o modificar la investigación después de encontrar una evidencia nueva.

Un flujo rígido puede automatizar una secuencia conocida. No cubre por sí solo todas las variantes de un ataque ni resuelve la falta de contexto.

El SOC necesita conservar la fiabilidad de los playbooks y añadir una capa capaz de razonar dentro de límites definidos.

Detectar no es comprender

Una **transferencia de datos a un dominio externo** puede corresponder a un proceso autorizado o a una exfiltración. **La señal técnica es la misma**; cambia el usuario, la criticidad del activo, el destino, la política aplicable y la existencia de una excepción documentada.

La capacidad de detección solo genera una decisión útil cuando se conecta con el entorno del cliente. **Esta necesidad explica el papel central de Contextualización en el modelo de Evolutio.**

El verdadero límite del SOC tradicional no está en detectar más, sino en comprender mejor.
Sin contexto, capacidad de investigación y decisiones ágiles, el volumen de alertas se convierte en una carga que dificulta responder a tiempo.



03 De la automatización tradicional al **SOC agéntico**

Del playbook al razonamiento dinámico

Un **playbook** ejecuta una **secuencia definida** de antemano. Un **agente** puede recibir un objetivo, reunir evidencias, valorar los resultados y **decidir qué consulta realizar a continuación**. Si encuentra un indicador inesperado, puede adaptar el plan de investigación sin abandonar las políticas que delimitan sus herramientas y permisos.

Ambos enfoques son complementarios. El agente resulta útil **para las fases variables** de enriquecimiento e investigación. El playbook **aporta previsibilidad** en acciones que deben ejecutarse siempre de la misma manera. La arquitectura combina razonamiento dinámico con automatizaciones deterministas, especialmente en contención y cierre.

Cuatro funciones de los agentes

Enriquecimiento

Consulta inteligencia, activos, identidades, exposición y fuentes internas.

Resultado: Caso acompañado de contexto y evidencias.

Investigación

Formula hipótesis, correlaciona señales y reconstruye secuencias.

Resultado: Veredicto explicado y recomendación.

Documentación

Genera cronologías, resúmenes y actualizaciones del expediente.

Resultado: Caso trazable y gestionable.

Respuesta

Propone o ejecuta acciones dentro de políticas definidas.

Resultado: Contención y remediación controladas.



Un sistema coordinado de agentes especializados

La **especialización** permite limitar el objetivo, las herramientas y los permisos de cada agente. **Un orquestador distribuye las tareas** y conserva el contexto necesario para que los resultados de un sistema alimenten al siguiente.

Esta estructura **reduce la dependencia de un único agente** con acceso generalizado y facilita evaluar cada función por separado.

Especialización no significa aislamiento. Los agentes comparten evidencias mediante un flujo controlado y escalan al analista cuando el caso es ambiguo, supera sus permisos o puede generar un impacto relevante.

La IA agéntica combina razonamiento dinámico con automatizaciones deterministas y supervisión humana.



Autonomía graduada

La autonomía debe definirse por tarea y riesgo. Un agente puede limitarse a observar; puede recomendar una acción; puede ejecutarla después de una aprobación; o **puede actuar de forma autónoma** dentro de condiciones previamente autorizadas.

La organización no necesita elegir entre automatización total y trabajo manual. Puede ampliar la autonomía a medida que valida la precisión, la seguridad y el valor de cada caso de uso.



04 La **arquitectura** del SOC agéntico

La arquitectura se apoya en seis principios: especialización, orquestación, integración, modularidad, trazabilidad y supervisión humana. Cada sistema tiene **un propósito definido** y puede **evolucionar sin obligar a reconstruir el conjunto**. Las evidencias y decisiones se registran para que el analista pueda revisar cómo se alcanzó un resultado.

La arquitectura concreta del servicio **parte de la telemetría del cliente** y la lleva a **Google Security Operations** mediante conectores, APIs o recolectores. La plataforma normaliza los eventos en **Unified Data Model (UDM)**, los enriquece y los correlaciona para detección, búsqueda e investigación.

La **interfaz unificada de SIEM y SOAR** convierte los hallazgos en alertas y casos, ejecuta playbooks y se integra con las herramientas de respuesta y de gestión del cliente.

Sobre esa base, **Gemini** y los **agentes aportan asistencia y razonamiento;** los sistemas propios de Evolutio incorporan el contexto del cliente, la inteligencia relevante y la gestión del servicio.

Así, la tecnología de Google y la operación de Evolutio forman un único flujo, desde el dato hasta la decisión, la respuesta y el cierre.



Un sistema coordinado de agentes especializados

CAPA	CONTENIDO
Datos y telemetría	Eventos y alertas de endpoints, identidades, red, cloud, exposición y fuentes externas.
Ingesta y normalización	Conectores, APIs y recolectores; normalización en UDM, enriquecimiento y correlación.
Operaciones de seguridad	Google SecOps SIEM+SOAR: detecciones, búsqueda, casos, playbooks y respuesta.
IA e inteligencia	Gemini, Google Threat Intelligence, Mandiant, VirusTotal y capacidades agénticas.
Sistemas de Evolutio	Contextualización, Inteligencia, Management y orquestación del servicio.
Entorno del cliente	Inventario, identidades, tickets, políticas, excepciones y procedimientos.
Gobierno	Aprobaciones, permisos, trazabilidad, métricas y supervisión.

La integración de estas capas permite combinar las **capacidades de Google Cloud** con los **sistemas y la operación de Evolutio**, dentro del entorno y los requisitos de cada cliente.

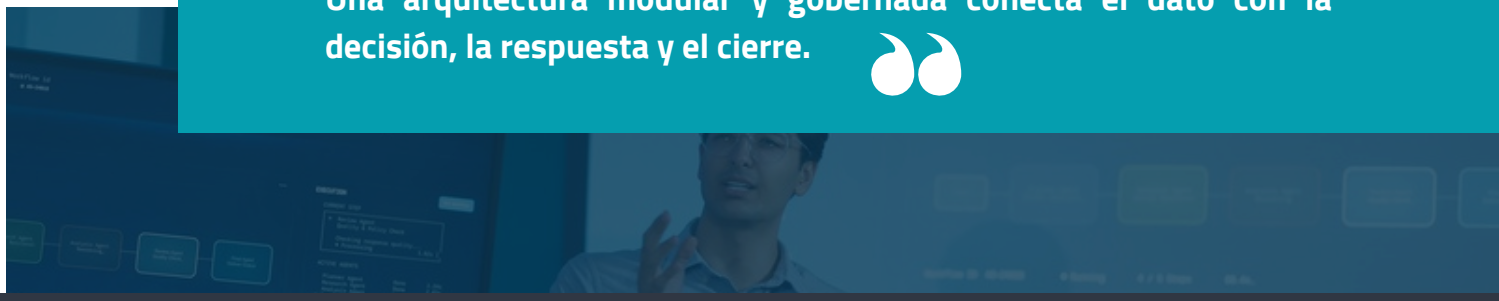
Contextualización y Management conectan los agentes con cada cliente



Los modelos, las fuentes y las herramientas de seguridad **cambian con rapidez**. Una arquitectura modular permite **incorporar nuevas capacidades, sustituir componentes e integrar entornos heterogéneos** sin rediseñar todo el servicio.

Evolutio concentra el desarrollo propio en los elementos que convierten la capacidad tecnológica en una operación adaptada al cliente.

Una arquitectura modular y gobernada conecta el dato con la decisión, la respuesta y el cierre.



05 Siete sistemas coordinados y tres **desarrollos diferenciales** de Evolutio

El modelo coordina **siete sistemas**:



Contextualización, **Inteligencia** y **Management** son desarrollos **propios de Evolutio**. **Contextualización** y **Management** forman el **núcleo diferencial** que conecta el razonamiento con el conocimiento y los procedimientos de cada cliente.

A continuación, **profundizamos en cada uno de los siete sistemas** y en el papel que desempeña dentro del modelo.

Siete sistemas coordinados; tres desarrollos propios que conectan la IA con el contexto y la operación de cada cliente.

Triaje



Triaje recibe la alerta, reúne las evidencias iniciales y establece su prioridad. **Su objetivo es reducir el tiempo entre la detección y el comienzo de una investigación útil.**

Se apoya en la búsqueda, el enriquecimiento, la inteligencia de amenazas y la gestión de casos de **Google Security Operations**.

El **agente de Triaje e Investigación** de **Google** amplía esta base con búsquedas dinámicas, veredicto, puntuación de confianza y evidencias documentadas.

El sistema **no trabaja de forma aislada**. Entrega las entidades y evidencias relevantes a **Contextualización**, que añade el conocimiento específico del cliente antes de que **Análisis** complete la investigación.



Contextualización

La Contextualización de Evolutio identifica las entidades presentes en una alerta, como usuarios, direcciones IP, dominios, URL y equipos.

Después coordina consultas al inventario, el directorio de identidades, el sistema de gestión de servicios y la documentación interna. **Cada dato conserva su fuente para que el analista pueda comprobarlo.**

El sistema **transforma datos dispersos en evidencias útiles**. No se limita a adjuntar información: selecciona la que cambia la interpretación del caso.

La criticidad del activo, los privilegios del usuario, un ticket de cambio o una excepción autorizada **pueden modificar tanto la prioridad como la respuesta**.



Análisis

Análisis formula hipótesis, solicita evidencias adicionales y contrasta explicaciones alternativas. **Correlaciona la telemetría con el contexto del cliente y la inteligencia de amenazas.**

El resultado es un veredicto acompañado de las **evidencias utilizadas y una recomendación de actuación**.

Google Security Operations aporta búsqueda sobre eventos normalizados en UDM, vistas de entidades, analítica de riesgos y acceso al dato original. **Gemini** ayuda a generar consultas YARA-L, resumir casos e investigaciones y analizar hallazgos.

El analista conserva la decisión en los casos que requieren criterio, afectan a sistemas críticos o pueden producir un impacto relevante.

Inteligencia

La **Inteligencia de Evolutio** convierte señales externas y conocimiento sobre amenazas en prioridades defensivas. Su valor no reside en acumular indicadores, sino en **explicar qué amenaza importa para una organización**, por qué resulta relevante y qué acción conviene priorizar.

Esta capacidad **se articula en tres ámbitos** complementarios: la **vigilancia del entorno digital** para identificar amenazas y exposiciones, el **Threat Hunting** para buscar de forma proactiva señales de actividad maliciosa y un **ciclo continuo de análisis y aprendizaje** que transforma los hallazgos en mejoras para la protección del cliente.



1 Vigilancia Digital e Inteligencia de Amenazas

La vigilancia amplía la visibilidad hacia Internet, la open web, la deep web y la dark web. Observa activos y servicios expuestos, dominios similares, abuso de marca, credenciales filtradas, infraestructura maliciosa y señales de campañas. Los hallazgos se relacionan con el sector, los activos, las personas y los proveedores del cliente.

Una señal externa puede activar distintas acciones: verificar una exposición, bloquear infraestructura, cambiar credenciales, reforzar una detección o iniciar una investigación. **El objetivo es ganar tiempo antes de que el riesgo se materialice dentro del entorno.**

Threat Hunting 2

Threat Hunting parte de una hipótesis y busca evidencias que una detección convencional **puede no haber convertido en alerta**. Analiza comportamientos, relaciones y secuencias, como el uso anómalo de credenciales válidas, herramientas administrativas empleadas con fines ofensivos, persistencia discreta o movimiento lateral.

En el modelo propuesto, **Evolutio formula y prioriza las hipótesis** a partir del contexto, la exposición y el perfil de riesgo del cliente. **Google Cloud aporta la búsqueda** sobre UDM, la **asistencia de Gemini** para generar hipótesis y consultas, y la inteligencia de **Google Threat Intelligence**, **Mandiant** y **VirusTotal**.

La documentación facilitada sitúa el **agente turnkey de Threat Hunting** en la evolución agéntica del producto; su disponibilidad y el reparto operativo exacto deben confirmarse antes de publicar.



3 El ciclo de Inteligencia

El ciclo recoge señales, las analiza, determina su relevancia, las convierte en acciones y utiliza el resultado **para mejorar la cobertura**.

Un hallazgo puede alimentar una detección, un hunt, una medida de protección o una respuesta. La información obtenida durante las investigaciones vuelve al sistema **para ajustar prioridades y formular nuevas hipótesis**.

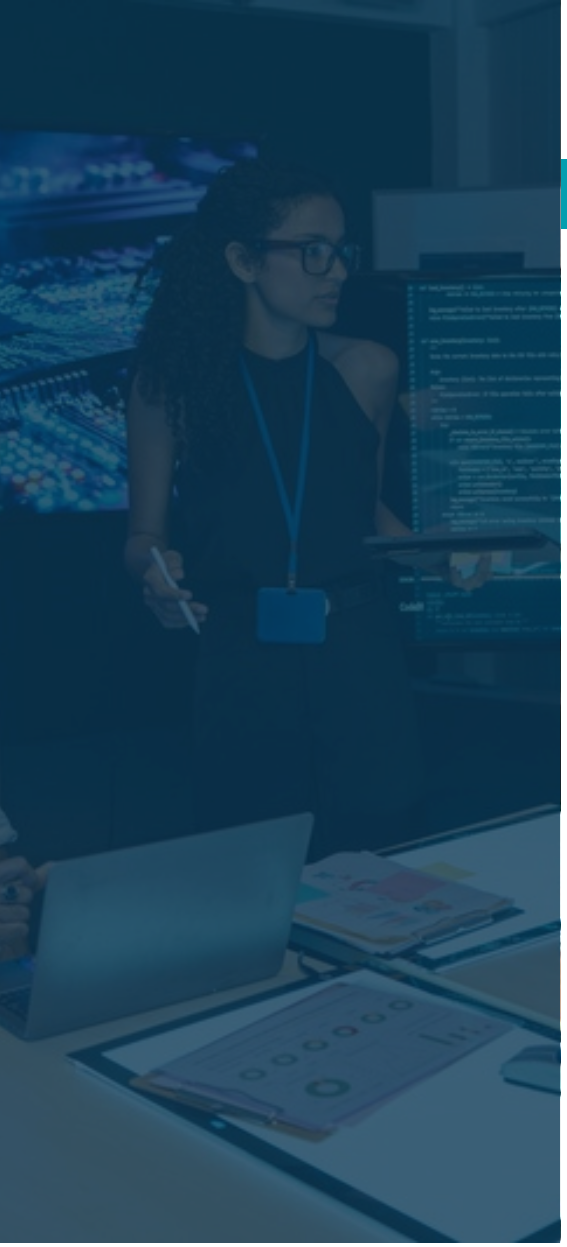
Respuesta

Respuesta prepara o ejecuta medidas de contención y remediación. **Google SecOps SOAR** aporta gestión de casos, un editor visual de playbooks e integraciones con herramientas de seguridad e ITSM; **Evolutio diseña y adapta los playbooks al entorno y a los procedimientos del cliente**.

Los agentes pueden proponer o preparar acciones, mientras que las tareas que exigen previsibilidad se ejecutan mediante **automatizaciones deterministas**.

Una acción de bajo riesgo **puede automatizarse dentro de límites definidos**. El aislamiento de un activo crítico, el bloqueo de una identidad privilegiada o una actuación con impacto en negocio **requieren aprobación**. **Todas las acciones y sus resultados quedan registradas.**





Management

La capacidad de Management de Evolutio conecta el trabajo de los agentes con la gestión cotidiana del servicio. Se apoya en los casos y conectores de **Google SecOps SOAR** para sincronizar información con el ITSM, mientras que **el desarrollo de Evolutio aplica los responsables**, prioridades, comunicaciones, escalados y condiciones de cierre El acordados con cada cliente.

Una **investigación técnicamente correcta** solo se convierte en un servicio cuando queda documentada, comunicada y gestionada según el procedimiento establecido.

El sistema **registra los hitos necesarios** para medir tiempos y localizar esperas. Esta continuidad permite interpretar MTTD, MTTA y MTTR junto con la gravedad del incidente, la **calidad de la decisión** y los acuerdos de nivel de servicio.

Aprendizaje

Aprendizaje recoge los resultados de las investigaciones y **los convierte en mejoras**. Identifica falsos positivos, fuentes insuficientes, consultas útiles, carencias de detección y condiciones de escalado que necesitan ajustes. Las lecciones **se incorporan a reglas**, instrucciones, conectores, políticas y futuros hunts.

Este aprendizaje es operativo. No implica utilizar los datos del cliente para entrenar modelos fundacionales. Su objetivo es **mejorar el comportamiento del servicio** y la base reutilizable de automatizaciones dentro del marco acordado.





06 Evolutio y Google Cloud. Un partnership que potencia el SOC agéntico

Evolutio y Google Cloud comparten una premisa: el defensor necesita operar con una velocidad comparable a la del atacante sin renunciar al control. La **IA** debe resolver tareas concretas, **integrarse en las herramientas del SOC** y entregar resultados que el analista pueda revisar.

El partnership combina capacidad tecnológica, inteligencia global y conocimiento operativo. La plataforma y los agentes aceleran la investigación; el modelo de Evolutio los conecta con los datos, las reglas y los procedimientos de cada cliente.

La base tecnológica de Google Cloud

Google Security Operations es la base del servicio: una plataforma cloud-native que integra SIEM y SOAR en una **misma experiencia para ingerir y normalizar telemetría**, enriquecerla, aplicar detecciones, investigar, gestionar casos y orquestar la respuesta.

El modelo MSSP descrito por **Google** combina aislamiento del dato en el entorno SIEM de cada cliente **con operación centralizada en SOAR**. La configuración concreta depende del servicio contratado.

Gemini añade interacción en lenguaje natural, conversión de consultas a YARA-L, resúmenes de casos e investigaciones, apoyo al hunting y sugerencias de playbooks. **Google Threat Intelligence integra el conocimiento de Google**, **Mandiant** y **VirusTotal**, y las reglas curadas permiten aplicar parte de esa inteligencia directamente sobre la telemetría del cliente.

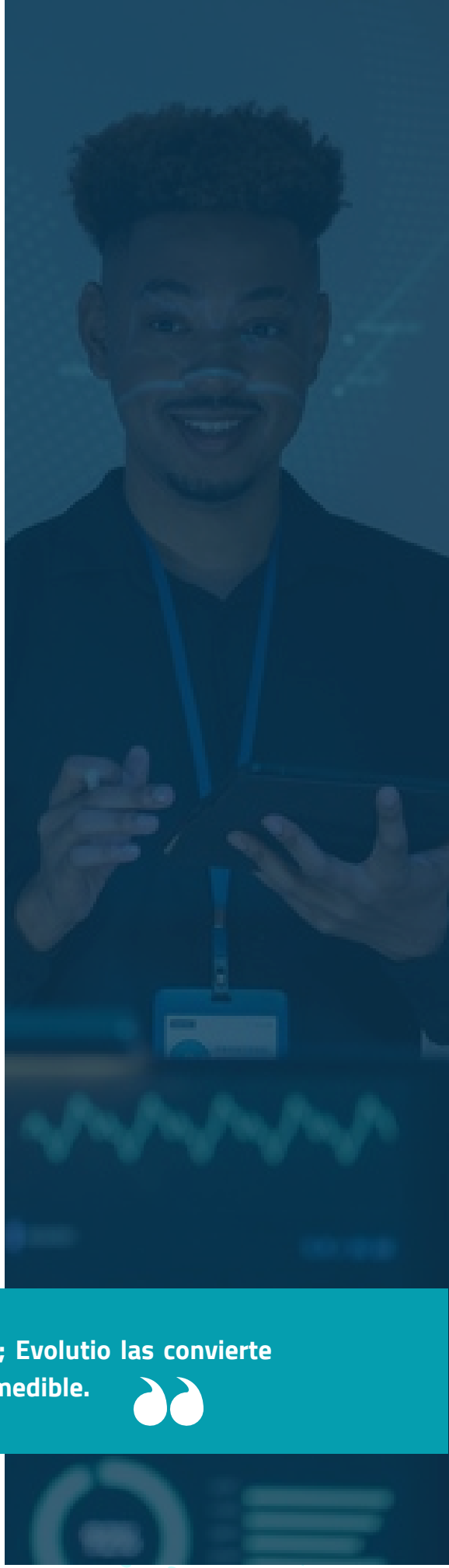
La capacidad operativa de Evolutio

En Evolutio diseñamos y operamos el servicio, integramos las fuentes del cliente y coordinamos los siete sistemas.

Tenemos **experiencia operando Google SecOps y su SOAR en un servicio multicliente**, creamos casos de uso vinculados a MITRE ATT&CK, desarrollamos playbooks e **integramos la plataforma con las herramientas de seguridad y gestión del cliente**.

Nuestros **desarrollos propios** añaden el conocimiento que una plataforma general no posee: la criticidad de los activos, las excepciones autorizadas, los interlocutores, los procedimientos y las condiciones de cierre.

Contextualización aporta significado a la alerta. Inteligencia selecciona y operacionaliza las amenazas relevantes. **Management** convierte la investigación en una operación gestionable y medible. **Inteligencia** convierte señales externas y conocimiento sobre amenazas en prioridades defensivas. **El conjunto permite aprovechar la evolución de Google Cloud sin perder la adaptación a cada organización.**



Google aporta plataforma e inteligencia; Evolutio las convierte en una operación adaptada, integrada y medible.

07 Un incidente **de principio a fin**

Una **plataforma de seguridad** detecta una transferencia inusual de datos hacia un dominio externo. La señal contiene el usuario, el equipo, el destino y el volumen transferido, pero **no permite determinar por sí sola si existe una actividad autorizada**.



Triaje

Triaje **recopila la telemetría inicial**, identifica las entidades y valora la prioridad. Comprueba **si existen señales relacionadas** y prepara el caso para la investigación.

Contextualización

Contextualización **consulta el directorio de identidades**, el inventario, los tickets y la normativa. El usuario pertenece a Finanzas, **tiene privilegios elevados** y utiliza un activo crítico. No aparece una autorización de transferencia y el destino contraviene la política interna.

Inteligencia

Inteligencia **comprueba el dominio**, su infraestructura y posibles relaciones con campañas conocidas. El resultado **aumenta o reduce la credibilidad de la hipótesis** de exfiltración y orienta nuevas consultas.

Análisis

Análisis **reconstruye la secuencia**, contrasta explicaciones y solicita evidencias adicionales. Revisa autenticaciones, procesos, accesos previos y comportamiento del equipo. **Entrega un veredicto** explicado con las fuentes utilizadas.



Decisión y Respuesta

El analista **valida el caso y aprueba las acciones previstas** para esa severidad. Respuesta puede bloquear el destino, aislar el equipo, revocar sesiones o iniciar otras **medidas de contención** según el procedimiento.

Management

Management **actualiza el ticket**, comunica el incidente a los interlocutores, registra los hitos y controla las condiciones de cierre. La evidencia **queda disponible para seguimiento** y posibles obligaciones de notificación.

Aprendizaje

El resultado se utiliza para **mejorar detecciones, instrucciones y consultas.** Si la investigación revela un patrón nuevo, puede generar una **hipótesis de hunting** para buscar actividad similar en otros activos.

¿Y si la transferencia estaba autorizada? Si **Contextualización** hubiera encontrado una autorización documentada, la misma alerta se habría valorado de otro modo.

El caso se cerraría como actividad legítima, con la evidencia que lo justifica, y el analista no habría tenido que reconstruirlo a mano. La señal es idéntica en los dos escenarios; **lo que cambia la decisión es el contexto del cliente.**

¿Cómo resolvería hoy su SOC esta alerta? **Nuestros expertos pueden analizarlo con usted en una reunión de trabajo.**

La misma alerta puede ser una exfiltración o una actividad legítima: el contexto del cliente cambia la decisión.



08 Control humano confianza y soberanía

1 El analista dentro del circuito

El **SOC agéntico** amplía la automatización **sin eliminar la responsabilidad humana**. El analista valida casos ambiguos, gestiona excepciones y aprueba acciones con impacto relevante. Los agentes absorben trabajo repetitivo y presentan evidencias; **el profesional conserva el criterio** y la autoridad definidos para el servicio.

2 Identidad y permisos de los agentes

Cada agente debe tener **una identidad diferenciada**, acceso limitado a las herramientas que necesita y condiciones claras de escalado. **Los permisos mínimos reducen el impacto de un error** y permiten atribuir cada consulta y acción. Las fuentes autorizadas, la memoria y el contexto también forman parte de la política del agente.

3 Trazabilidad y explicabilidad

El sistema **debe registrar qué evidencias consultó**, qué hipótesis formuló, qué política aplicó y qué acciones ejecutó. La **trazabilidad** permite reconstruir el caso, revisar un resultado y demostrar cómo se alcanzó una decisión. Una **explicación útil** cita las fuentes y separa los hechos de la inferencia.

4 Confianza y autonomía progresiva

La **confianza se construye con pruebas controladas** y resultados medibles. Antes de ampliar permisos, el equipo evalúa precisión, errores, escalados y comportamiento ante excepciones. Un agente puede comenzar recomendando acciones y **avanzar hacia la ejecución** solo en escenarios bien delimitados.

Soberanía del dato

Una **investigación** puede contener identidades, vulnerabilidades y detalles sobre activos críticos. El **Gateway de IA** de la arquitectura **asigna a cada flujo el modelo** y el entorno de ejecución compatibles con los **requisitos del cliente**. La decisión considera sensibilidad, ubicación, permisos, coste y capacidad necesaria para la tarea.

En **Google SecOps**, el diseño MSSP permite **aislar la telemetría en entornos SIEM dedicados por cliente** y centralizar la operación autorizada mediante SOAR. La plataforma incorpora **controles como IAM, VPC Service Controls**, registros de auditoría y residencia de datos, con 12 meses de retención en caliente como configuración de referencia. La región, la retención, el aislamiento y los accesos se fijan en la arquitectura y el contrato de cada servicio.

La soberanía va más allá del lugar de ejecución: exige controlar qué información recibe el modelo, durante cuánto tiempo se conserva, qué herramientas puede invocar y quién puede revisar el resultado.

Encaje regulatorio

La **automatización** puede ayudar a reunir evidencias, construir cronologías y preparar la **información necesaria para notificaciones**. NIS2 establece una secuencia de alerta temprana, notificación e **informe final para incidentes significativos**. El sistema debe facilitar ese proceso sin sustituir la evaluación jurídica ni la responsabilidad de la entidad.

El **gobierno del SOC agéntico debe integrarse** con los procedimientos de gestión de incidentes, continuidad y cumplimiento. **La trazabilidad sirve tanto para mejorar la operación como para justificar las decisiones adoptadas.**



La autonomía se gana con evidencias: permisos mínimos, trazabilidad y supervisión humana.

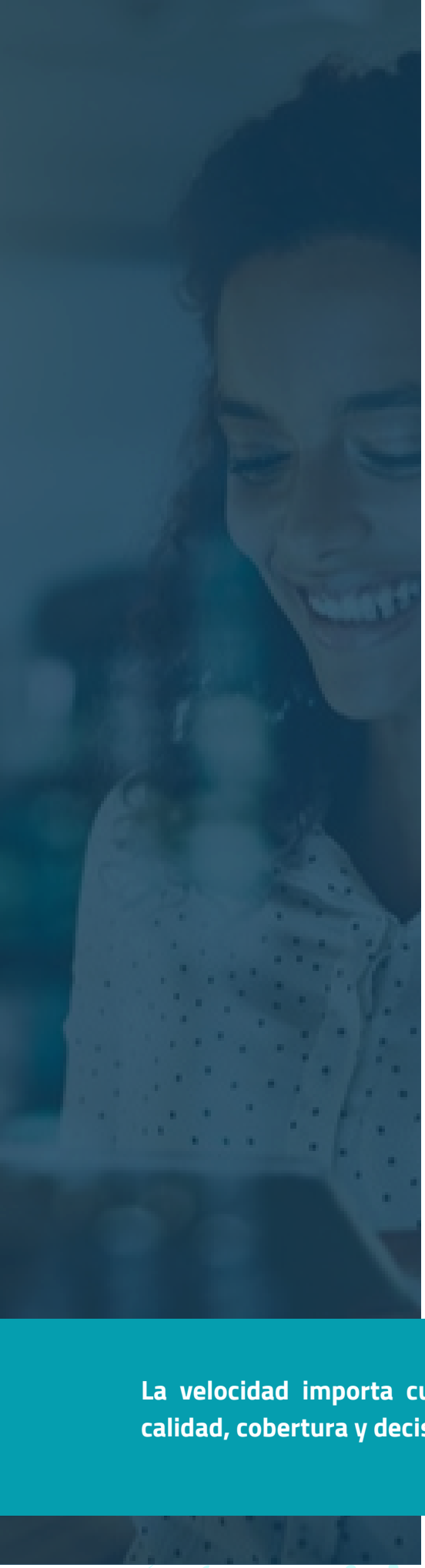


09 Del rendimiento técnico al **impacto empresarial**

Modelo de medición

La **automatización** debe evaluarse con una línea base y criterios constantes. **Los tiempos por sí solos no bastan:** una reducción del MTTR pierde valor si aumenta el número de decisiones incorrectas o de acciones revertidas.

INDICADOR	QUÉ MIDE	CÓMO INTERPRETARLO
Tiempo de triaje	Intervalo hasta disponer de una primera valoración útil.	Comparar por severidad y tipo de alerta.
MTTD	Tiempo medio de detección.	Depende de cobertura y calidad de telemetría.
MTTA	Tiempo hasta el reconocimiento o inicio de atención.	Permite localizar esperas en la cola.
MTTR	Tiempo medio de resolución.	Debe acompañarse de calidad y alcance del cierre.
Cobertura	Porcentaje de alertas o casos investigados.	Distinguir investigación completa de cierre automático.
Calidad	Consistencia de veredictos y acciones.	Revisar falsos positivos, falsos negativos y reversiones.
Escalados	Casos transferidos al analista.	Analizar causa, riesgo y utilidad del escalado.



Impacto sobre el equipo

Para el equipo, el principal beneficio es **dejar atrás las búsquedas manuales**: los casos se documentan de forma consistente y llegan preparados para revisión. El tiempo recuperado puede dedicarse a **hunting**, **ingeniería de detección**, **respuesta compleja** y **mejora de la cobertura**.

La **estandarización** también reduce la dependencia del conocimiento individual. Las **instrucciones y fuentes quedan incorporadas al flujo**, y el analista puede revisar cómo se utilizó cada evidencia.

Impacto para la organización

La **reducción de los tiempos de investigación** acorta la ventana durante la que un atacante puede avanzar sin respuesta. También permite **priorizar antes los activos críticos**, preservar evidencias y coordinar con mayor rapidez a seguridad, tecnología, continuidad y cumplimiento.

Una operación más consistente **facilita mantener los niveles de servicio** y preparar la información necesaria para decisiones, escalados y notificaciones. Al absorber tareas repetitivas, el modelo **permite gestionar más casos** sin aumentar en la misma proporción el trabajo manual y reserva la capacidad experta para los incidentes con mayor impacto potencial.

La velocidad importa cuando se acompaña de calidad, cobertura y decisiones correctas.

10 Cómo empezar. Del primer caso de uso a la autonomía progresiva

El punto de partida es conocer su situación actual: la calidad de la telemetría, las integraciones disponibles y el grado de documentación de los procesos. La organización necesita **identificar qué fuentes aportan contexto** sobre activos, identidades y exposición, y si puede medir los tiempos y resultados actuales.

También debe **definir quién aprueba una acción**, **cómo se gestionan las excepciones** y **qué evidencia necesita para ampliar la autonomía**. Sin esa base, el piloto puede automatizar tareas, pero no demostrar una mejora sostenible.

El **primer caso** debe combinar volumen suficiente, beneficio visible y riesgo controlado. **El equipo establece una línea base**, define qué puede observar, recomendar y ejecutar el agente, y **prueba el flujo bajo supervisión humana**.

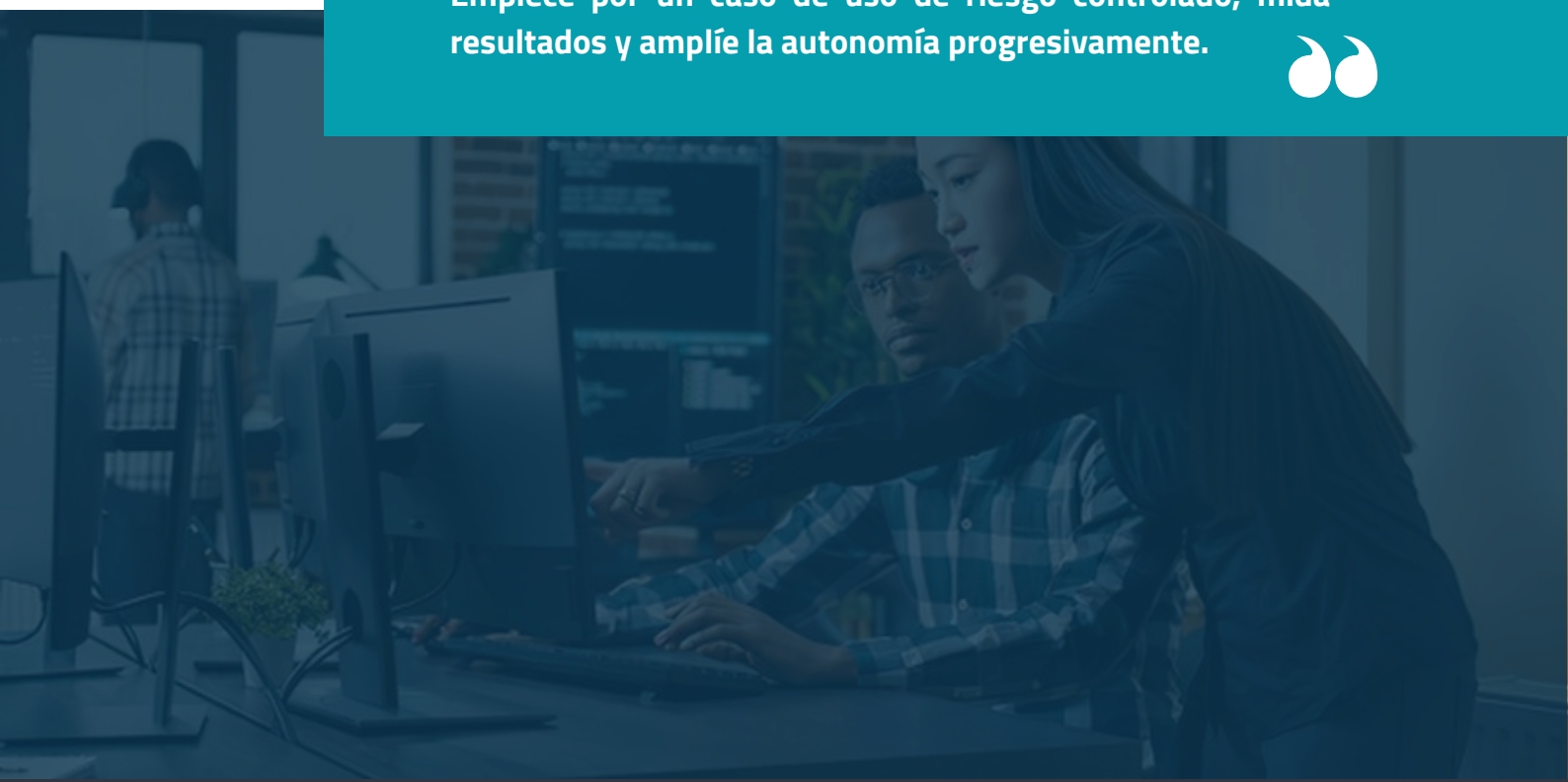


El **piloto** se evalúa con el **modelo del capítulo 9**. Si los resultados cumplen los criterios de precisión, trazabilidad y valor, **se incorporan nuevos casos** y se amplían los permisos de forma gradual. Las políticas, instrucciones, conectores y fuentes **se revisan periódicamente**.

En **Evolutio acompañamos a cada organización en estas fases**, desde la evaluación inicial hasta la ampliación progresiva de la autonomía.

Evaluar	**Confirmar datos, integraciones, procesos y línea base.**
Seleccionar	**Elegir un caso de alto volumen y riesgo controlado.**
Diseñar	**Definir herramientas, permisos, fuentes y escalados.**
Probar	**Validar precisión, seguridad, trazabilidad y comportamiento.**
Medir	**Comparar con la línea base mediante el modelo del capítulo 9.**
Ampliar	**Incorporar casos y autonomía de forma progresiva.**

Empiece por un caso de uso de riesgo controlado, mida resultados y amplíe la autonomía progresivamente.



11 Conclusiones

Los atacantes operan **a una velocidad que el SOC tradicional no puede igualar** únicamente con procesos manuales. El defensor necesita **reducir el tiempo dedicado a recopilar y correlacionar evidencias** para concentrarse en las decisiones que requieren criterio.

El **SOC agéntico** combina agentes especializados con **automatizaciones deterministas y supervisión humana**. El objetivo es **aumentar la capacidad de investigación y respuesta** sin perder previsibilidad en las acciones críticas.

Contextualización, Inteligencia y Management convierten la capacidad general de la IA en una operación adaptada. Incorporan conocimiento del cliente, conectan amenazas con acciones y llevan el resultado hasta los procedimientos del servicio.



El reto no es solo acelerar el SOC, sino hacerlo con control, contexto y confianza.

El **partnership entre Evolutio y Google Cloud** une **Google Security Operations**, **Gemini** y la inteligencia de **Google Threat Intelligence** y **Mandiant** con el conocimiento operativo y los desarrollos propios de **Evolutio**.

La **autonomía** debe crecer con evidencia. Trazabilidad, control humano, soberanía y un modelo de medición **permiten ampliar el alcance sin convertir la velocidad en un riesgo adicional.**



Transforme sus operaciones de seguridad

Descubra cómo aplicar el modelo de SOC agéntico de Evolutio y Google Cloud en su organización.

Solicite una reunión con nuestros expertos

Analizaremos su punto de partida, los casos de uso con mayor potencial y el camino para incorporar autonomía de forma progresiva.

evolutio.com 91 270 6000 info@evolutio.com

