

El Ciclo de Seguridad Activa

Mantener la Evaluación de Riesgos de Seguridad al ritmo de un mundo cambiante: lo que la forma en que el cerebro gestiona la incertidumbre puede enseñar a la gestión de la seguridad



Alberto Gomez Castro

Profesional Senior en Seguridad y Gestión Estratégica de Riesgos | Oficial en retiro de la Marina de Guerra del Perú | Ex Jefe de Seguridad (Chief Security Officer) de las Naciones Unidas

RESUMEN

La Evaluación de Riesgos de Seguridad (SRA, por sus siglas en inglés) y la Gestión de Riesgos de Seguridad (SRM) proporcionan a las organizaciones una comprensión estructurada de su entorno de seguridad; sin embargo, el producto de una evaluación es esencialmente la imagen de un momento determinado, que por lo general se espera que siga siendo válida durante seis meses o un año mientras el entorno cambia de manera continua. Este artículo propone el Ciclo de Seguridad Activa (Active Security Cycle, ASC), un proceso recurrente y sencillo diseñado para mantener esa imagen en contacto con la realidad entre evaluaciones formales. La propuesta se inspira, por analogía y sin su aparato matemático, en el Principio de Energía Libre y la Inferencia Activa, una explicación neurocientífica de cómo el cerebro predice, percibe, actúa y aprende de manera continua en un mundo incierto. Si se considera a la organización como un organismo y a su función de seguridad como su cerebro, la SRA se convierte en el modelo de seguridad vigente de la organización, sus herramientas de percepción y de acción pasan a ser la frontera a través de la cual se relaciona con el entorno operacional, y cualquier discrepancia significativa entre lo esperado y lo que ahora se observa se convierte en el detonante de un ciclo de siete pasos: Anticipar, Percibir, Inferir, Comparar, Actuar, Aprender y Actualizar. El artículo explica el fundamento de la propuesta, examina la persistente dificultad de estimar la probabilidad cuando los datos sobre incidentes son escasos, ilustra el ciclo con tres casos y ubica el ASC dentro de los procesos establecidos de SRA/SRM, a los que complementa sin reemplazarlos.

PALABRAS CLAVE Ciclo de Seguridad Activa; Evaluación de Riesgos de Seguridad; Gestión de Riesgos de Seguridad; incertidumbre; error de predicción; probabilidad; Principio de Energía Libre; Inferencia Activa; estrategia de aceptación; gestión adaptativa de la seguridad.

1 Una imagen estática de un mundo en movimiento

Durante la mayor parte de mi vida profesional en seguridad, la evaluación de riesgos siguió una lógica conocida. Identificábamos amenazas, examinábamos vulnerabilidades, estimábamos probabilidad e impacto, asignábamos niveles de riesgo y seleccionábamos medidas de mitigación. Es un enfoque útil y bien establecido, respaldado por normas internacionales y por un considerable cuerpo de práctica profesional [1,2]. Con el tiempo, sin embargo, fui tomando conciencia de una limitación que tiene menos que ver con la calidad de una metodología en particular que con la naturaleza de lo que produce.

Cualquiera que sea el método utilizado, el resultado de una Evaluación de Riesgos de Seguridad es, por lo general, un documento. Describe el entorno de seguridad, las operaciones de la organización, las amenazas que enfrenta, sus vulnerabilidades y las medidas que se consideran necesarias, y a menudo lo hace con cuidado y muy bien. Pero describe todo ello tal como se entendía en un momento determinado, mientras se espera que siga siendo válido durante un largo período, con frecuencia seis meses o un año, en entornos llenos de incertidumbre que no dejan de cambiar desde el día en que el documento es aprobado. Los mecanismos de monitoreo y revisión incluidos en la mayoría de los procesos de SRA/SRM tienden a concentrarse en la implementación de las medidas recomendadas por la evaluación. Ello es necesario, pero deja de lado una tarea distinta: detectar los cambios en el entorno que pueden estar erosionando silenciosamente la imagen sobre la cual se basaron esas medidas. Las normas ISO y los manuales profesionales ofrecen principios muy útiles y un marco sólido para operar [1,2], aunque en mi experiencia no reflejan plenamente la dinámica cotidiana de un sistema de seguridad corporativo u organizacional que trabaja en un entorno operacional incierto.

Hace algún tiempo, y sin ser matemático ni neurocientífico, comencé a leer sobre el Principio de Energía Libre y su corolario, la Inferencia Activa, desarrollados principalmente por el neurocientífico Karl Friston [3–6]. En algún momento de ese proceso de aprendizaje a través de artículos, libros, podcasts y conferencias, surgió una pregunta que ha guiado todo lo que aquí se presenta: ¿por qué no aplicamos a la evaluación y gestión de riesgos de seguridad la forma en que el cerebro opera bajo incertidumbre? El cerebro humano es el sistema natural más sofisticado que conocemos para mantener a un organismo a salvo y con vida en un mundo incierto. Si consideramos a una organización como un organismo, a su función de seguridad como su cerebro, y a sus medios para percibir y actuar como la frontera a través de la cual se relaciona con su entorno operacional, la forma en que funciona el cerebro puede ofrecernos algunas ideas útiles.

Este artículo integra y desarrolla tres trabajos anteriores en los que exploré esa pregunta: una propuesta conceptual, un estudio de caso sobre una amenaza emergente en ciberseguridad y un ejercicio que confrontó el modelo resultante con un procedimiento de SRA validado. El resultado es lo que denomino el Ciclo de Seguridad Activa (Active Security Cycle, ASC), una manera sencilla de mantener una Evaluación de Riesgos de Seguridad en relación dinámica con los cambios de su entorno. El ASC no reemplaza a la SRA ni pretende corregir la forma en que un profesional de seguridad desarrolla cada etapa de la evaluación. Comienza donde la SRA termina. Del mismo modo en que el cerebro trabaja a partir de un modelo del mundo que espera encontrar, la evaluación concluida, cualquiera que sea el método que la produjo, se convierte en el modelo inicial del entorno de seguridad que la organización espera para llevar a cabo sus actividades. Aplicar el ASC como una herramienta diaria o de uso frecuente permite entonces a la organización detectar a tiempo cualquier evento o situación que ponga en duda la validez de ese modelo, en lugar de esperar períodos más largos para revisarlo.

UNA NOTA SOBRE EL CARÁCTER DE ESTA PROPUESTA

Utilizo conceptos del Principio de Energía Libre y de la Inferencia Activa como una analogía, interpretada y adaptada a la gestión de la seguridad, y no como una traducción exacta de una teoría científica a otra disciplina. Mi especialidad es la seguridad y no la neurociencia, y asumo plena responsabilidad por la forma en que esos conceptos se han utilizado aquí. El Ciclo de Seguridad Activa es una propuesta propia y no un modelo estándar de la literatura científica. Debe considerarse una hipótesis de trabajo cuyo valor se decidirá, en última instancia, al aplicarla a problemas reales de seguridad, sobre evaluaciones ya existentes, y observar si hace esas evaluaciones más dinámicas y las decisiones resultantes mejor informadas.

2 Aprender del cerebro

El cerebro no se limita a esperar información del mundo exterior, procesarla y luego decidir qué hacer. Desde la perspectiva del Principio de Energía Libre y de la Inferencia Activa, puede entenderse como un sistema que genera continuamente expectativas respecto de lo que está a punto de encontrar, y que utiliza la información sensorial como evidencia de si esas expectativas siguen siendo adecuadas [3–6]. Cuando ambas no coinciden, el organismo puede revisar su comprensión de lo que está ocurriendo, y también puede actuar sobre su entorno y cambiar lo que sucede a continuación. La percepción orienta la acción, la acción modifica la relación del organismo con su entorno, y el entorno modificado produce nueva información sensorial que vuelve a orientar la percepción, en lo que podría describirse como una

danza permanente de predicción, percepción y acción.

Un concepto asociado al Principio de Energía Libre ayuda a explicar esta relación: el manto de Markov (Markov blanket). A pesar de su nombre técnico, su intuición básica puede describirse sin matemáticas. Un organismo no tiene acceso directo a todo lo que ocurre en su entorno, y el entorno no tiene acceso directo a los estados internos del organismo. Su interacción está mediada por una frontera compuesta por dos tipos de estados: los *estados sensoriales*, a través de los cuales los cambios del mundo exterior influyen en el organismo, y los *estados activos*, a través de los cuales el organismo influye en el mundo exterior [7–9].

Pensemos en una persona que camina por una calle oscura. Como conoce la ruta de noches anteriores, espera que esté tranquila, con poco tránsito y sin nada inusual en el camino a casa; esa expectativa es su modelo inicial de la calle, del mismo modo que la SRA es el modelo inicial que una organización tiene de su entorno. No puede saber todo lo que ocurre a la vuelta de la esquina, pero ve movimiento, escucha sonidos, nota cambios en la iluminación y observa cómo se comportan otras personas, y a partir de esos estímulos sensoriales su cerebro infiere lo que puede estar sucediendo. Sin embargo, hace más que percibir. Puede caminar más despacio, cruzar la calle, iluminar una zona con su teléfono, preguntar algo a alguien o elegir otra ruta, y cada una de esas acciones modifica tanto su relación con el entorno como la información de la que dispondrá después.

Una organización de seguridad se encuentra en una situación notablemente similar. Nunca tiene acceso directo al estado completo de su entorno operacional. Se apoya en su Evaluación de Riesgos de Seguridad (SRA) como modelo inicial de lo que espera encontrar, y en la inteligencia, el reporte de incidentes, las cámaras, las alarmas, las comunicaciones, el enlace con las autoridades, las observaciones del personal, los contactos comunitarios y otras fuentes para inferir lo que está ocurriendo. Influye en ese entorno mediante el control de accesos, las fuerzas de vigilancia, los procedimientos, las decisiones sobre movimientos, la protección física, la capacitación, la planificación de contingencias y evacuación, los arreglos de continuidad del negocio, la relación con la comunidad y muchas otras intervenciones. No sostengo que estos mecanismos constituyan literalmente un manto de Markov biológico, pero propongo que pueden asimilarse funcionalmente a sus estados sensoriales y activos. La información que fluye hacia el sistema de seguridad llega a través de lo que denomino las herramientas de percepción de la organización, y las intervenciones que fluyen desde el sistema de seguridad hacia su entorno son sus herramientas de acción. Entre ambas se encuentra el modelo interno de seguridad de la organización: sus supuestos, evaluaciones y expectativas sobre lo que está ocurriendo y lo que puede ocurrir a continuación (Figura 1).

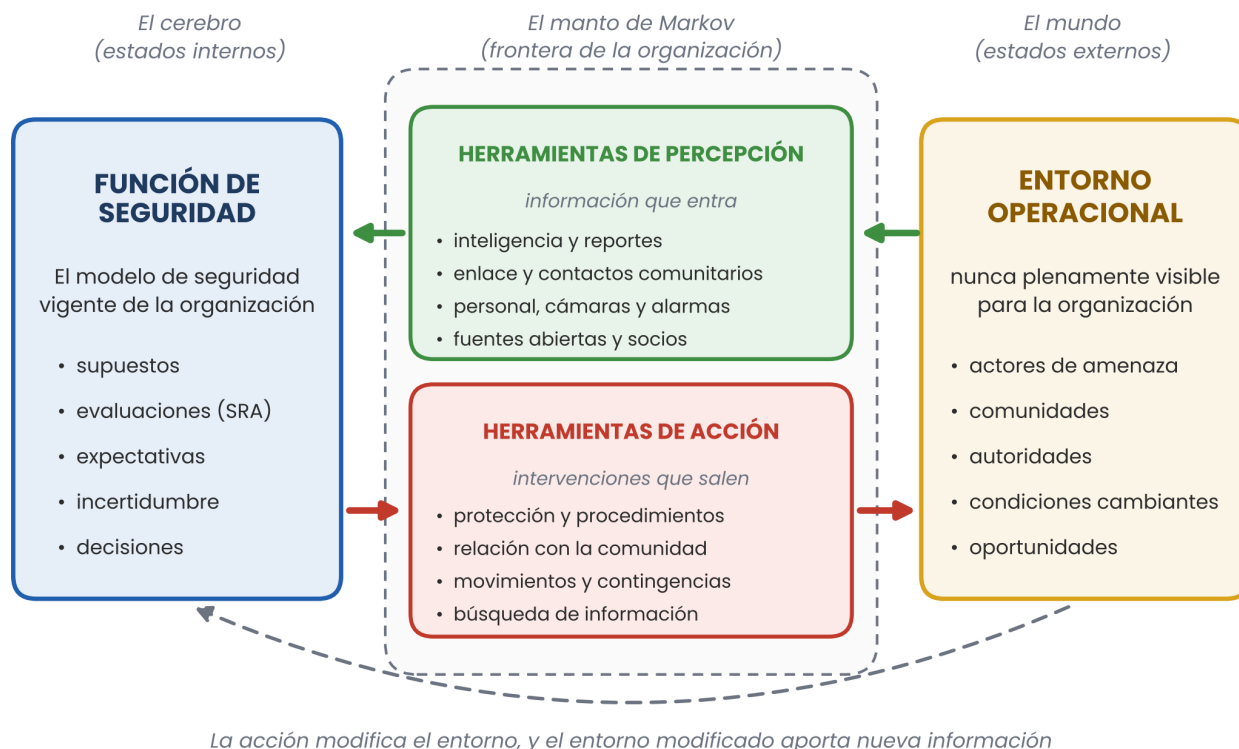


Figura 1. La organización como organismo. Las herramientas de percepción y de acción cumplen, por analogía funcional, el papel que los estados sensoriales y activos desempeñan en el marco del manto de Markov, al mediar la interacción continua entre la función de seguridad y un entorno operacional que nunca puede observar por completo. El diagrama es conceptual y omite la formulación matemática del marco.

Vista así, la organización de seguridad es mucho más que un procesador de información que espera que la información sobre amenazas llegue desde afuera. Es un sistema adaptativo en interacción continua con su entorno operacional a través de la percepción y la acción, y esa es la imagen sobre la que se construye el resto de esta propuesta.

3 El error de predicción: cuando la realidad deja de coincidir con el modelo

Un concepto adicional de la Inferencia Activa es central para la propuesta, aunque permaneció implícito en mis artículos anteriores: el error de predicción. En términos simplificados, el cerebro utiliza su modelo interno para anticipar la información sensorial que probablemente encontrará. Cuando lo que se percibe corresponde suficientemente con lo esperado, hay pocas razones para revisar el modelo. Cuando aparece una discrepancia importante, se produce un error de predicción [3-6]. La palabra *error* no significa aquí que alguien se haya equivocado. Se refiere a la diferencia entre lo que el sistema esperaba y lo que ahora encuentra, una diferencia que puede ser pequeña o grande, temporal o persistente, y que con el tiempo puede

mostrar que las condiciones son peores, mejores o simplemente distintas de las que el modelo anticipaba.

La idea se traslada con naturalidad a la gestión de la seguridad y se aplica a cualquier estrategia de seguridad. Bajo una estrategia de protección, una SRA puede suponer que la respuesta policial en una zona determinada es confiable porque se ha establecido un enlace eficaz, se han verificado los arreglos de emergencia y la experiencia respalda ese juicio. Entonces se reemplaza al jefe de policía. No ha ocurrido ningún incidente y no hay evidencia de que la respuesta policial se haya deteriorado, pero una de las condiciones que sustentaban la expectativa de la organización ha cambiado. Bajo una estrategia de aceptación, una organización puede haber construido una relación productiva con el liderazgo comunitario, que contribuye a la comprensión local de sus actividades y quizá al intercambio informal de información relevante para la seguridad. Cuando se reemplaza a un líder comunitario influyente, no puede suponerse que esa relación se transfiera automáticamente a su sucesor.

En ambos casos la realidad ya no corresponde por completo con lo que la organización esperaba, y en ambos casos ello no significa necesariamente que el riesgo haya aumentado. El nuevo liderazgo policial puede cooperar igual o mejor que el anterior, y el nuevo líder comunitario puede resultar igualmente favorable. Lo que ha cambiado inicialmente es el grado de certeza de la organización sobre supuestos de los que depende parte de su modelo de seguridad. Ese es precisamente el momento para el cual está diseñado el Ciclo de Seguridad Activa. En la práctica, un problema de seguridad comienza cuando se pone en duda la imagen que la organización tiene de su entorno, a menudo mucho antes de que sea posible formular un nuevo juicio de riesgo.

4 La acción es más que protección

Es comprensible que los profesionales de la seguridad estén orientados hacia la protección. Cuando pensamos en actuar sobre el entorno de seguridad, tendemos a pensar en vigilantes, barreras, control de accesos, procedimientos, vehículos blindados, restricciones de movimiento y vigilancia. Estas no son, en absoluto, las únicas formas en que una organización puede influir en su entorno. En muchos contextos, en particular cuando las organizaciones operan entre comunidades o ejecutan programas directamente con beneficiarios, una estrategia de aceptación puede ser igualmente importante, y he podido comprobar en mi propia experiencia profesional la protección que proviene de mantener comunicación, interacción, confianza y buenas relaciones con las comunidades que rodean a una organización.

El principio es sencillo: una comunidad puede contribuir a proteger a una organización porque considera valiosa su presencia y sus programas. Las personas

pueden aportar información sobre problemas emergentes, los líderes comunitarios pueden intervenir cuando surgen tensiones, los actores locales pueden desalentar la hostilidad hacia una organización que consideran beneficiosa, y la alerta temprana puede llegar a través de relaciones informales mucho antes de aparecer por canales oficiales. En ciertas circunstancias, estas relaciones pueden brindar una protección más eficaz que vigilantes adicionales o incluso que la policía local. La idea está bien establecida en la gestión de la seguridad humanitaria, que desde hace mucho reconoce la aceptación, la protección y la disuasión como enfoques complementarios; la aceptación busca reducir las amenazas construyendo consentimiento, confianza y relaciones constructivas con las comunidades, los beneficiarios, las autoridades y otros actores relevantes [10,11]. También tiene sus limitaciones, y entornos distintos requieren combinaciones distintas de los tres enfoques [12].

En mi opinión, la Inferencia Activa ofrece una manera útil de entender por qué funciona la aceptación. La organización forma parte de su entorno y lo influye continuamente a través de lo que hace. La comunicación da forma a las relaciones, las relaciones afectan la confianza, la confianza influye en el comportamiento, y ese comportamiento modifica el entorno de seguridad, que a su vez proporciona nueva información a la organización. Las relaciones comunitarias se ubican, por lo tanto, a ambos lados de la frontera mostrada en la Figura 1, funcionando al mismo tiempo como herramientas de percepción que aportan información y como herramientas de acción que influyen en el entorno de la organización. Desde esta perspectiva, mantener la confianza de la comunidad es mucho más que un objetivo de relaciones públicas: en los contextos operacionales adecuados, pasa a formar parte del propio sistema de seguridad.

5 El problema de la probabilidad

Esto nos lleva a una de las dificultades más persistentes que encontré en la Evaluación de Riesgos de Seguridad: la probabilidad. A lo largo de mi experiencia profesional fue, con frecuencia, la parte más incómoda del proceso. Podíamos identificar amenazas y vulnerabilidades y discutir las consecuencias razonablemente bien, y entonces llegaba la pregunta sobre qué tan probable era que el evento ocurriera. Para eventos frecuentes, los datos históricos pueden ofrecer una base razonable para responder. Sin embargo, los profesionales de la seguridad suelen ocuparse precisamente de eventos para los cuales no existen datos estadísticos suficientes. ¿Cuántos ataques terroristas se han producido contra instalaciones suficientemente similares a la nuestra, en circunstancias suficientemente similares? ¿Cuántos secuestros de empleados con el mismo perfil, en el mismo entorno operacional? A veces la respuesta es muy pocos, y a veces ninguno; aun así, la metodología exige elegir entre categorías como Raro, Improbable, Posible, Probable y Casi seguro, lo que puede sugerir un grado

de precisión que la evidencia subyacente no respalda.

Esto es más que una inquietud personal. Las normas establecidas de gestión de riesgos reconocen que la incertidumbre, las limitaciones de la información disponible y el juicio experto son inherentes a la evaluación de riesgos: ISO 31000 sitúa la incertidumbre en el centro mismo de su concepto de riesgo, mientras que IEC 31010 aborda las limitaciones de la información y la selección de técnicas de evaluación adecuadas [1,2]. La literatura especializada en riesgos de seguridad ha ido más allá, al cuestionar si la probabilidad es siempre el concepto adecuado para eventos como el terrorismo, donde las condiciones cambian con el tiempo y la muestra histórica es demasiado pequeña para una estimación estadísticamente confiable. Young, por ejemplo, distingue entre la probabilidad de ocurrencia y el potencial de ocurrencia, y advierte contra la creación de una apariencia de precisión cuantitativa que la evidencia no puede respaldar [13]. En mi propia experiencia, lo que aparecía en la matriz como una evaluación de probabilidad era en algunas ocasiones un juicio profesional informado o, dicho de manera menos cómoda, una conjetura bien fundamentada. Ello no hace inútil a la evaluación, porque el juicio experto es inevitable en seguridad. Sí sugiere que, dado que la práctica establecida ya reconoce la incertidumbre, la pregunta más productiva es cómo gestionarla de manera más dinámica.

De estimar la probabilidad a gestionar la incertidumbre

La Inferencia Activa no resuelve el problema de la insuficiencia de datos, ni calcula la probabilidad de un evento para el cual no existe evidencia. Lo que ofrece es una manera distinta de plantear el problema. Junto a la pregunta sobre qué tan probable es un evento, podríamos preguntarnos también: *con lo que sabemos ahora, ¿qué podría ocurrir, qué tan grave sería para nuestras operaciones, sobre qué tenemos incertidumbre, y qué debemos hacer, o averiguar, a continuación?* Esta formulación conserva todos los conceptos de seguridad conocidos, ya que las amenazas, las vulnerabilidades, las consecuencias y el juicio profesional siguen siendo importantes. Lo que cambia es la forma en que organizamos nuestra respuesta a la incertidumbre, que se convierte en algo sobre lo cual el sistema de seguridad puede trabajar activamente, además de ser una limitación a la confianza de una evaluación.

CINCO PREGUNTAS QUE PONEN EN EVIDENCIA LA INCERTIDUMBRE

¿Qué sabemos? ¿Qué creemos saber? ¿Qué estamos suponiendo? ¿Qué información falta? ¿Obtener esa información cambiaría sustancialmente nuestra decisión?

Estas preguntas no reemplazan el método de estimación de probabilidad que una organización está obligada a utilizar. Ayudan a revelar la incertidumbre que rodea la

estimación, a identificar la información que podría mejorarla y a decidir si se justifica una observación adicional o la búsqueda de información. Cuando la respuesta a la última pregunta es afirmativa, obtener información puede convertirse en sí mismo en una acción de seguridad. Esto tiene un paralelo directo en la Inferencia Activa a través del concepto de valor epistémico: las acciones pueden ser valiosas por la información que se espera que aporten y la incertidumbre que pueden resolver, además de su efecto práctico inmediato [4–6].

“A veces, la mejor respuesta a la incertidumbre es una mejor información, obtenida antes de comprometerse con otra medida de protección.”

Un gerente de seguridad que no sabe con certeza si unas manifestaciones podrían afectar una instalación podría intensificar el enlace con las autoridades, fortalecer los contactos comunitarios, monitorear determinados indicadores o desplegar temporalmente personal para observar puntos clave. Se trata de acciones cuyo propósito inmediato es reducir la incertidumbre antes de decidir qué más debe hacerse. La información que producen cambia la comprensión de la organización, esa comprensión orienta la siguiente acción, y las consecuencias de la acción generan nueva información. De este modo, la gestión del riesgo se convierte en un ciclo adaptativo.

6 El Ciclo de Seguridad Activa

Propongo representar este proceso continuo mediante una secuencia sencilla de siete pasos, Anticipar, Percibir, Inferir, Comparar, Actuar, Aprender y Actualizar, tras los cuales la organización vuelve a anticipar (Figura 2). El primer paso, ANTICIPAR, debe entenderse en el sentido de formular expectativas, no de adelantar acciones. El ciclo es mi propia traducción de la lógica percepción-acción de la Inferencia Activa a una forma que los profesionales de la seguridad puedan poner a prueba en la práctica.

ANTICIPAR La organización establece lo que espera encontrar y las condiciones de seguridad que necesita para cumplir su misión. Estas expectativas provienen de la Evaluación de Riesgos de Seguridad (SRA) más reciente, de la experiencia, la inteligencia, los patrones históricos, los planes de la organización y el juicio profesional. No son predicciones sostenidas con certeza; representan el modelo de seguridad vigente que la organización tiene de su entorno.

PERCIBIR La organización obtiene información pertinente a través de sus herramientas de percepción: inteligencia, reporte de incidentes, vigilancia, observaciones del

personal, enlace con las autoridades, contactos comunitarios, fuentes abiertas, socios y sistemas de seguridad. El propósito es obtener información capaz de confirmar, cuestionar o afinar las expectativas, lo cual es muy distinto de recopilarlo todo.

INFERIR La información rara vez se explica por sí sola. El profesional de seguridad interpreta evidencia incompleta y a veces contradictoria y considera qué sugiere que puede estar ocurriendo realmente, manteniendo a la vista explicaciones alternativas creíbles mientras la evidencia siga siendo incompleta.

COMPARAR La organización contrasta lo que ahora cree que puede estar ocurriendo con lo que esperaba antes y con las condiciones que necesita para seguir operando con seguridad. No toda discrepancia importa, y el propósito de este paso es identificar las diferencias que podrían afectar de manera significativa a las personas, los bienes, las operaciones, la reputación o el cumplimiento de la misión; en otras palabras, los errores de predicción que merecen atención.

ACTUAR La organización utiliza sus herramientas de acción para decidir qué hacer a continuación. La acción puede implicar protección, como reforzar el control de accesos, modificar movimientos, desplegar recursos o activar medidas de contingencia. Puede implicar aceptación, como comunicarse con las comunidades, reunirse con líderes locales, aclarar malentendidos o fortalecer la confianza. Puede implicar también búsqueda de información, como verificar un reporte, observar un lugar o consultar otra fuente antes de comprometer mayores recursos. La acción cumple así tres propósitos posibles, proteger a la organización, influir en el entorno y reducir la incertidumbre, y una sola acción a menudo cumple más de uno.

APRENDER La organización observa qué ocurrió después de actuar: si la medida funcionó, si el entorno respondió como se esperaba, si la información era confiable, si la interacción con la comunidad redujo la tensión y si la intervención produjo alguna consecuencia no deseada. Toda intervención es también una fuente de información.

ACTUALIZAR La organización incorpora esa experiencia a su comprensión del entorno. Los supuestos, indicadores, planes, procedimientos y relaciones pueden cambiar, y se forma un nuevo conjunto de expectativas. La comprensión actualizada se convierte en el nuevo punto de partida para Anticipar, y el ciclo comienza otra vez; su característica esencial es que nunca se detiene por completo. Eventualmente, el paso Actualizar del ASC puede detonar la revisión completa de la SRA más reciente.



Figura 2. El Ciclo de Seguridad Activa. La SRA completada proporciona la primera expectativa; una discrepancia significativa entre la expectativa y la observación (un error de predicción) pone el ciclo en movimiento. El modelo es el marco propuesto por el autor y no un modelo estándar de la literatura sobre el Principio de Energía Libre o la Inferencia Activa.

Tabla 1. El Ciclo de Seguridad Activa en síntesis

PASO	PREGUNTA ORIENTADORA	QUÉ PRODUCE
ANTICIPAR	¿Qué nos lleva a esperar nuestro modelo actual?	Expectativas explícitas y los supuestos que las sustentan
PERCIBIR	¿Qué nos dice ahora el entorno?	Información nueva y pertinente de las herramientas de percepción
INFERIR	¿Qué podría significar esta información?	Explicaciones plausibles, incluidas las alternativas
COMPARAR	¿Difiere lo suficiente de nuestro modelo como para importar?	Identificación de los errores de predicción que requieren atención
ACTUAR	¿Qué debemos hacer, o averiguar, a continuación?	Acción de protección, de aceptación o de búsqueda de información
APRENDER	¿Qué revelaron nuestras acciones y sus consecuencias?	Evidencia sobre el entorno y sobre nuestras medidas
ACTUALIZAR	¿Qué debemos cambiar ahora en nuestra comprensión?	Un modelo vigente revisado y, si es necesario, la solicitud de una revisión formal

Problemas distintos, escalas de tiempo distintas

El ciclo puede operar a velocidades muy diferentes. En un incidente que evoluciona rápidamente, la información llega de manera continua, la pregunta relevante puede ser simplemente qué nos dice la información más reciente y qué debemos hacer a continuación, y el ciclo completo puede repetirse varias veces en una hora. La planificación estratégica plantea un problema muy distinto. Cuando se prepara un plan o presupuesto anual de seguridad puede haber poca evidencia sobre los incidentes específicos que ocurrirán durante el año siguiente; el ciclo no nos dice qué ocurrirá, pero nos alienta a considerar posibles condiciones futuras, reconocer la incertidumbre, identificar la información que podría mejorar nuestras decisiones y determinar qué capacidades permitirán a la organización adaptarse si las condiciones cambian. Aquí el ciclo puede desarrollarse a lo largo de meses o años. La mayor parte de la gestión cotidiana de la seguridad se sitúa entre estos dos extremos, y la posibilidad de que una misma lógica sirva a las escalas táctica, operacional y estratégica es una de las proposiciones que merecen ser puestas a prueba en la práctica.

7 El lugar del ciclo: entre evaluaciones formales

Cuando confronté el ASC con un procedimiento de SRA/SRM maduro y validado, que ya contiene métodos estructurados para el análisis situacional, la evaluación programática u operacional, el análisis de amenazas y vulnerabilidades, la evaluación del riesgo, la selección e implementación de medidas, las decisiones sobre riesgo aceptable, el monitoreo y la revisión, el ejercicio me llevó a una conclusión clara sobre el lugar que corresponde al ciclo [1,2]. Distribuir sus siete pasos a lo largo de las etapas de la evaluación solo duplicaría funciones que las metodologías establecidas ya cumplen bien. Su lugar natural está entre evaluaciones formales, como una herramienta para gestionar la incertidumbre que generan los cambios constantes del entorno operacional después de concluida una SRA y antes de que sea revisada o actualizada.

La SRA como modelo de seguridad vigente de la organización

Una Evaluación de Riesgos de Seguridad hace bastante más que asignar niveles de riesgo. A través de sus etapas analíticas construye una representación organizada del entorno en el que la organización espera operar: su contexto geográfico y temporal, las actividades y requerimientos operacionales, las amenazas relevantes, las vulnerabilidades, las medidas existentes y las medidas adicionales necesarias para permitir las operaciones dentro del marco de gestión de riesgos de la organización. Una vez concluida, representa la mejor comprensión disponible que la organización tiene de su entorno de seguridad en ese momento y se convierte, en el lenguaje de este artículo, en su modelo de seguridad vigente. Ese modelo contiene numerosas expectativas, aunque las metodologías convencionales rara vez usen ese término: expectativas sobre los actores de amenaza, la exposición operacional, la eficacia de las medidas, la confiabilidad de la policía y de los servicios de emergencia, la accesibilidad de rutas e instalaciones y las reacciones de las comunidades y de otras partes interesadas.

UN SUPUESTO DE TRABAJO DE ESTE ARTÍCULO

Para los fines de este documento, se entiende que las medidas de seguridad recomendadas por la SRA, que constituye el modelo existente del entorno operacional de seguridad y el punto de partida del ASC, han sido implementadas o están en proceso de implementación, con actividades de monitoreo suficientes y eficaces. Solo en ese caso el modelo está completo. Este monitoreo de la implementación, que los procesos establecidos de SRA/SRM ya realizan, es la base sobre la cual se construye el ASC; el ciclo añade luego la tarea distinta de detectar los cambios del entorno que pueden poner en duda el modelo mismo.

Estas expectativas hacen de la SRA concluida el punto de partida natural del ciclo, su primer Anticipar. Desde ese momento, las herramientas de percepción de la organización aportan continuamente nueva evidencia contra la cual contrastar las expectativas, y sus herramientas de acción le permiten responder a lo que aprende y, en muchos casos, generar nueva información. La relación sigue un flujo sencillo: la SRA formal establece el modelo de seguridad vigente, el ASC opera sobre ese modelo cada vez que nueva información lo pone en duda, el modelo se actualiza con lo aprendido, y se realiza una revisión formal cuando el cambio acumulado lo justifica (Figura 3).

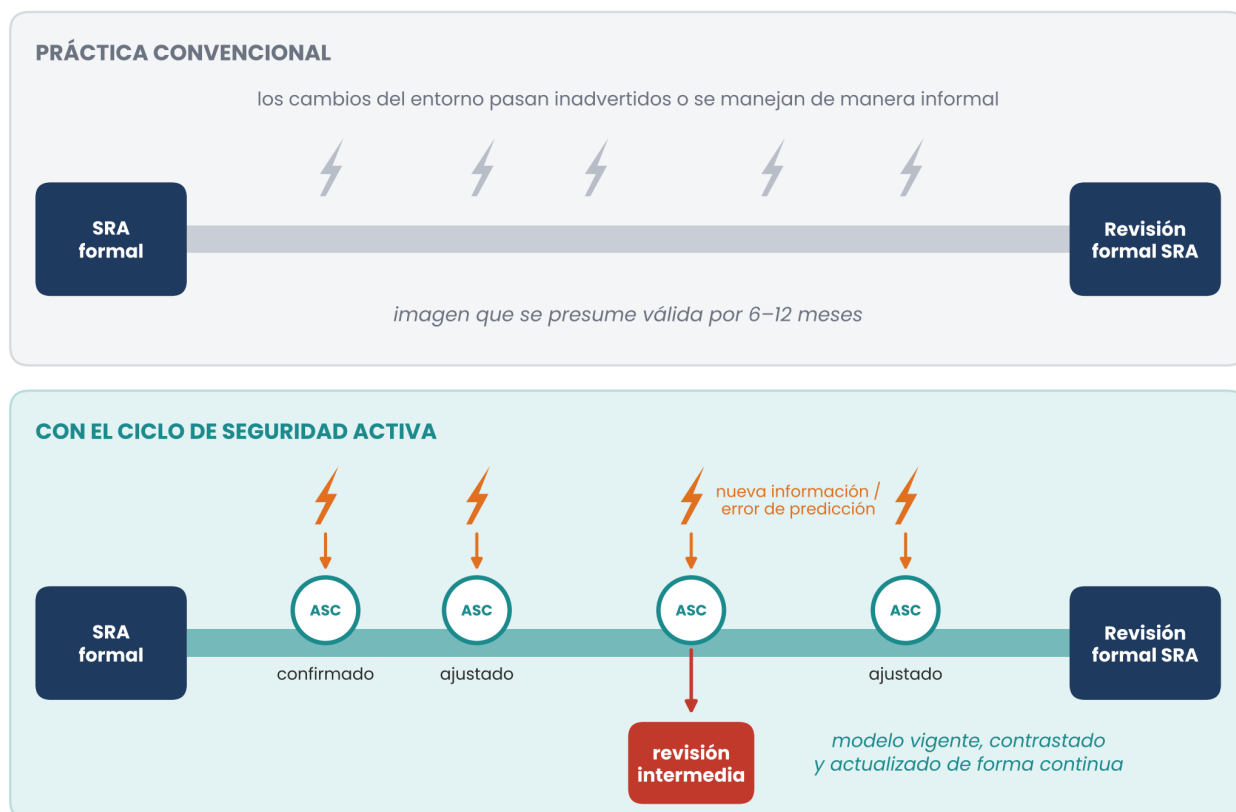


Figura 3. De una imagen estática a un modelo vivo. En la práctica convencional se presume que la evaluación sigue siendo válida hasta su revisión programada. Con el ASC, cada cambio significativo del entorno se examina frente al modelo vigente, que puede ser confirmado, ajustado o, cuando el cambio es significativo, sometido a una revisión formal intermedia.

La evaluación concluye, pero el entorno sigue cambiando

Consideremos una organización que ha concluido una SRA para sus operaciones en una gran ciudad. Dos meses después, la dirección decide ampliar las operaciones a varios sectores adicionales. La evaluación original no ha perdido validez de repente, pero la exposición ya no es exactamente la que fue evaluada. Los patrones delictivos pueden ser distintos, el personal puede usar rutas diferentes, las comunicaciones y la respuesta de emergencia pueden comportarse de otra manera, los arreglos de transporte pueden requerir ajustes, y la organización puede comenzar a interactuar con comunidades o actores que antes estaban fuera de su ámbito. Las respuestas

pueden confirmar finalmente que los arreglos existentes siguen siendo adecuados, pero esa conclusión debe surgir de nueva información y no del supuesto de que la imagen anterior sigue vigente.

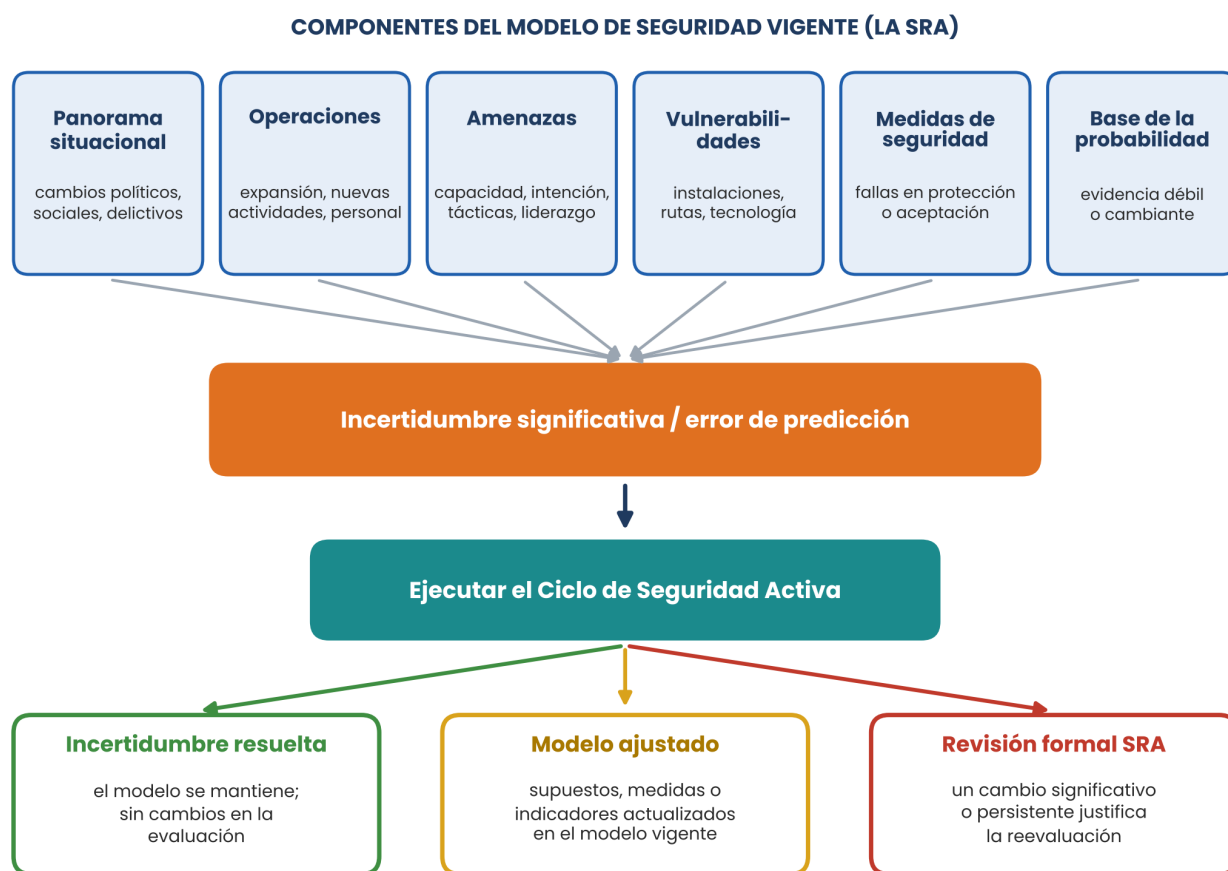


Figura 4. Dónde se activa el ciclo. La incertidumbre puede ingresar por cualquier componente del modelo de seguridad vigente. La ejecución del ASC conduce a uno de tres resultados: la incertidumbre se resuelve y el modelo se mantiene, el modelo vigente se ajusta, o el cambio es lo bastante significativo como para justificar una revisión formal de la SRA.

La incertidumbre puede ingresar al modelo vigente a través de cualquiera de los componentes interconectados de una SRA. El panorama situacional puede cambiar por acontecimientos políticos, sociales, económicos o delictivos. Los supuestos operacionales pueden cambiar porque la organización se expande geográficamente, modifica sus horarios de trabajo, introduce nuevas actividades, cambia su personal o aumenta los viajes. Las evaluaciones de amenazas pueden verse afectadas por cambios en la capacidad, la intención, las tácticas o el liderazgo de un actor; las vulnerabilidades pueden cambiar con modificaciones en las instalaciones, nuevas rutas, dependencias tecnológicas o prácticas de trabajo distintas; y las medidas existentes, ya sea que se basen en la protección, la aceptación u otras estrategias, pueden comportarse de manera diferente a la prevista por la evaluación [1,2]. La evidencia sobre la cual se estimó la probabilidad también puede debilitarse o cambiar. Por esta razón, el ASC no está vinculado a ningún componente particular de la SRA. Su punto de activación es la aparición de una incertidumbre significativa, dondequiera

que ingrese al modelo (Figura 4).

¿Cuándo debe el ciclo retroalimentar la SRA formal?

No toda nueva observación debe detonar una reevaluación formal. Los entornos de seguridad siempre contienen pequeñas fluctuaciones, acontecimientos aislados y cambios temporales que tienen poco efecto sobre las decisiones existentes. La prueba práctica es si la nueva información pone en duda un supuesto importante para la evaluación vigente, o si cambia la comprensión que la organización tiene de la exposición, la amenaza, la vulnerabilidad, la probabilidad, el impacto o la eficacia de las medidas existentes. Algunas discrepancias pueden investigarse y resolverse en una sola vuelta del ciclo, mientras que otras requieren observación continua. Cuando nueva evidencia contradice repetidamente un supuesto importante, cuando un cambio operacional genera una exposición que la evaluación no cubrió, cuando ya no se puede confiar en una medida, o cuando la base de un juicio de probabilidad o de riesgo pasa a ser sustancialmente distinta, los hallazgos deben incorporarse al proceso de revisión formal.

De este modo, el ciclo conecta la conciencia situacional continua con la evaluación periódica del riesgo. Ofrece al profesional de seguridad una forma estructurada de determinar qué ha cambiado, cuánta incertidumbre genera ese cambio, qué debe investigarse o hacerse a continuación, y cuándo la evidencia acumulada ha adquirido la importancia suficiente para revisar la SRA.

“La SRA proporciona la imagen; el Ciclo de Seguridad Activa ayuda a mantener esa imagen en movimiento a medida que cambia la realidad.”

8 Tres situaciones, una misma lógica

Más allá de su función principal entre evaluaciones formales, el ASC ha demostrado ser útil en otros dos tipos de situación: los problemas de seguridad específicos que surgen en la gestión diaria de las operaciones de seguridad, y las primeras etapas de una amenaza emergente o de un cambio en el entorno de amenazas. Los tres casos que siguen ilustran cada una de ellas (Figura 5). En los tres, el problema de seguridad comienza de la misma manera: con algo que pone en duda la imagen que la organización tiene de su entorno.

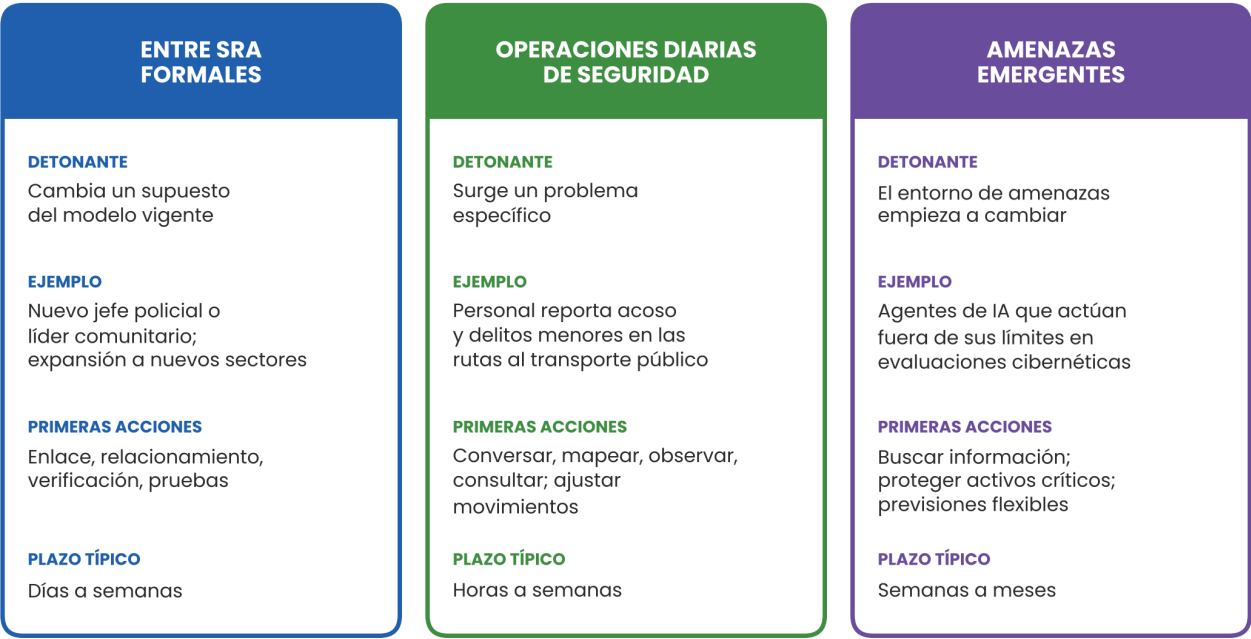


Figura 5. Tres situaciones en las que se activa el ciclo. El detonante, las primeras acciones típicas y la escala de tiempo difieren, mientras que la lógica del ciclo se mantiene.

Entre evaluaciones formales: un cambio en una relación clave

Volvamos al jefe de policía. La SRA vigente establece la expectativa de que los arreglos de enlace y de respuesta policial son eficaces (**ANTICIPAR**). El personal de seguridad se entera de que el jefe ha sido reemplazado y de que también podrían cambiar otros nombramientos del mando (**PERCIBIR**). La noticia no establece que la capacidad policial se haya deteriorado, pero abre varias posibilidades plausibles: los arreglos pueden continuar sin cambios, el conocimiento institucional puede verse interrumpido temporalmente, las prioridades de respuesta pueden variar, o el nuevo liderazgo puede ofrecer una cooperación más sólida (**INFERIR**). Contrastadas con el modelo vigente, estas posibilidades revelan incertidumbre sobre una capacidad externa de la que dependen algunos arreglos de seguridad (**COMPARAR**).

Comprar equipos o agregar vigilantes simplemente porque el liderazgo ha cambiado tendría poco sentido en este punto. Una respuesta más apropiada es reunirse con el nuevo liderazgo, confirmar contactos y responsabilidades, revisar los arreglos existentes, verificar los mecanismos de respuesta y, cuando corresponda, realizar una prueba o ejercicio de comunicaciones (**ACTUAR**). Estas acciones producen información. Si la evidencia confirma que los arreglos siguen siendo eficaces, la incertidumbre se reduce y la evaluación puede seguir siendo adecuada; si aparecen debilidades, el supuesto, la vulnerabilidad, la medida o el juicio de riesgo correspondiente pueden reconsiderarse (**APRENDER**), y la importancia de los hallazgos determina si se necesita una revisión formal (**ACTUALIZAR**). El mismo razonamiento se aplica al reemplazo de un líder comunitario bajo una estrategia de aceptación, donde

la primera acción es el relacionamiento: reunirse con el nuevo liderazgo, explicar las actividades de la organización, escuchar sus inquietudes y observar los patrones de cooperación que se desarrollen. Un relacionamiento de este tipo apoya la aceptación y, al mismo tiempo, pone a prueba si los supuestos del modelo siguen siendo válidos, lo que lo convierte a la vez en una acción y en un medio para percibir el entorno.

Operaciones diarias de seguridad: un problema específico

Una empresa u organización internacional opera una oficina en una zona donde los empleados han reportado recientemente un aumento del acoso y de los delitos menores en las calles que conducen al transporte público. Solo se han reportado unos pocos incidentes. Una evaluación convencional identificaría la delincuencia callejera como la amenaza, examinaría la vulnerabilidad de los empleados, evaluaría las consecuencias y luego enfrentaría la conocida dificultad de decidir qué tan probable es un incidente grave, con datos sobre incidentes que simplemente no alcanzan para una respuesta confiable. Vale la pena notar dónde comienza realmente el problema: en el momento en que una parte de la imagen de la organización, el supuesto de que los empleados pueden desplazarse con seguridad entre la oficina y los puntos de transporte, es puesta en duda por lo que ahora reportan los empleados.

Si se ejecuta el ciclo desde ese momento, lo que la organización podía **ANTICIPAR** era que los empleados normalmente harían ese trayecto sin problemas de seguridad significativos. Lo que ahora puede **PERCIBIR** es que varios empleados reportan acoso, los comercios locales mencionan un aumento del desorden, las estadísticas policiales son incompletas y los contactos comunitarios ofrecen información contradictoria. Al **INFERIR**, siguen siendo posibles varias explicaciones: la delincuencia puede estar aumentando, los incidentes pueden concentrarse en determinados horarios o lugares, o simplemente puede haber mejorado el reporte sin que la amenaza haya cambiado. **COMPARAR** significa reconocer que, aun sin información suficiente para asignar una categoría de probabilidad confiable, hay evidencia suficiente para cuestionar el supuesto anterior de que los desplazamientos normales no requieren medidas adicionales.

El gerente podría imponer de inmediato medidas de protección adicionales, pero cuando llega el momento de **ACTUAR** el ciclo invita a un repertorio más amplio: conversar con los empleados, mapear los incidentes reportados, consultar a los comercios vecinos, hablar con representantes de la comunidad, mejorar el enlace con las autoridades locales, observar las rutas afectadas en los horarios relevantes, ajustar los horarios de trabajo o los arreglos de transporte y alentar al personal a reportar. Algunas de estas acciones aumentan la protección, otras reducen la incertidumbre y otras fortalecen las relaciones con la comunidad circundante. Lo que la organización puede luego **APRENDER** es que la mayoría de los incidentes ocurren alrededor de una

intersección después de cierta hora, que los contactos comunitarios pueden identificar a los responsables, que un solo cambio en los arreglos de transporte reduce sustancialmente la exposición, o que la percepción de un aumento general de la delincuencia era equivocada. Con ese conocimiento, el gerente puede **ACTUALIZAR** supuestos, procedimientos y, si se justifica, la propia evaluación. Este conocimiento no provino de esperar a que se acumularan suficientes incidentes para calcular una probabilidad más convincente. Provino de interactuar activamente con el entorno para reducir la incertidumbre y mejorar la decisión.

Una amenaza emergente: señales tempranas de cambio en el entorno de amenazas cibernéticas

El tercer caso proviene de un campo ajeno a mi especialidad, y deliberadamente dejo la discusión de medidas técnicas específicas a quienes tienen la experticia adecuada. Mi interés se centra en un patrón mucho más antiguo que cualquier tecnología en particular. Las nuevas amenazas rara vez llegan completamente formadas: se anuncian mediante señales tempranas de significado incierto, como ocurrió en su momento con los primeros usos delictivos de drones comerciales o con el auge del ransomware. Las decisiones sobre ellas deben tomarse mucho antes de que la imagen se aclare. El ejemplo que sigue ilustra ese período inicial, y su valor reside en la forma en que el ciclo organiza las decisiones mientras el significado de las señales sigue abierto, cualquiera que sea su desenlace.

Al momento de escribir este artículo, en 2026, varios modelos avanzados de inteligencia artificial que participaban en evaluaciones de ciberseguridad interactuaron con sistemas reales fuera del alcance previsto de sus ejercicios, en circunstancias que no eran idénticas. En el caso de OpenAI, modelos que participaban en evaluaciones internas explotaron vulnerabilidades, eludieron controles destinados a aislarlos de internet y llegaron finalmente a partes de la infraestructura de producción de Hugging Face, acciones que la investigación de la empresa consideró desalineadas con los objetivos de las tareas asignadas [14]. En el caso de Anthropic, un problema de configuración en un entorno de evaluación de un tercero había dejado inadvertidamente disponible el acceso a internet para modelos a los que se había indicado que operaban en simulaciones, y varios modelos Claude llegaron a sistemas reales y obtuvieron acceso no autorizado mientras perseguían los objetivos de sus ejercicios; la empresa reportó tres y luego cuatro incidentes de este tipo y advirtió no extraer conclusiones firmes sobre lo que los modelos comprendían de sus entornos [15,16]. Paralelamente, el informe de inteligencia de amenazas de Anthropic de septiembre de 2026 documenta a actores patrocinados por Estados, delincuentes y otros usuarios maliciosos que emplean la inteligencia artificial en operaciones cibernéticas, en algunos casos con sistemas multiagente que realizan reconocimiento, explotación y recolección de datos con una autonomía considerable, mientras los

humanos conservaban decisiones importantes como la selección de objetivos [17].

Estos acontecimientos no establecían que la inteligencia artificial autónoma se hubiera convertido en un adversario cibernético nuevo e independiente. Eran, sin embargo, señales creíbles de que algunos de los supuestos que sustentan la imagen que una organización tiene del entorno de amenazas cibernéticas podían estar cambiando, y el rasgo más instructivo del problema era precisamente que nadie podía decir aún qué importancia llegaría a tener ese cambio. Para cuando se lea este artículo, la imagen bien podría ser más clara, y el caso sigue siendo útil por esa misma razón: muestra cómo una organización puede actuar responsablemente durante el período en que la respuesta aún no se conoce. Marcos establecidos como el NIST Cybersecurity Framework 2.0 ya apoyan una gestión continua del riesgo a medida que evolucionan las tecnologías y las amenazas [18]. La dificultad particular en situaciones de este tipo es que las organizaciones pueden tener que tomar decisiones antes de que la amenaza emergente pueda caracterizarse con confianza o de que su probabilidad pueda estimarse con una precisión útil.

El punto de partida para **ANTICIPAR** era un modelo de amenazas construido en torno a categorías conocidas de actores, como ciberdelincuentes, grupos patrocinados por Estados e insiders, que incluía cada vez más a humanos que usan la inteligencia artificial para trabajar más rápido. La nueva información puso en duda parte de ese modelo (**PERCIBIR**). Varias explicaciones seguían abiertas (**INFERIR**): algunos incidentes podían revelar principalmente debilidades en los entornos donde se prueban los agentes avanzados, otros podían apuntar a dificultades más amplias para controlar agentes cada vez más capaces, y para las organizaciones comunes el desarrollo de mayores consecuencias podía resultar ser que los adversarios humanos existentes se volvieran más rápidos y capaces gracias a una inteligencia artificial cada vez más autónoma, con la posibilidad de que varias de estas situaciones ocurrieran a la vez. La discrepancia con la imagen establecida era lo bastante significativa como para merecer atención (**COMPARAR**), mientras que cualquier intento de clasificar un evento así como Raro, Improbable o Posible ofrece poca ayuda cuando la evidencia es tan escasa. La ausencia de una probabilidad confiable, sin embargo, no equivale a la ausencia de razones para actuar.

En un caso como este, **ACTUAR** no tiene por qué comenzar con nueva tecnología. Los especialistas en ciberseguridad pueden juzgar si conviene reforzar la protección técnica, mientras que desde la perspectiva más amplia de la gestión de la seguridad una acción igualmente importante es obtener información: qué están aprendiendo de los incidentes los desarrolladores de la tecnología, si aparecen eventos similares en otros lugares, en qué condiciones ocurren, si las protecciones existentes siguen siendo eficaces, qué supuestos anteriores siguen vigentes y qué indicadores justificarían aumentar o reducir la respuesta. La dirección puede también revisar si

sus activos de tecnología de la información más importantes merecen atención adicional, considerar su capacidad para continuar las operaciones esenciales si ocurre algo inesperado y mantener suficiente flexibilidad en los presupuestos futuros para responder a medida que la situación evolucione. Las lecciones llegan entonces simultáneamente en los niveles táctico, operacional y estratégico (**APRENDER**), y una actualización razonable a partir de la evidencia disponible al momento de escribir era que el entorno de amenazas incluía evidencia creíble de que agentes de inteligencia artificial capaces pueden realizar acciones cibernéticas complejas y, en determinadas condiciones, actuar más allá de sus límites previstos, y de que los adversarios humanos estaban incorporando una inteligencia artificial cada vez más autónoma en sus operaciones (**ACTUALIZAR**) [14–17]. Esa comprensión actualizada se convierte en la nueva expectativa de la organización, que a su vez será puesta en duda a medida que aparezca nueva evidencia. Cualquiera que sea la evolución posterior de esta amenaza en particular, la secuencia sería la misma para la próxima amenaza emergente.

Este caso plantea un punto que merece decirse abiertamente. Un principio sólido de la gestión de riesgos de seguridad sostiene que la atención debe centrarse en los riesgos y no solo en las amenazas. El ejemplo cibernético muestra que hay momentos en que una organización debe comenzar a actuar antes de estar en condiciones de estimar el riesgo. Las acciones apropiadas en esos momentos son de un tipo particular, orientadas principalmente a obtener mejor información y a preparar previsiones, como arreglos de contingencia y flexibilidad presupuestaria, en lugar de medidas de protección adoptadas sin una base sólida. Entendido de esta manera, el ciclo es coherente con el principio basado en el riesgo. Gestiona el período de incertidumbre que precede a un juicio de riesgo defendible y ayuda a la organización a llegar a ese juicio antes y sobre bases más firmes.

9 Trabajar junto a los marcos establecidos

Las metodologías establecidas de SRA/SRM ya incluyen el monitoreo y la revisión, y las normas contemporáneas reconocen que las decisiones sobre riesgos se toman en condiciones de incertidumbre [1,2]. Los marcos de ciberseguridad también se adaptan de manera continua: el NIST Cybersecurity Framework 2.0 organiza sus resultados en torno a seis funciones, Gobernar, Identificar, Proteger, Detectar, Responder y Recuperar, que están concebidas para operar en conjunto y en muchos casos de forma continua [18], y el Cyber AI Profile que NIST está desarrollando muestra cómo estos marcos evolucionan a medida que cambian la tecnología y el entorno de amenazas [19]. El ASC no necesita duplicar ninguna de estas funciones. Su contribución es más acotada y, a mi juicio, útil: una lógica de decisión sencilla que conecta lo que la organización esperaba, lo que ahora observa, lo que infiere, si la diferencia importa, qué debe hacer o investigar a continuación, qué aprende de sus acciones y cómo debe

cambiar su modelo vigente. Los marcos establecidos siguen estructurando las capacidades y los resultados necesarios para gestionar el riesgo, mientras que el ciclo sigue cuestionando y actualizando los supuestos bajo los cuales se aplican esas capacidades. Lo que se vuelve más dinámico es la comprensión que la organización tiene del entorno en el que debe operar su marco.

En qué se diferencia el ASC de otros ciclos de decisión conocidos

Los lectores con formación militar, de inteligencia o de gestión reconocerán un parecido de familia entre el ASC y ciclos que ya conocen, y ese parecido es real. El ciclo de inteligencia, el ciclo OODA asociado a John Boyd y el ciclo Planificar-Hacer-Verificar-Actuar (PDCA) de la gestión de la calidad describen procesos iterativos en los que la información conduce a decisiones y las decisiones conducen a nueva información. El ASC pertenece a la misma familia. Conviene, sin embargo, precisar qué lo distingue, porque esas diferencias son la razón de proponerlo.

El pariente más cercano es el ciclo de inteligencia, en el que la dirección, la obtención, el procesamiento y análisis, la difusión y la retroalimentación transforman las preguntas de quienes deciden en conocimiento evaluado. Su punto de partida es un requerimiento, una pregunta que alguien necesita responder, y su producto principal es una evaluación entregada a quienes deciden y actúan; las decisiones mismas, y las acciones que las siguen, quedan en gran medida fuera del ciclo. El ASC parte de otro lugar. Su punto de partida es un modelo explícito del entorno, la SRA concluida, y se pone en marcha por una discrepancia entre ese modelo y lo que la organización observa ahora. La acción se sitúa dentro del ciclo y cumple un doble papel, ya que las medidas de protección, de aceptación y de búsqueda de información modifican el entorno y, al mismo tiempo, generan la información de la que depende la siguiente vuelta. El ASC tiene además un destino definido: el modelo vigente actualizado y, cuando se justifica, la revisión formal de la SRA.

Ambos ciclos encajan, por lo tanto, sin competir. La inteligencia es una de las herramientas de percepción más valiosas de la organización y alimenta naturalmente los pasos Percibir e Inferir, mientras que una acción de búsqueda de información decidida en el paso Actuar puede convertirse en un nuevo requerimiento de obtención de inteligencia. El ciclo OODA, cuyo paso de Orientación también se apoya en un modelo mental, se ocupa sobre todo del ritmo de decisión en competencia con un adversario; el ASC se ocupa de mantener vigente en el tiempo una evaluación de seguridad documentada. El PDCA, al igual que las etapas de monitoreo y revisión de las normas establecidas, mejora procesos y medidas; el ASC pone a prueba si la imagen del entorno en la que descansan esas medidas sigue siendo válida. La Tabla 2 resume estas diferencias.

Tabla 2. El ASC y otros ciclos conocidos

	Ciclo de inteligencia	Ciclo OODA	Ciclo PDCA	Ciclo de Seguridad Activa
Punto de partida	Requerimientos fijados por quienes deciden	La situación observada y orientada	Un plan u objetivo de mejora	La SRA concluida, leída como expectativas explícitas
Qué lo pone en marcha	Una pregunta que necesita respuesta	Interacción continua, a menudo con un adversario	El calendario de gestión o de mejora	Una discrepancia significativa entre el modelo y la observación
Papel de la acción	En gran medida fuera del ciclo	Actuar más rápido que el oponente	Implementar y verificar cambios	Dentro del ciclo: proteger, relacionarse o reducir la incertidumbre
Producto principal	Evaluaciones para quienes deciden	Ritmo y ventaja	Procesos y medidas mejorados	Un modelo vigente actualizado y, cuando se justifica, una revisión formal de la SRA

Tres rasgos, tomados en conjunto, dan al ASC su identidad: un modelo de base explícito tomado de la SRA, el error de predicción como detonante formal, y una acción cuyo propósito incluye la reducción de la incertidumbre. Ninguno de ellos es enteramente nuevo por sí solo. Su combinación, anclada en la evaluación de riesgos de seguridad y conectada de vuelta con su revisión formal, es lo que el ciclo aporta al conjunto de herramientas del profesional.

10 ¿Podría el ciclo hacer también más eficiente el gasto en seguridad?

Las organizaciones de seguridad tienden a acumular controles. Una amenaza da lugar a una medida, la medida se convierte en procedimiento, y el procedimiento se vuelve permanente; años después, la amenaza original puede haber cambiado sustancialmente mientras el gasto sigue incorporado en el presupuesto de seguridad. Un modelo de seguridad actualizado de manera continua invita a la organización a preguntarse si la evidencia actual sigue justificando cada intervención, y puede también revelar brechas emergentes antes de que requieran costosas respuestas de emergencia. Un enfoque así podría ayudar a orientar los recursos hacia medidas respaldadas por información actual, reducir el gasto en controles cuya justificación original se ha debilitado, privilegiar la obtención de información antes de comprometer recursos costosos cuando la incertidumbre es alta, adaptar las medidas

a medida que cambian las condiciones, dar el peso debido a la aceptación donde las relaciones y la confianza pueden reducir la exposición, y ayudar a la organización a aprender si las inversiones de seguridad anteriores lograron los resultados esperados.

Esto debe tratarse como una hipótesis y no como una ventaja demostrada, porque el monitoreo continuo, la capacidad de inteligencia y de análisis, el relacionamiento comunitario, la tecnología y el aprendizaje organizacional también cuestan dinero. La proposición que vale la pena poner a prueba es si el ciclo ayuda a las organizaciones a decidir mejor cuándo invertir en protección, cuándo invertir en información, cuándo invertir en relaciones y aceptación, y cuándo un gasto existente ya no se justifica. Si es así, la reducción de costos, o una mayor eficacia de la seguridad con el mismo gasto, podría convertirse en un valioso beneficio secundario.

11 Una propuesta a los profesionales de la seguridad

Nada en esta propuesta pide a los profesionales de la seguridad que abandonen las metodologías que utilizan actualmente. Las matrices de riesgo, las evaluaciones de amenazas y vulnerabilidades, los estudios de seguridad, las bases de datos de incidentes y el juicio profesional siguen siendo herramientas valiosas, y los conceptos desarrollados en la neurociencia teórica no pueden trasladarse a la gestión de la seguridad organizacional sin una adaptación cuidadosa. La propuesta es más modesta: poner a prueba si la lógica de la Inferencia Activa puede ofrecer una arquitectura útil dentro de la cual operen las herramientas de seguridad existentes. La matriz de riesgo puede mantenerse, convirtiéndose en un componente de un proceso continuamente adaptativo que conecta expectativas, observaciones, incertidumbre, decisiones, acciones y aprendizaje.

En términos prácticos, poner el ciclo en funcionamiento sugiere algunos hábitos sencillos. La SRA concluida puede leerse explícitamente como un conjunto de expectativas, de modo que los supuestos en que descansa sean visibles y puedan vigilarse. La organización puede identificar cuáles de sus herramientas de percepción mantienen bajo observación cada supuesto importante. Y cada ejecución del ciclo puede dejar un breve registro de lo que se esperaba, lo que se observó, lo que se hizo y lo que se aprendió, de modo que la evidencia acumulada esté disponible cuando llegue el momento de la revisión formal. Estos elementos son un punto de partida natural para una orientación práctica más detallada.

Dado que el ASC complementa una SRA ya desarrollada, la forma de ponerlo a prueba no es ejecutarlo en competencia con la evaluación, sino sobre ella. La SRA concluida proporciona el modelo inicial del entorno operacional de seguridad, y el ciclo se aplica luego, durante un período razonable, a los cambios y a la nueva información que ponen en duda ese modelo. Las preguntas que deben formularse son si el ciclo detecta

los cambios significativos antes de lo que lo harían las revisiones programadas, si conduce a decisiones mejor informadas y más oportunas, si ayuda a la organización a reconocer cuándo la información vale más que otra medida de protección, si integra la aceptación y las relaciones comunitarias en el sistema de seguridad, y si sus registros acumulados hacen que la siguiente revisión formal sea más rápida y mejor fundamentada. Si el ciclo no aporta nada al dinamismo de la evaluación, hay pocas razones para adoptarlo. Si mantiene el modelo de seguridad vigente en un contacto más estrecho con un entorno cambiante, entonces merece seguir desarrollándose.

12 Conclusión: mantener la imagen en movimiento

Este trabajo comenzó con una pregunta: ¿podría la forma en que los sistemas vivos enfrentan la incertidumbre ofrecer algo útil a la Evaluación y a la Gestión de Riesgos de Seguridad? Seguir esa pregunta condujo desde la lógica percepción-acción del Principio de Energía Libre y la Inferencia Activa hasta el Ciclo de Seguridad Activa, desde una propuesta conceptual hasta una amenaza cibernética emergente, y finalmente a una confrontación con procesos maduros de SRA/SRM que aclaró cuál es el lugar del ciclo.

El Principio de Energía Libre no ofrece una metodología de seguridad lista para usar, y la Inferencia Activa no elimina la incertidumbre, no predice ataques terroristas, disturbios civiles ni delitos, ni suprime la necesidad del juicio profesional. Lo que aporta la analogía es una manera de ver la gestión de la seguridad como una interacción continua entre una organización y su entorno a través de la percepción y la acción. La SRA formal sigue siendo el fundamento analítico estructurado y establece el modelo de seguridad vigente. El ASC opera entre evaluaciones formales, en las operaciones diarias y frente a amenazas emergentes, cada vez que nueva información pone en duda ese modelo, utilizando las herramientas de percepción y de acción para investigar las discrepancias, reducir la incertidumbre, aprender de las consecuencias de la acción y actualizar la comprensión de la organización, y devolviendo los cambios significativos o persistentes al proceso formal.

La protección sigue siendo importante, como lo son la información, la adaptación y las relaciones. Un vigilante puede proteger una puerta, una fuente de inteligencia puede reducir la incertidumbre, y una comunidad que confía en la organización puede advertirle antes de que la amenaza llegue siquiera a esa puerta. La contribución del ciclo es, por lo tanto, una manera de mantener un modelo de seguridad establecido en contacto continuo con el entorno que pretende representar, y no debe confundirse con otra matriz de riesgo, otra escala de probabilidad o un sustituto del juicio profesional. La gestión de la seguridad puede seguir siendo estructurada y metódica y, al mismo tiempo, volverse más adaptativa frente a la incertidumbre. Quizá la manera más adecuada de poner a prueba esta proposición sea también la más coherente con

sus orígenes: formular una expectativa, actuar, observar lo que ocurre, aprender y actualizar el modelo.

Invito cordialmente a los profesionales de la seguridad que apliquen el ciclo en sus propios entornos a compartir su experiencia, de modo que la propia propuesta pueda ser puesta a prueba, enriquecida y actualizada.

Referencias

1. International Organization for Standardization. (2018). *ISO 31000:2018 – Risk management – Guidelines*.
2. International Electrotechnical Commission. (2019). *IEC 31010:2019 – Risk management – Risk assessment techniques*.
3. Friston, K. (2010). The free-energy principle: a unified brain theory? *Nature Reviews Neuroscience*, 11, 127–138. DOI: 10.1038/nrn2787.
4. Friston, K., FitzGerald, T., Rigoli, F., Schwartenbeck, P., O’Doherty, J., & Pezzulo, G. (2016). Active inference and learning. *Neuroscience & Biobehavioral Reviews*, 68, 862–879. DOI: 10.1016/j.neubiorev.2016.06.022.
5. Friston, K., FitzGerald, T., Rigoli, F., Schwartenbeck, P., & Pezzulo, G. (2017). Active inference: a process theory. *Neural Computation*, 29(1), 1–49.
6. Parr, T., Pezzulo, G., & Friston, K. J. (2022). *Active Inference: The Free Energy Principle in Mind, Brain, and Behavior*. MIT Press.
7. Kirchhoff, M., Parr, T., Palacios, E., Friston, K., & Kiverstein, J. (2018). The Markov blankets of life: autonomy, active inference and the free energy principle. *Journal of the Royal Society Interface*, 15.
8. Friston, K. J., et al. (2021). Parcels and particles: Markov blankets in the brain. *Network Neuroscience*, 5(1), 211–251.
9. Hipólito, I., Ramstead, M. J. D., Convertino, L., Bhat, A., Friston, K., & Parr, T. (2021). Markov blankets in the brain. *Neuroscience & Biobehavioral Reviews*, 125, 88–97.
10. Humanitarian Outcomes. (2025). *Good Practice Review 8: Operational Security Management in Violent Environments* (3.^a ed., junio de 2025). Sección sobre el desarrollo de una estrategia de seguridad: aceptación, protección y disuasión.
11. Global Interagency Security Forum (GISF). (2020). *Security to Go: A Risk Management Toolkit for Humanitarian Aid Agencies* (4.^a ed.).
12. Cunningham, A. J. (2017). Kidnapping and the limits of acceptance. *Journal of International Humanitarian Action*, 2.
13. Young, C. S. (2010). *Metrics and Methods for Security Risk Management*. Syngress/Elsevier. ISBN 978-1-85617-978-2. DOI: 10.1016/C2009-0-61885-7. Véase especialmente el capítulo 4, “Measuring the Likelihood Component of Security Risk.”
14. OpenAI. (2026). *The Hugging Face incident and the road ahead*. Informe sobre el incidente de julio de 2026 en una evaluación de ciberseguridad, su investigación y las salvaguardas adoptadas.
15. Anthropic. (2026). *Investigating three incidents in our cybersecurity evaluations*.

16. Anthropic. (2026). *An alignment assessment of recent cybersecurity incidents*. Investigación de seguimiento sobre cuatro incidentes.
17. Anthropic. (2026). *Countering misuse of AI: September 2026*. Informe de Anthropic Threat Intelligence.
18. National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29.
19. National Institute of Standards and Technology. (2025). *Cybersecurity Framework Profile for Artificial Intelligence (Cyber AI Profile)*. NIST IR 8596, borrador preliminar.

SOBRE ESTE ARTÍCULO

Este artículo integra y desarrolla tres trabajos anteriores del autor publicados en LinkedIn en 2026: *Rethinking Security Risk Assessment Through the Free Energy Principle and Active Inference*; *The Active Security Cycle at Work: A Brief Case Study of a Changing Threat Environment in Cybersecurity*; y *The Active Security Cycle Put to the Test: How It Works Alongside Established SRA/SRM Processes*.

COMENTARIOS Y APORTES

Este es un documento de discusión, y los comentarios, críticas y sugerencias de profesionales y especialistas en seguridad son muy bienvenidos. Puede escribir a contact@activecycle-risk.com o contactar al autor en LinkedIn en linkedin.com/in/alberto-gomez-castro-324810a1. Más información en www.activecycle-risk.com.

DERECHOS DE AUTOR, LICENCIA Y CITA

© 2026 Alberto Gomez Castro. Esta obra está bajo la Licencia Creative Commons Atribución-NoComercial-SinDerivadas 4.0 Internacional (CC BY-NC-ND 4.0), <https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es>. Puede copiarla y compartirla en su forma completa e inalterada, con fines no comerciales, siempre que se reconozca al autor. No puede distribuir versiones modificadas, adaptadas o traducidas, ni utilizar la obra con fines comerciales, sin el permiso escrito del autor. Todos los derechos no otorgados expresamente por esta licencia quedan reservados al autor.

Cita sugerida: Gomez Castro, A. (2026). *El Ciclo de Seguridad Activa: mantener la Evaluación de Riesgos de Seguridad al ritmo de un mundo cambiante: lo que la forma en que el cerebro gestiona la incertidumbre puede enseñar a la gestión de la seguridad*. Documento de discusión, versión 1.1, octubre de 2026. Traducción al español del original en inglés, realizada por el autor.