Ciberestrés

la situación en 2026

Un estudio realizado por
aDvens e ISMS Forum

Contenido

Ciberestrés: la situación en 2026

Síntesis

Aunque los indicadores más recientes apuntan a una mejora apreciable en las condiciones de trabajo de los responsables de ciberseguridad en materia de estrés laboral, persisten desafíos de considerable relevancia que no deben ser subestimados.

La naturaleza intrínsecamente exigente de esta función implica que el estrés asociado a su ejercicio debe seguir siendo **reconocido, evaluado y gestionado** de forma rigurosa y proporcional.

Aun cuando se observan ciertos avances en la percepción del estrés, la presión inherente al rol continúa siendo significativa y afecta a una parte importante del colectivo.

El objetivo primordial es garantizar que dicha presión no comprometa ni el nivel de seguridad global de las organizaciones ni el rendimiento y bienestar de quienes tienen la responsabilidad de salvaguardarlo.

Principales conclusiones

Un aspecto positivo es que los resultados muestran una mejora considerable en los niveles de estrés percibido: frente a 2024, donde el PSS situaba a un 39 % de los CISOs en zona roja, en 2026 esta franja se reduce al 23,1 %, y la media de estrés baja de 19,3 a 17,3 puntos.

Esta evolución apunta a una mayor consolidación del rol y a un entorno más preparado para gestionar la presión operativa.

Otra buena noticia es la mejora en el soporte personal: el porcentaje de CISOs que se sienten comprendidos o apoyados por sus allegados durante las crisis crece significativamente, pasando del 69,5 % registrado en 2024 al 86,7 % en 2026, lo que sugiere una mayor capacidad de afrontamiento y un entorno relacional más favorable.

Por otro lado, hemos notificado una caída espectacular en la percepción de imagen negativa de los CISOs, del 74% al 30,7%. Es el cambio más grande de todo el estudio (−43 puntos porcentuales) y sugiere un avance muy significativo en el reconocimiento de la profesión.

Pero hay que mantener la cautela: más de seis de cada diez responsables de ciberseguridad sigue estresado con frecuencia (61,5 %) y casi uno de cada cuatro sufre estrés elevado (23,1 %).

Aunque muchos factores de presión son inherentes al rol (p. ej., **57,3%** se siente cómodo con la adrenalina y la urgencia de una crisis), se observa una menor aceptación de los imprevistos (**del 41,5% al 32%**) y un ligero incremento de la sensación de impotencia ante la amenaza asimétrica (del 56,1 % al 60 %).

La vigilancia permanente también sigue siendo elevada, aunque baja ligeramente (del 61 % baja al 54,7 % que “no desconecta”).

Entonces, ¿es grave que aproximadamente el 61,5 % de los responsables de ciberseguridad (sumando los resultados del estrés moderado de la zona naranja y el estrés elevado de la zona roja) estén estresados?

Sigue siendo una cifra muy elevada y, sobre todo, continúa teniendo un impacto directo en la seguridad.

En un contexto de crecimiento de amenazas, ampliación de superficies de ataque y presión normativa, es imprescindible seguir reforzando el rol y las condiciones de trabajo del CISO para poder afrontar lo previsto y, sobre todo, los imprevistos y las exigencias del rol sin un estrés excesivo.

Cifras
a tener en cuenta

N = 75 para todas las preguntas de estresores (porque 9 personas dejaron vacío el bloque completo).

N = 78 para PSS10.

N = 84 para demografía.

57,3%

de los CISOs afirma sentirse cómodo con la adrenalina en 2026

La presión y la sensación de urgencia propias de una cibercrisis, lo que significa que más de cuatro de cada diez profesionales no toleran bien esa presión. Aunque la formulación de esta pregunta difiere ligeramente respecto a la de 2024 —donde el 74,4 % declaraba haber experimentado altos niveles de adrenalina y urgencia en cibercrisis—, la tendencia apunta a que la gestión emocional de estas situaciones sigue siendo un reto relevante para una parte significativa del colectivo.

Cifras
a tener en cuenta

Nuevas preguntas sobre sueños y angustia

El 54 % de los CISOs ha soñado con ciberataques (32,9 % ocasionalmente + 21,1 % en varias ocasiones), y el 57,9 % ha sentido una brecha entre su capacidad de acción y las expectativas de la organización.

EL 54,7% permanece en alerta constante sin poder desconectar

El 54,7 % permanece en alerta constante sin poder desconectar, indicador directamente relacionado con el miedo constante a que se produzca un ciberataque o una situación de alto riesgo.

EL 61,5 % presenta niveles de estrés relevantes

En España, donde se considera estresados a quienes se sitúan en las zonas naranja y roja, aproximadamente el 61,5 % de los responsables de ciberseguridad presenta niveles de estrés relevantes, lo que confirma que la presión sigue siendo elevada.

EL 85,3 % ha identificado sus factores de estrés

El 85,3 % de los encuestados ha identificado sus factores de estrés, pero solo el 33,3 % ha previsto un plan de acción, y el 69,3 % nunca ha solicitado formación o asistencia para gestionar su carga mental. Esta desconexión entre saber que hay un problema y actuar sobre él es una conclusión muy valiosa para las recomendaciones.

EL 42,1% ha dado su autorización a una postura de seguridad

El 42,1 % ha dado su autorización a una postura de seguridad que era contraria a sus convicciones por desánimo o angustia ante las negociaciones necesarias para defenderlas.

0.2 MUESTRA DEL ESTUDIO

El panel de encuestados procede de la comunidad de miembros del ISMS Forum, que reúne a r**esponsables de ciberseguridad de empresas y administraciones españolas**.

Las respuestas se recopilaron a través de un **cuestionario** publicado en línea por el **ISMS Forum**, que se completó durante **febrero de 2026.**

Rol del profesional

CISOs

Directores de IT

Expertos en ciberseguridad (gestión de riesgos y otros)

Tamaño de la organización

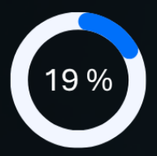
Organizaciones con menos de 1 000 empleados

Organizaciones con más de 1 000 empleados

Antigüedad en el puesto

<1 año

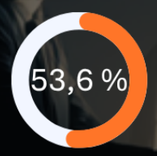
1–3 años



3–5 años

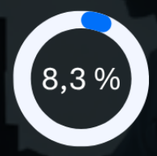
≥5 años

Tamaño de los equipos gestionados

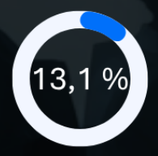


Equipos muy reducidos (1 – 5 personas)

Equipos pequeños/medianos (6 – 15 personas)

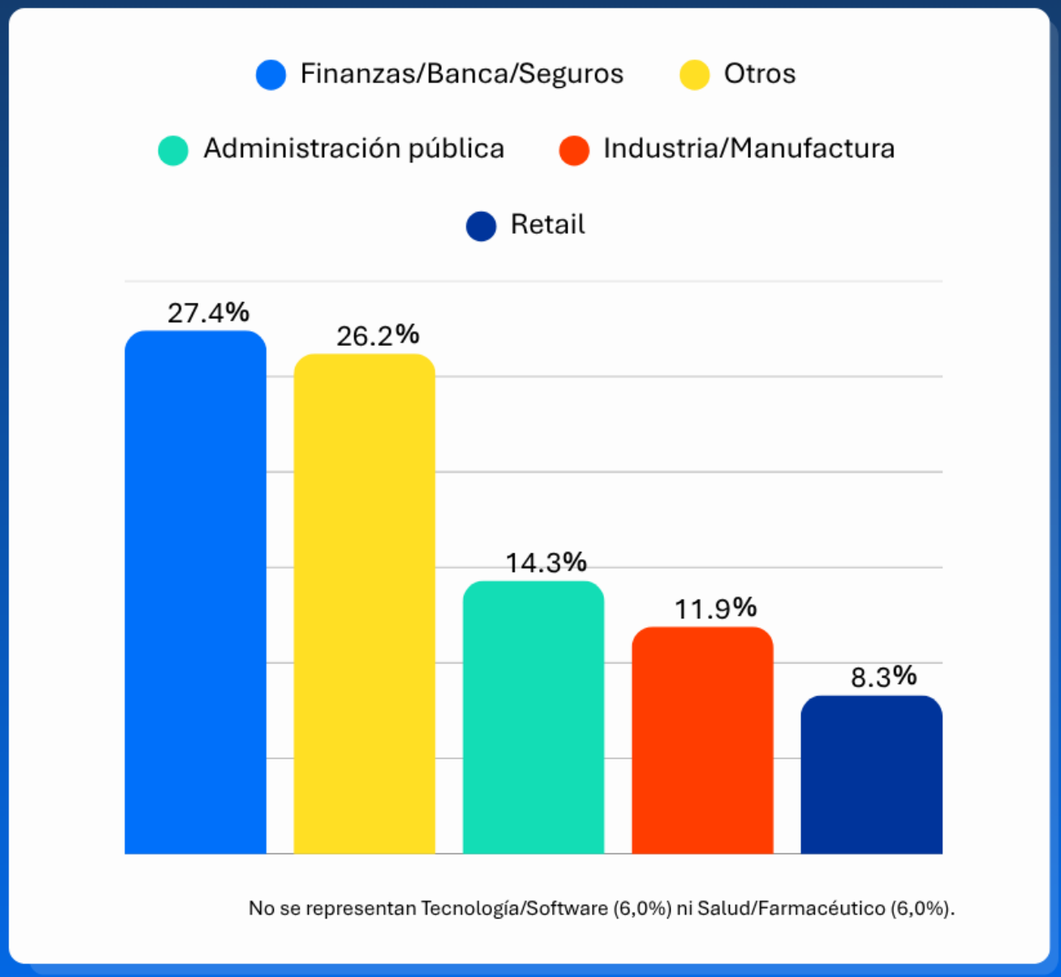


Equipos medianos/grandes (16 - 30 personas)



Equipos muy grandes (>= 30 personas)

Principales sectores representados



No se representan Tecnología/Software (6,0%) ni Salud/Farmacéutico (6,0%).

0.3 RECOPILACIÓN DE TESTIMONIOS

2026 trae una novedad significativa: por primera vez en esta edición, varios encuestados dieron un paso adelante y aceptaron compartir su experiencia de forma individual, con o sin anonimato.

Hablar de estrés no es tarea fácil. Hacerlo públicamente, menos aún. Por eso, el testimonio de estos profesionales tiene un valor especial: sus palabras dan vida a los datos, anclan los resultados en situaciones reales y abren pistas de reflexión sobre lo que los números, por sí solos, no siempre logran explicar. A lo largo de este documento, sus voces aparecerán donde más iluminan.

¿Qué mide —y qué no mide— este estudio?

Este estudio no pretende abarcarlo todo. Su foco es preciso: comprender el estrés tal y como lo vive un responsable de ciberseguridad debido a su profesión. Factores como la situación familiar, las dinámicas de equipo, las relaciones jerárquicas o la salud general de la organización quedan deliberadamente fuera del alcance del análisis —no porque sean irrelevantes, sino porque pertenecen a una esfera distinta.

Lo que sí se examina con detenimiento son los criterios que definen, de forma intrínseca, el ejercicio de esta función: sus exigencias propias, sus tensiones características, su singularidad.

¿Hacia un estado de madurez/edad de la razón?

1.1 2024-2026:

EVALUACIÓN Y EVOLUCIÓN DEL ESTRÉS PERCIBIDO

Ya utilizada en 2024, la escala de estrés percibido (Perceived Stress Scale o PSS) es un modelo de medición internacional reconocido que permite evaluar de manera global si una persona considera que tiene la capacidad de afrontar acontecimientos o momentos difíciles, sin especificarlos.

Para el estudio de 2026, la muestra de personas encuestadas varia respecto al informe general: de las **84 personas** que participaron en la encuesta, hubo **6 que no rellenaron las preguntas de la escala PSS10**, por lo que, para realizar el estudio de este apartado, la muestra definitiva será de **78 encuestados con PSS completo**.

Más información sobre la escala en el anexo

Al sumar las puntuaciones de las 10 preguntas formuladas (véanse los detalles más adelante), obtenemos un total comprendido entre 0 y 40 para cada participante. Las respuestas se codifican en una escala de 0 (Nunca) a 4 (A menudo). Las preguntas 4, 5, 7 y 8 son preguntas positivas y se puntúan de forma invertida, conforme a la metodología PSS10 estándar.

84

CISOs encuestados, de los cuales 78 tienen PSS completo

17,3

Score PSS medio

23,1%

En zona de riesgo (≥22)

7,7%

En riesgo de depresión clínica (dentro del estrés elevado)

En una primera lectura, los resultados muestran una evolución significativa en el perfil de estrés percibido entre 2024 y 2026. Mientras que en 2024 cerca de un tercio de los responsables de ciberseguridad se situaba en zona verde —niveles bajos de estrés— en 2026 este grupo crece moderadamente, representando el 38,5% de los participantes.

La zona naranja, correspondiente a niveles de estrés moderado, alcanza también el 38,5%.
Por su parte, la zona roja, asociada a niveles elevados de estrés, experimenta una reducción importante: del 39 % registrado en 2024 se desciende al 23,1% en 2026: una caída de casi 16 puntos porcentuales que representa una mejoría real en el bienestar de la comunidad CISO-española. Sin embargo, el grupo más preocupante, el de quienes superan los 28 puntos y se acercan al umbral de agotamiento, sigue siendo significativo (7,7 %, frente al 12,2 % registrado en 2024 para el mismo umbral).

En conclusión, en 2024, el 69,5 % de los CISOs españoles experimentaba estrés con efectos negativos (zona naranja + zona roja).
En 2026, esta proporción desciende al 61,5 %. El score medio baja de 19,3 a 17,3.

Una mejora real, aunque no suficiente para bajar la guardia: casi uno de cada cuatro CISOs sigue en zona de riesgo para su salud.

Como es habitual en estudios basados en autopercepción, es razonable considerar la existencia de posibles sesgos de respuesta: las personas expuestas a niveles más altos de estrés pueden estar más predispuestas a participar, mientras que determinados colectivos del sector —especialmente en entornos con fuerte presencia masculina— tienden a infradeclarar su carga mental. Aunque estos sesgos no pueden cuantificarse con los datos disponibles, conviene tenerlos presentes en la interpretación de los resultados.

MUESTRA DE 2026

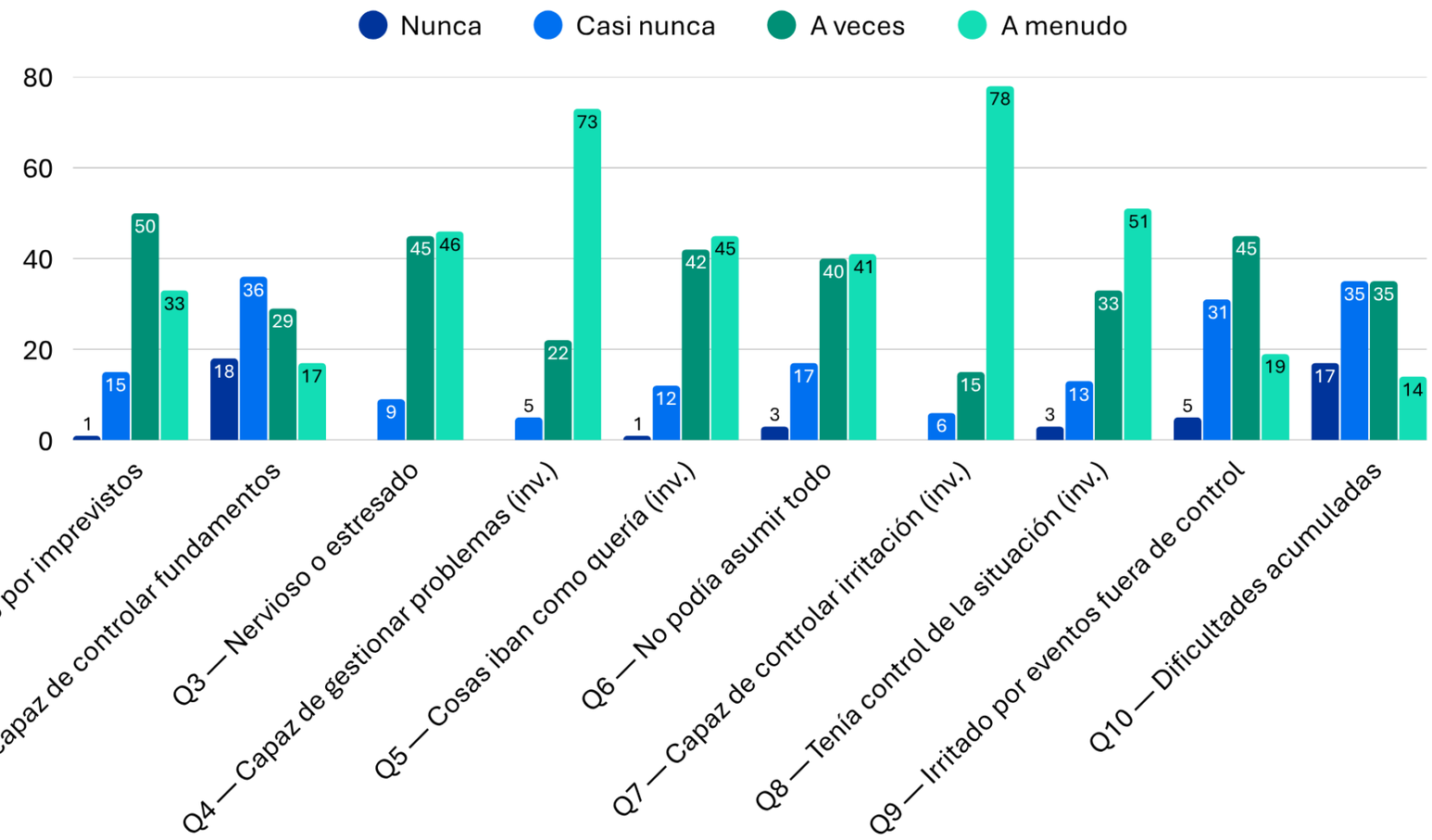
La muestra de 2026 presenta un perfil representativo del colectivo analizado, con un **claro predominio de profesionales que desempeñan funciones de CISO y una alta presencia de organizaciones de gran tamaño**. Además, los datos de 2026 muestran que la mayor parte de los participantes acumula una experiencia prolongada en su función, con un **54,8 %** que lleva cinco años o más en el puesto. No obstante, existe también un grupo relevante que aporta diversidad en términos de trayectoria profesional: un **23,8 %** cuenta con entre uno y tres años de antigüedad y un **2,4 %** lleva menos de un año en el cargo.

El análisis por antigüedad revela un patrón interesante: Dejando de lado el grupo de menos de un año (solo 2 personas, muestra insuficiente para extraer conclusiones), el grupo con mayor estrés es el de **quienes llevan entre 3 y 5 años...**

El análisis pregunta a pregunta revela los puntos de mayor tensión.

- **La pregunta 3** (sentirse nervioso o estresado) sigue generando la respuesta más alta de las preguntas directas (no invertidas), con un 46% de encuestados que responden "bastante a menudo" o "a menudo".
- **Las preguntas 6** (no poder asumir todas las tareas) **y 1** (molestia ante imprevistos) también concentran respuestas en la parte alta de la escala.

*La categoría 'A menudo' agrupa las respuestas 'Bastante a menudo' y 'A menudo' del cuestionario original.



Las preguntas invertidas (Q4, Q5, Q7, Q8) muestran resultados llamativamente positivos: los CISOs españoles se sienten competentes, capaces de controlar su irritación y de manejar sus problemas profesionales. Esta fortaleza individual contrasta con las señales de presión sistémica que reflejan las preguntas directas.

BINGO
de la cibernética

“Siento un desajuste total entre mi capacidad de actuación y las expectativas de mi organización en materia de gestión de riesgos cibernéticos“.	“Tengo que presentar un cuadro de mando con indicadores en rojo”.	“Pierdo los nervios durante una presentación en el comité ejecutivo de mi balance y mi plan de acción“.	“Me angustio durante una auditoría o al responder a un cuestionario del cliente porque siento que aún estoy muy lejos de alcanzar el objetivo“.
“Mi superior me pregunta sobre un incidente imprevisto: no sé qué responder o me angustio”.	★BINGO★		“He soñado con ciberataques y/o cibercrisis“.
“Me siento desorientado, sin una visión real ni capacidad para determinar las direcciones que debe tomar mi estrategia cibernética“.	“Doy una opinión favorable sobre una postura de seguridad con la que no estoy de acuerdo por desánimo o por el miedo a negociar con las partes interesadas“.	“He autorizado una excepción o el incumplimiento de una norma de la PSSI por miedo al conflicto o por temor a que un compañero me cuestione”.	“He tenido que apartar a alguien —o a mí mismo— del dispositivo de gestión de crisis por encontrarse en situación de pánico o bloqueo”.

38,7% le resulta complicado adaptar de forma continua sus análisis y estrategias

86,7% gestionar el riesgo cibernético es una tarea difícil.

Si examinamos las nuevas preguntas relativas a las fuentes de estrés en la edición de 2026, observamos que una parte significativa de los responsables de ciberseguridad continúa experimentando dificultades estructurales en su función. En concreto, el **38,7%** declara que le resulta complicado adaptar de forma continua sus análisis y estrategias ante un entorno de amenazas cambiante. Asimismo, la complejidad intelectual de la gestión del riesgo se confirma como un factor de presión ampliamente compartido: el **86,7%** afirma que gestionar el riesgo cibernético es una tarea difícil. Estas cifras refuerzan la sensación, presente en buena parte del colectivo, de que la misión cibernética exige un esfuerzo constante y que el objetivo de “estar al día” siempre se percibe como algo complicado de conseguir.

A pesar de ello, los responsables se muestran relativamente confiados en su capacidad de comunicación ante la dirección. El **85,3%** considera que durante una presentación o comité es capaz de expresarse con claridad, mostrar empatía y convencer a sus interlocutores. No obstante, esta autopercepción convive con una realidad operativa más matizada: el **57,9%** ha percibido una discrepancia entre las expectativas de su organización y su propia capacidad de actuación. Esa brecha se materializa, en ocasiones, en decisiones comprometidas: el **42,1%** reconoce haber dado su aprobación a una postura de seguridad con la que no estaba plenamente de acuerdo, ya fuera de forma ocasional o en varias ocasiones, con el fin de evitar una negociación difícil o desgastante.

85,3% durante una presentación o comité es capaz de expresarse con claridad, mostrar empatía y convencer a sus interlocutores

57,9% ha percibido una discrepancia entre las expectativas de su organización y su propia capacidad de actuación

42,1% econoce haber dado su aprobación a una postura de seguridad con la que no estaba plenamente de acuerdo

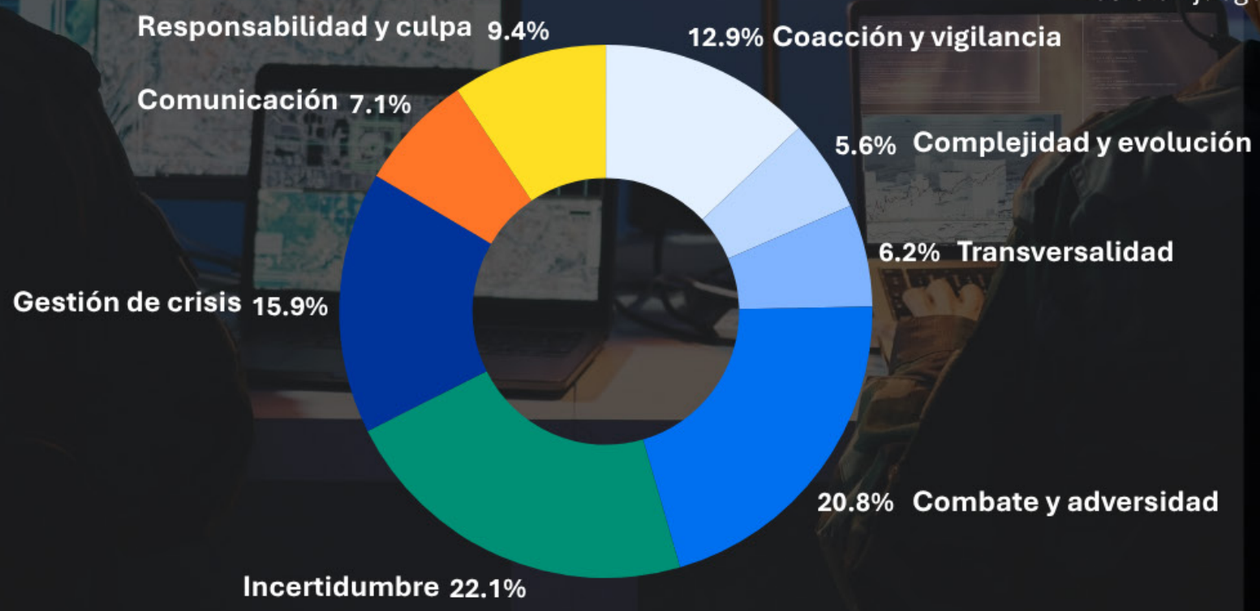
En cuanto a su papel en la gestión de incidentes, los datos muestran una realidad menos visible pero reveladora. Aunque los responsables de ciberseguridad lideran habitualmente la coordinación de las crisis, el **16 %** ha tenido que apartar a una persona —o a sí mismo— del dispositivo de gestión de crisis por encontrarse en situación de pánico.

Por otra parte, la influencia de las amenazas va más allá del horario laboral: el 54 % declara haber soñado con ciberataques o situaciones de crisis en alguna ocasión. Este último resultado ilustra de manera especialmente clara la permeabilidad entre la vida profesional y personal en estos roles, y confirma que la responsabilidad asociada a la función no se desconecta fácilmente.

1.2 FACTORES DE ESTRÉS

Para intentar explicar el nivel de estrés percibido evaluado mediante el PSS, nuestro estudio también se ha centrado, al igual que en 2024, en los factores que contribuyen a este estrés y que serían específicos del ámbito de la ciberseguridad.

Las 22 preguntas relativas a estos factores pueden clasificarse en 8 familias. El peso de estas familias se calcula en relación con el peso de los factores de estrés en la evaluación de la percepción de los encuestados: cuanto más se considera que un factor aumenta el estrés, más peso tiene en la siguiente distribución. Estos dominios reflejan la singularidad de una función que combina la complejidad técnica con la adversidad permanente, la responsabilidad sin poder pleno y la necesidad de justificarse ante todos sin que todos comprendan realmente lo que está en juego.



Se observa una distribución relativamente equilibrada entre las distintas familias de factores de estrés identificadas, aunque dos ejes concentran casi la mitad del peso total. En primer lugar, la incertidumbre y lo desconocido **(22,1%)** se consolida como la principal fuente de presión: la dificultad intelectual de gestionar el ciberriesgo, la imposibilidad de desconectar y la percepción de inestabilidad profesional configuran un escenario de alerta permanente.

En segundo lugar, **el combate y la adversidad (20,8%)** refleja la singularidad de una profesión que se enfrenta a adversarios invisibles en condiciones de asimetría creciente, donde la capacidad de defensa se percibe como estructuralmente inferior a la de ataque. La **gestión de crisis (15,9%)** completa el podio, evidenciando que la presión asociada a la toma de decisiones bajo incertidumbre y la adrenalina de los ciberincidentes sigue siendo un componente central del rol.

Más allá de estos tres ejes dominantes, otros factores contribuyen de forma significativa al estrés acumulado. La **coerción y vigilancia (12,9%)** recoge el desgaste asociado a una imagen profesional aún marcada por percepciones negativas y a la sensación de ser considerado "excesivo".

La **responsabilidad y la culpa (9,4%)**, aunque no encabeza el ranking, engloba vivencias que pueden adquirir una dimensión profundamente personal:

la percepción de tener que justificar de forma continua las propias decisiones y la carga asociada a no haber podido evitar un incidente pueden repercutir de manera directa sobre el bienestar, derivando incluso en situaciones de malestar profesional sostenido.

Asimismo, la **complejidad y evolución constante del entorno (5,6%)** confirma que la necesidad de adaptarse permanentemente constituye un factor de desgaste progresivo, aunque los CISOs españoles parecen cada vez mejor equipados para afrontarlo.

Encuentre los resultados

22,1%

La incertidumbre y lo desconocido se consolida como la principal fuente de presión

ESTAS SON LAS PRINCIPALES CONCLUSIONES DEL ANÁLISIS DE LOS FACTORES DE ESTRÉS

LOS GRANDES SÍ
LO QUE MÁS CONTRIBUYE AL ESTRÉS

Las respuestas afirmativas más rotundas revelan los factores que generan mayor presión entre los CISOs españoles en 2026. El podio lo encabeza la singularidad de la profesión, seguida de la dificultad intelectual inherente a la gestión del riesgo y del sentimiento de impotencia ante un combate asimétrico.

Factor estresante	2024	2026
Profesión singular: adversarios invisibles y maliciosos (P19)	74,4%	90,7%
Gestión del ciberriesgo es intelectualmente difícil (P28)	89 %	86,7 %
Impotente ante el combate asimétrico (P22)	56,1 %	60 %
Tiene que justificar la utilidad de sus acciones (P33)	74,4 %	65,3 %
Situación profesional incierta (P27)	62,2 %	58,7 %
Incomprendido o considerado 'excesivo' (P14)	75,6 %	57,3 %
Constantemente en alerta, sin poder desconectar (P26)	61 %	54,7 %

Uno de los cambios más notables entre 2024 y 2026 es el incremento en la percepción de singularidad de la profesión: el porcentaje de quienes consideran que tratar con **adversarios invisibles** es algo inusual en el mundo empresarial **sube del 74,4 % al 90,7 %.**

Este dato no indica necesariamente más estrés, sino una mayor toma de conciencia colectiva de la especificidad del rol.

La presión del reconocimiento sigue siendo una de las señales más persistentes:

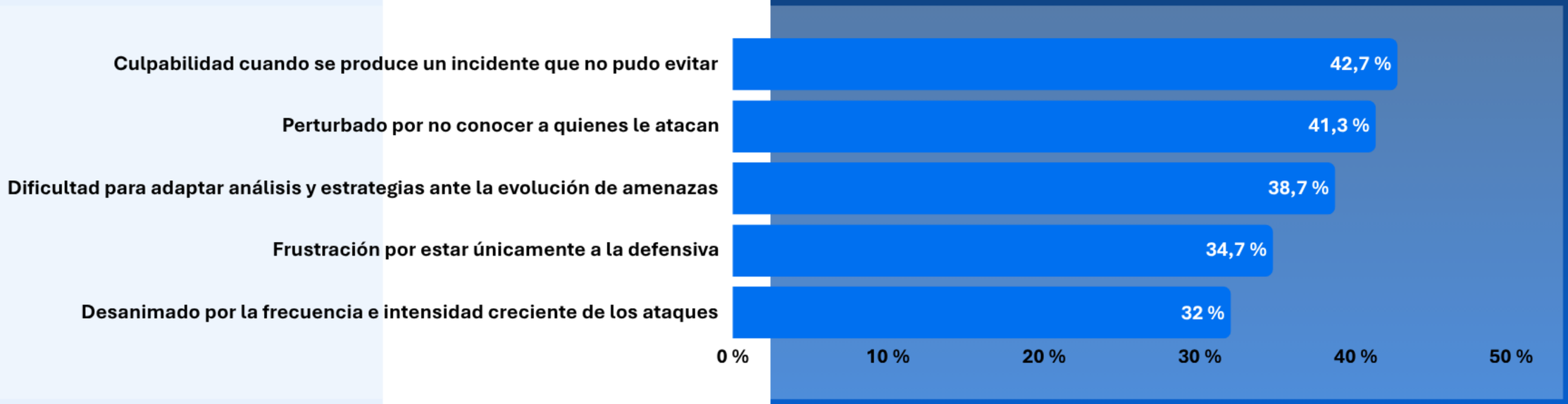
en 2026, el **65,3 % de los encuestados siente que tiene que justificar la utilidad de sus acciones,** y el 57,3 % se percibe como incomprendido o considerado excesivo.

Son cifras menores a las de 2024 (74% y 76% respectivamente), lo que indica una **evolución positiva**, pero siguen siendo preocupantes en un colectivo que lidera la defensa digital de sus organizaciones.

El 60% de los CISOs se siente impotente ante la naturaleza asimétrica del combate cibernético. En 2024 era el 56,1 %. La sensación de combatir en inferioridad de condiciones sigue creciendo, a pesar de la mejora general en el nivel de estrés.

LOS INDECISOS: TENSIONES PERSISTENTES

Más allá de los factores dominantes, el análisis revela un conjunto de tensiones que permanecen activas para una parte significativa de la comunidad de CISOs, situándose en una franja intermedia (entre el 30% y el 45%) que no es mayoritaria pero tampoco marginal

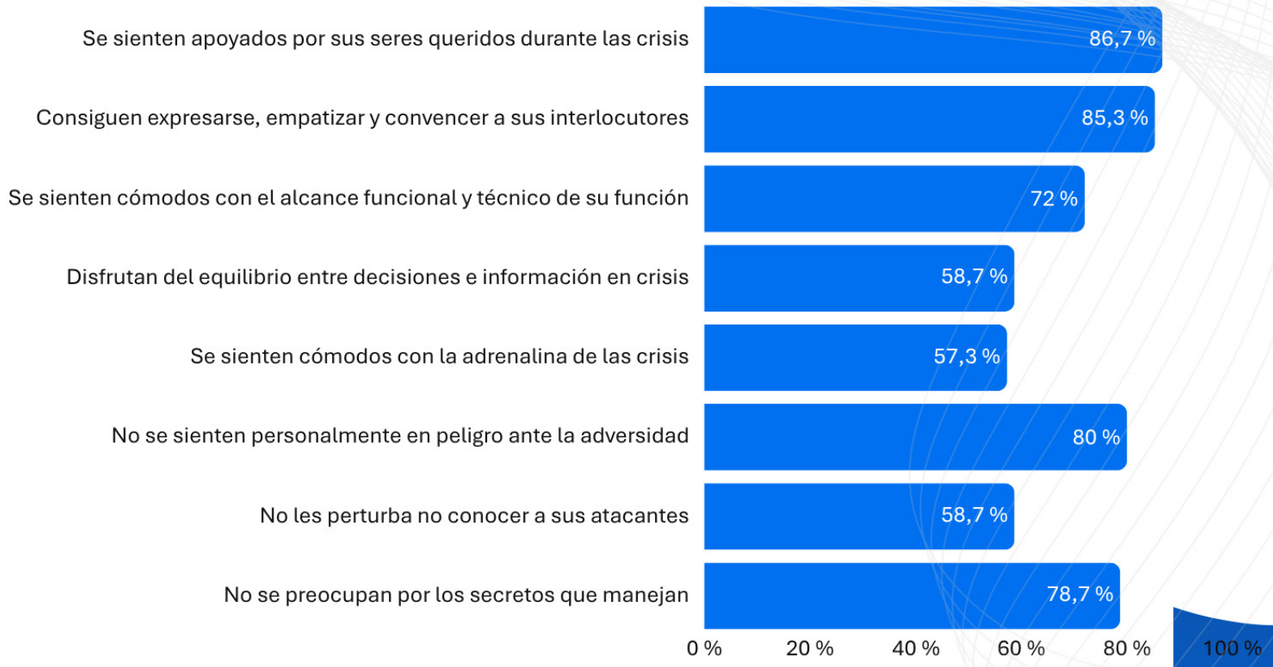


Estos factores comparten un rasgo común: reflejan la tensión entre la voluntad de actuar y las limitaciones inherentes al rol. La culpabilidad tras un incidente (42,7 %) y la perturbación por no conocer al adversario (41,3 %) evidencian una carga emocional que, aunque no afecta a la mayoría, sí incide sobre una parte sustancial del colectivo y puede agravarse en contextos de alta presión operativa.

LOS FACTORES DE RESILIENCIA

LO QUE LOS CISOS CONTROLAN BIEN

El análisis no busca solo identificar lo que genera estrés, sino también comprender las **fuentes de resiliencia y equilibrio de la profesión**.
Varios factores destacan de forma consistente como puntos de fortaleza



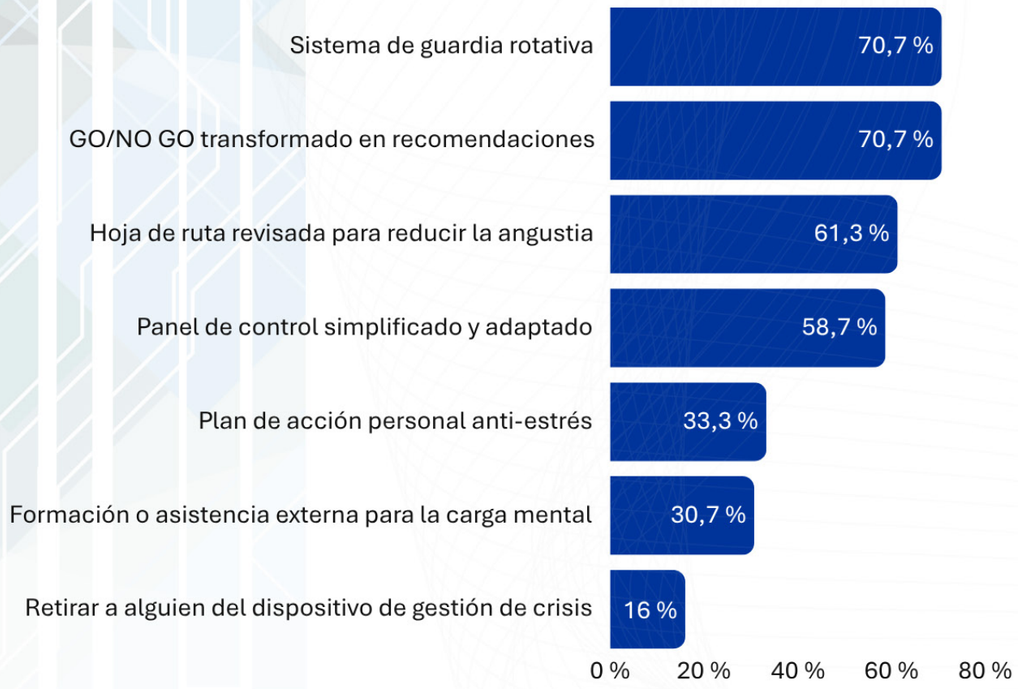
El apoyo de las personas cercanas sube de forma notable entre 2024 y 2026 (del 69,5 % al 86,7 %), lo que sugiere una **mayor apertura de los CISOs a hablar de su trabajo con su entorno personal**, o bien una mayor comprensión por parte de ese entorno de las exigencias del rol.

En 2026, el 57,3 % de los CISOs afirma sentirse cómodo con la adrenalina, la presión y la sensación de urgencia propias de una crisis de ciberseguridad.

Aunque la formulación de esta pregunta difiere ligeramente respecto a la de 2024 —donde el 74% declaraba haber experimentado altos niveles de adrenalina y urgencia—, el dato sugiere que más de cuatro de cada diez profesionales no gestionan bien esa presión operativa, lo que convierte la tolerancia a la crisis en un eje de trabajo relevante para la profesión.

NUEVAS HERRAMIENTAS Y PRÁCTICAS ANTI-ESTRÉS

Una de las principales novedades de la edición 2026 es la incorporación de **preguntas sobre las acciones concretas que los CISOs han puesto en marcha para gestionar su estrés y el de sus equipos**. Los resultados muestran una comunidad claramente más activa en este terreno que en 2024.



La implementación de guardias rotativas y la conversión del **GO/NO GO** en recomendaciones de riesgo son las prácticas más extendidas, con un **70,7 %** de adopción cada una, lo que refleja una comunidad que ha interiorizado la **necesidad de organizarse para gestionar la presión**.

Este aumento generalizado en la adopción de **prácticas anti-estrés** es probablemente uno de los factores que explican la **mejora en el score PSS** medio entre 2024 y 2026.

No se trata solo de que la situación haya mejorado externamente, sino de que **los profesionales** han desarrollado **mayor capacidad de gestión interna**.

Al igual que en 2024, una parte significativa de los responsables de ciberseguridad continúa sufriendo una imagen o prejuicios negativos sobre su función.

En 2024, el **74%** de los encuestados **afirmaba que su trabajo adolecía de ideas preconcebidas negativas** capaces de complicar su tarea e incluso generar aislamiento.

En 2026, este indicador registra la caída más pronunciada de todo el estudio: **solo el 30,7% sigue percibiéndolo así**, lo que sugiere un avance muy significativo en el reconocimiento de la profesión dentro de las organizaciones.

No obstante, un indicador complementario matiza este optimismo:

el **57,3% de los CISOs sigue sintiéndose incomprendido o juzgado como "excesivo"** al hacer recomendaciones, **una mejora respecto al 75,6% de 2024** pero que confirma que el déficit de comprensión del rol persiste en más de la mitad del colectivo.

Además, en 2024 el **74,4 %** manifestaba la sensación de tener que **justificar constantemente la utilidad de sus acciones**. Esta cifra desciende **en 2026 al 65,3 %**, una **mejora notable** aunque el dato sigue siendo significativo: casi **dos de cada tres CISOs sienten que deben justificar lo que hacen**.

Casi dos de cada tres

CISOs sienten que deben justificar lo que hacen.

En lo que respecta a las competencias, el **75,6 % de los CISOs afirmaba en 2024** contar con las **habilidades técnicas y metodológicas adecuadas**.

En **2026**, el porcentaje de quienes no sienten que les falte experiencia técnica asciende al **82,7 %, manteniendo la percepción de solidez profesional**.

Sin embargo, ambos años muestran el reto de la evolución continua: **en 2024, un 54,9 %** declaraba tener **dificultades para ajustarse a la velocidad** del cambio, mientras que e**n 2026 el 61,3 %** afirma **no encontrar difícil adaptarse**, lo que indica una mejora real en la sensación de control frente a un entorno cambiante.

El 82,7 %,

afirma contar con las habilidades técnicas y metodológicas adecuadas

La singularidad adversarial de la profesión se mantiene estable e incluso se intensifica.

En 2024, el 74,4 % afirmaba enfrentarse a adversarios "invisibles" y malintencionados; en **2026** esta percepción **sube al 90,7 %**.

La «frustración del defensor», por el contrario, mejora: en 2024 el 47,6 % se sentía frustrado por no poder contraatacar, mientras que **en 2026 desciende al 34,7 %**.

La «frustración del defensor» mejora

descendiendo en 2026 al 34,7% frente al 47,6% de 2024.

En cuanto a la aceptación de los imprevistos, **en 2024** el **41,5%** de los CISOs afirmaba **apreciar lo inesperado y lo imprevisible,** un rasgo que puede interpretarse como indicador de resiliencia ante la incertidumbre. **En 2026**, este porcentaje desciende al **32%,** lo que puede reflejar un **mayor agotamiento acumulado** o una menor capacidad para encontrar estimulante lo que antes se percibía como fuente de energía.

7 de cada 10

Dicho de otro modo, **casi siete de cada diez CISOs** ya **no** encuentran **atractiva** la dimensión imprevisible de su trabajo.

Uno de los indicadores más sensibles es el de la alerta constante.

En **2024** el **61 %** afirmaba estar **permanentemente alerta** e incapaz de desconectar.

En **2026** esta cifra **mejora**, bajando al **54,7 %**, lo que sugiere que la profesionalización y ampliación de los equipos está empezando a aliviar esta carga.

En contraposición, cuando estalla una crisis, los responsables de ciberseguridad demuestran una notable fortaleza. En **2024**, el **69,5 %** se sentía **apoyado** por su entorno más cercano. En **2026** este apoyo se eleva al **86,7 %** y **el 57,3 %** asegura **sentirse cómodo con la adrenalina, la urgencia y la presión** asociadas a una crisis.

Finalmente, el sentimiento de culpa muestra una evolución favorable: en 2024, el 58,5 % reconocía sentir culpa cuando un incidente no podía evitarse, detectarse o limitarse.

En 2026 42,7 %

sugiere una **mayor madurez** organizativa en la **distribución de la responsabilidad** ante los incidentes.

En **2026** este porcentaje desciende al **42,7 %**, una mejora de 15 puntos que sugiere una **mayor madurez organizativa** en la distribución de la responsabilidad ante los incidentes.

> «La ciberseguridad es gobierno y supervisión. Los CISOs supervisamos pero los compañeros TICs y de negocio se sienten controlados.
>
> La Alta Dirección siempre dice que la ciberseguridad es lo más importante cuando ocurre un incidente crítico; en el día a día no les importa y sus expectativas son muy altas, con el poco apoyo y dinero que dedican.»
>
> Encuestado anónimo del Informe del estrés de los CISOs 2026

PERSPECTIVAS SOBRE LOS RESULTADOS

«¿Qué opiniones tienen sobre los resultados?»

Benjamin Leroux, Chief Marketing Officer, Advens

Los datos de esta edición 2026 admiten dos lecturas, y quiero asumir las dos.
La primera es alentadora: el número de CISO en situación de estrés controlado ha aumentado casi ocho puntos en tres años. Pero el número de profesionales en zona de vigilancia también ha subido ocho puntos. Y en total, más del 60% declaran un nivel de estrés preocupante. Hemos gestionado mejor los casos más extremos, pero no hemos resuelto el problema de fondo. Conozco a muchos CISO. Son, en su mayoría, apasionados, personas que aceptan e incluso buscan la adversidad permanente de este oficio. Esa pasión es una fortaleza. Pero no puede con todo. Este año hemos incorporado preguntas para explorar algo más difícil de decir: ¿acaba el estrés afectando a las decisiones? ¿Lleva la presión a bajar los brazos, a autorizar una excepción que no debería autorizarse? Las respuestas no son tranquilizadoras.

¿Qué queda por hacer? *El management tiene un papel concreto: escucha real, respaldo visible, recursos alineados con las ambiciones de seguridad que se proclaman. Los propios CISO tienen que poder reivindicar la formación en gestión y liderazgo como parte legítima de su desarrollo. Y hace falta formalizar las prácticas de pilotaje: un CISO que ha construido un sistema que funciona sin que él tenga que estar en todas partes es más resiliente y más eficaz. Por último, las comunidades como ISMS Forum tienen un papel que va más allá del intercambio técnico: hablar de las dificultades del oficio, de sus contradicciones, de sus momentos de duda, no es una señal de debilidad. Es una condición para progresar. La ciberseguridad no es solo una cuestión de tecnología. Es también, y profundamente, una cuestión humana.*

Jesús Abascal, CISO Plenitude

«Para vivir en la incertidumbre, hay que aceptar que la brecha siempre puede existir, y ese primer paso ya ayuda a reducir el estrés. En mi caso, el equilibrio está apoyado sobre dos pilares clave. Por una parte, tener planes de respuesta realmente probados mediante TTX exigentes y fuera de mi zona de confort, me da mucha tranquilidad y paz mental. Por otra parte, es imprescindible aprender a desconectar de verdad, algo que sé que me cuesta, pero el deporte es un buen aliado. Yo lo consigo en la montaña, especialmente haciendo espeleología, donde no hay cobertura ni interrupciones; solo foco, silencio y la posibilidad de resetear mi mente para volver con claridad.

Jesús Abascal es Responsable de Seguridad de la Información en Eni Plenitude Iberia, especializado en ciberseguridad, riesgos y cumplimiento en entornos IT/OT. Cuenta con amplia experiencia en sectores como energía y legal, donde ha liderado iniciativas para mejorar la resiliencia y la madurez en seguridad. Además, es divulgador activo, profesor, mentor y actualmente realiza un doctorado en ciberseguridad e inteligencia artificial

Susana Calvo, CISO Puig.

La expresión mantener el equilibrio entre "seguridad" y "operación" a veces puede hacernos un flaco favor. En momentos de estrés o de picos de trabajo, nos podemos ver tentados a "excepcionar" más de la cuenta. Sin embargo, ser consistentes y firmes en nuestras decisiones, genera más confianza en el negocio y en nuestros stakeholders. La consistencia y el equilibrio son fundamentales y hemos de creer firmemente en estos valores. Las excepciones, seguirán existiendo, pero han de ser eso, "excepciones", sólo algunos casos contados, que deberemos gestionar como riesgos y dar visibilidad de los mismos a la organización.

Ingeniera Superior de Telecomunicaciones lleva más de 20 años trabajando en el ámbito de ciberseguridad, 9 años EY en consultoría, 6 años en Volkswagen en sector de automoción, 4 años en Grifols industria farmacéutica y actualmente en el sector del lujo y las fragancias desde enero de 2026 en Puig. Siempre vinculada al ámbito de la ciberseguridad, ha liderado múltiples proyectos de gestión de riegos, creación de las prácticas de ciberseguridad en varias empresas, montando equipos de alto rendimiento motivados y comprometidos con la ciberseguridad, asegurando el alineamiento con el negocio. Firme creyente en implementar una práctica consistente y coherente de ciberseguridad que esté alineada con la cultura de la empresa como clave de éxito de una buena función de ciberseguridad. Participa en foros y conferencias para poder seguir creciendo como profesional de la práctica de cyber y estar al día de las nuevas tecnologías y poder incorporarlas adecuadamente.

DIFICULTADES AÚN MUY PRESENTES

Centrémonos en tres grandes dificultades a través del prisma de los testimonios recopilados

2.1 La soledad del CISO y el valor de la comunidad

Los datos de 2026 confirman que el 65,3 % de los CISOs siente que debe justificar constantemente la utilidad de sus acciones, y el 57,3 % se percibe como incomprendido o considerado excesivo. Estas cifras dibujan una función que, a pesar de su creciente importancia estratégica, sigue operando con un déficit de reconocimiento interno. Sin embargo, el estudio también revela un factor de protección relevante:

los espacios de intercambio entre pares actúan como un amortiguador real del estrés. Para muchos CISOs, compartir experiencias con quienes viven las mismas presiones es la principal vía de desahogo y aprendizaje, tanto profesional como personal.

Testimonio de un CISO del sector Finanzas/Banca con >5 años en su puesto

«Aunque el trabajo es muy interesante y variado y te permite un aprendizaje continuo, el nivel de estrés es muy elevado por la gran carga de trabajo constante y por el poco apoyo que se recibe de los puestos de dirección (prácticamente mi único apoyo en el ejecutivo es el Director de Tecnología).

Los eventos en los que compartes experiencias con otros CISOs me son de mucha utilidad tanto profesionalmente, como personalmente para compartir experiencias más personales.»

Encuestado anónimo del Informe del estrés de los CISOs 2026

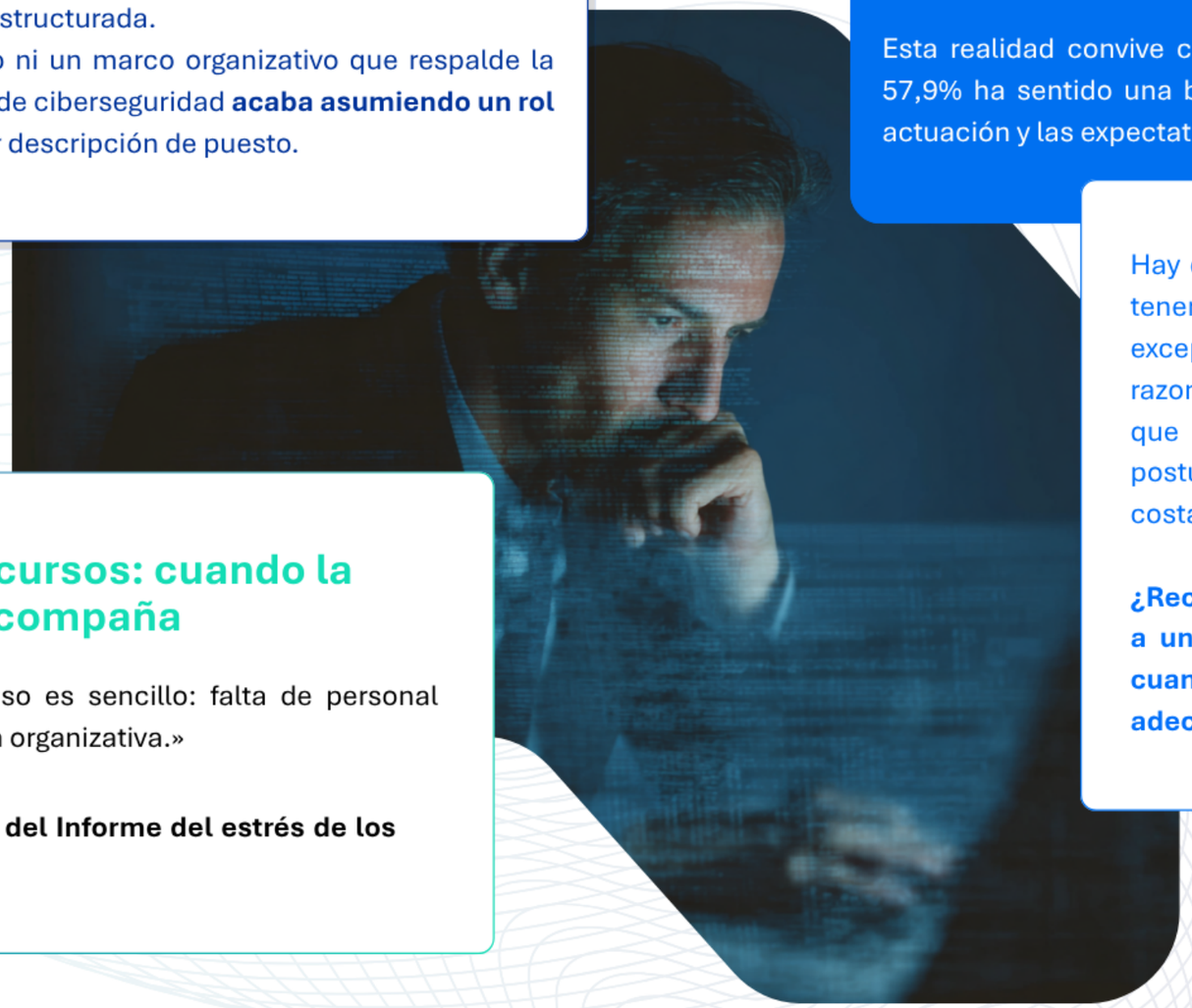
2.2 La brecha de recursos: cuando la estructura no acompaña

El **53,6 %** de los CISOs encuestados en 2026 gestiona su función con un equipo de entre **1 y 5 personas**.

En sectores críticos como la salud, donde la superficie de exposición no deja de crecer y la regulación se endurece, esta realidad se traduce en una presión difícilmente sostenible.

El estudio muestra que la falta de recursos no solo alimenta el estrés: **condiciona la capacidad del CISO** para construir una defensa mínimamente estructurada.

Sin personal cualificado ni un marco organizativo que respalde la función, el responsable de ciberseguridad **acaba asumiendo un rol que desborda** cualquier descripción de puesto.



La brecha de recursos: cuando la estructura no acompaña

«El resumen en mi caso es sencillo: falta de personal cualificado y estructura organizativa.»

Encuestado anónimo del Informe del estrés de los CISOs 2026

2.3 La tentación de reducir el nivel de exigencia

El estudio revela que los responsables de ciberseguridad a veces conceden excepciones o incumplimientos de sus propias políticas de seguridad por miedo al conflicto o a la confrontación (42,1%).

Esta realidad convive con una percepción más amplia de desajuste: el 57,9% ha sentido una brecha demasiado grande entre su capacidad de actuación y las expectativas de su organización.

Hay que relativizar estos resultados. No es una anomalía tener que conceder excepciones a una política. Estas excepciones pueden estar justificadas. Pero si se hace por razones de evasión psicológica, es más preocupante, ya que la evaluación de los riesgos y beneficios de cada postura forma parte del trabajo, por lo que no debería costar mucho convencer.

¿Recetaría un médico, cansado de insistir, antibióticos a un paciente que se mantiene firme en su postura, cuando está convencido de que los antibióticos no son adecuados para el caso en cuestión?

→ Perspectivas profesionales/«lo que queda por hacer»

¿Qué dice Advens?

La evolución de los resultados entre 2024 y 2026 confirma lo que intuíamos: el estrés de los CISOs no es una variable fija ni un destino inevitable. Depende del contexto, de las herramientas disponibles, del reconocimiento institucional y del apoyo del entorno.

El hecho de que el score medio haya bajado casi dos puntos entre ediciones es un resultado que nos llena de esperanza, pero también de responsabilidad.

En Advens seguimos convencidos de que mejorar el bienestar de los responsables de ciberseguridad no es solo un imperativo ético: es también una palanca para mejorar la eficacia colectiva de los sistemas de defensa.

Un CISO que gestiona bien su estrés toma mejores decisiones, comunica mejor y construye equipos más resilientes.

La incorporación en 2026 de nuevas preguntas sobre situaciones vividas y acciones implementadas enriquece considerablemente el análisis.

Por primera vez, podemos hablar no solo de niveles de estrés sino de comportamientos: qué hacen los CISOs para protegerse, qué funciona y qué sigue pendiente. Ese es el paso que faltaba para pasar del diagnóstico a la acción.

Testimonio de José Luis, CEO España & Portugal

Cuando lanzamos este estudio por primera vez en 2024, lo hicimos con una intuición y una pregunta. La intuición era que algo no iba bien en la forma en que esta profesión se vive por dentro.

La pregunta era si los datos nos darían la razón. Nos la dieron, y con creces. Dos años después, volvemos a preguntar. Y lo que encuentro más valioso de esta segunda edición no es tanto la mejora en los indicadores —que la hay, y es real— sino lo que hemos conseguido hacer visible por el camino. Hoy se habla de la salud mental del CISO. Se habla en foros, en consejos de dirección, entre colegas. Eso, hace tres años, no pasaba.

Pero no nos engañemos. Que el termómetro marque un poco menos no significa que la fiebre haya desaparecido.

Seguimos ante una profesión donde la presión no descansa, donde el reconocimiento llega tarde y donde las expectativas crecen más rápido que los medios. NIS2, DORA, la regulación de la inteligencia artificial... cada nuevo marco amplía el tablero de juego del CISO sin que nadie le pregunte si tiene fichas suficientes para jugarlo. Desde Advens, nuestro compromiso es claro: seguiremos midiendo, seguiremos preguntando y seguiremos poniendo este tema donde tiene que estar.

Porque cuidar a quienes protegen no es un lujo. Es una condición para que todo lo demás funcione.

Moisés López, Head of GRC en Advens Iberia

Una edición más del informe que pone sobre la mesa el estrés al que están sometidos los ISOs/responsables de seguridad en España. En esta ocasión, y aunque el informe da para uchas reflexiones, me gustaría poner el foco en tres aspectos:

a evolución del “stopper” (visión Go/No Go) que se mueve cada vez más, creo que certadamente, a una visión de búsqueda de recomendaciones, probablemente más cercano a egocio, estrategia y gestión del riesgo. Eso sí, siempre que no venga condicionado por el egundo punto que llama mi atención, el 42,1% ha dado su autorización a una postura de eguridad que era contraria a sus convicciones por desánimo o angustia ante las negociaciones ecesarias para defenderlas, un dato no muy alentador sobre el apoyo interno que están ecibiendo los CISOs.

omo tercer y último punto, no me gustaría dejar pasar el nada despreciable 57,9% que ha entido una brecha entre su capacidad de acción y las expectativas de la organización, un dato ue me parece tremendamente elevado y una desalineación entre la labor del CISO y como es ercibida internamente.

n definitiva, ser CISO sigue siendo deporte de riesgo, aunque van mejorando las condiciones ara practicarlo.”

¿Y el ISMS Forum?

ISMS Forum nació con el objetivo de ser un espacio de conocimiento compartido para los profesionales de la seguridad de la información en España. Este estudio, del que somos co-promotores desde 2024, encarna perfectamente ese espíritu: combina rigor metodológico, escucha real de la comunidad y voluntad de incidir en las condiciones de ejercicio de la profesión.

Los datos de 2026 confirman que el tema del estrés ha ganado legitimidad en el discurso profesional. Hoy los CISOs hablan más abiertamente de su carga mental, de sus límites y de sus estrategias de adaptación. Ese es, en sí mismo, un progreso. ISMS Forum seguirá siendo un espacio donde esas conversaciones puedan tener lugar, con respaldo empírico y sin tabúes.

Testimonio de Roberto, presidente del ISMS

El estrés del CISO no es un factor externo, sino un elemento consubstancial a su rol dentro de un ciclo natural de "crear-destruir-crear" donde la preparación para la defensa es el principio fundamental.

Esta presión se ve exacerbada por una velocidad de cambio que alcanza el paroxismo, enfrentando novedades y desafíos cada hora, en un entorno de "frenesí técnico" marcado por la carencia de fuerza de trabajo y niveles de desempeño extremos. A esta carga operativa se suma un marco regulatorio extenuante y de origen más político que técnico, como la normativa NIS2, que obliga al profesional a dedicar esfuerzos masivos al cumplimiento mientras intenta gestionar riesgos geopolíticos crecientes.

Finalmente, el agotamiento se intensifica debido a la dificultad de traducir su lenguaje técnico a niveles ejecutivos y a la asunción solitaria de responsabilidades que deberían ser transversales desde aspectos legales hasta recursos humanos, lo que convierte la función en un "uno para todos" agotador en lugar de un compromiso organizacional conjunto. Ante esta realidad, el CISO debe transitar hacia la "prosiliencia", aceptando que "las cosas van a ir mal" y enfocándose en anticipar el golpe en lugar de intentar evitar lo inevitable.

Testimonio de Beatriz García, subdirectora y responsable de la Unidad de Proyectos de ISMS Forum

Tras cuatro años de trabajo continuado con la comunidad CISO y desde mi formación en psicología, he constatado que el estrés asociado a este rol no responde únicamente a factores operativos.

La combinación de altas demandas, capacidad de influencia limitada y apoyo insuficiente, ampliamente descrita por la psicología del trabajo, se manifiesta de forma consistente en el ejercicio diario de la función CISO.

El CISO ocupa una posición de frontera dentro de la organización, donde la responsabilidad estratégica convive con la ambigüedad y, en muchos casos, con el aislamiento. Esta brecha entre lo que debe hacerse y lo que la organización puede asumir genera una carga emocional y cognitiva significativa.

En este contexto, el papel de ISMS Forum resulta determinante: el apoyo entre iguales y la creación de entornos de confianza actúan como mecanismos de protección frente al estrés sostenido.

Asimismo, nuestras guías, estudios y marcos metodológicos refuerzan el sentido de control en escenarios de alta incertidumbre. Este estudio refleja la evolución de la profesión, pero también sus vulnerabilidades, y subraya que el bienestar del CISO es un elemento estructural para la resiliencia organizativa y del ecosistema ciber en España.

3.2 LA EXPERIENCIA COMO ESCUDO FRENTE AL ESTRÉS

El análisis por antigüedad revela un patrón llamativo: los CISOs que llevan **más de 5 años** en el puesto registran un **score PSS medio de 17,5, inferior** al de quienes se encuentran en la franja de **3 a 5 años (18,4).**

La veteranía no elimina la presión, pero parece dotar al profesional de **herramientas internas para gestionarla**: la capacidad de relativizar, de distinguir lo urgente de lo importante, y de confiar en las soluciones que ya ha probado.

Testimonio

«Con la edad y la experiencia, se va aprendiendo a controlar mejor el estrés, a relativizar los problemas y acertar con las soluciones.»

CISO / Responsable de Ciberseguridad de una empresa del sector industrial con >5 años en su puesto.

Este hallazgo tiene implicaciones directas para las organizaciones: acompañar al CISO especialmente en la franja de 3 a 5 años en el puesto, donde el estrés alcanza su punto más alto según los datos de este estudio, puede **marcar la diferencia entre la retención y el abandono**.

3.3 HERRAMIENTAS

Además de la sensibilización, a veces es necesario recurrir a herramientas o acciones que permitan una respuesta más rápida ante una situación de angustia. En este sentido, aún queda trabajo por hacer, ya que dos de cada tres encuestados (66,7 %) no han previsto un plan de acción específico para gestionar mejor su estrés. Es cierto que un plan de acción de este tipo no siempre es necesario, pero las cifras de este estudio permiten afirmar que existen situaciones que requieren respuestas adecuadas.

Es necesario poder identificarlas y ponerlas en práctica.
A primera vista, parece que la profesión no cuenta con las herramientas adecuadas para hacer frente al estrés. Sin embargo, ha sabido adaptarse y adaptar otras herramientas para responder a este fenómeno.

La primera de ellas es la guardia. Con demasiada frecuencia, el responsable de ciberseguridad, por falta de medios financieros o humanos, debe estar disponible en todo momento para reaccionar en caso de alerta, en particular. Ante esta situación, el 70,7 % de los encuestados ha implantado un sistema de guardia compartida entre varias personas. Se trata de una herramienta muy extendida en numerosas profesiones, cuyos efectos sobre el nivel de estrés experimentado pueden ser muy positivos e inmediatos.

En cuanto a las soluciones, es importante recordar el interés de algunas herramientas clásicas. Los cuadros de mando son también un buen ejemplo. Para algunos, si se utilizan «mal», se convierten en una fuente de angustia, ya que pueden ser sinónimo de incapacidad para llevar adelante un plan de acción, imposibilidad de remediar fallos, etc.

Una revisión de los indicadores o de su método de cálculo podría convertir estos cuadros de mando en auténticas guías para ayudar al responsable de ciberseguridad, a sus superiores y a su equipo a avanzar con tranquilidad.

Otra herramienta que hay que reinventar para ayudar a controlar el estrés: el ejercicio de crisis. El 32,9 % de los responsables de ciberseguridad se sintieron angustiados e indefensos ante su jefe ante un incidente que no habían imaginado.

Evidentemente, es ilusorio pensar que se pueden prever todos los escenarios de incidentes y ponerse a prueba ante cada uno de ellos. No obstante, el ejercicio de crisis puede ayudar a tranquilizarse:

1. Si se demuestra suficiente imaginación en el diseño del escenario del ejercicio de crisis.
2. Si se integra en el propio ejercicio una reflexión o incluso una formación sobre la presión y el estrés que provoca la crisis.

¿El estrés, una cuestión de gestión?

El estrés es un tema recurrente entre los profesionales de la ciberseguridad. Este estudio confirma que una proporción significativa de los CISOs sigue experimentando niveles de estrés con efectos negativos.

Y no son los únicos: otras funciones del ecosistema ciber, como los **equipos CERT o los profesionales de respuesta a incidentes**, se encuentran igualmente en primera línea.

> ***Los ejemplos no faltan en un sector expuesto de forma permanente a situaciones de emergencia, crisis e incertidumbre.***

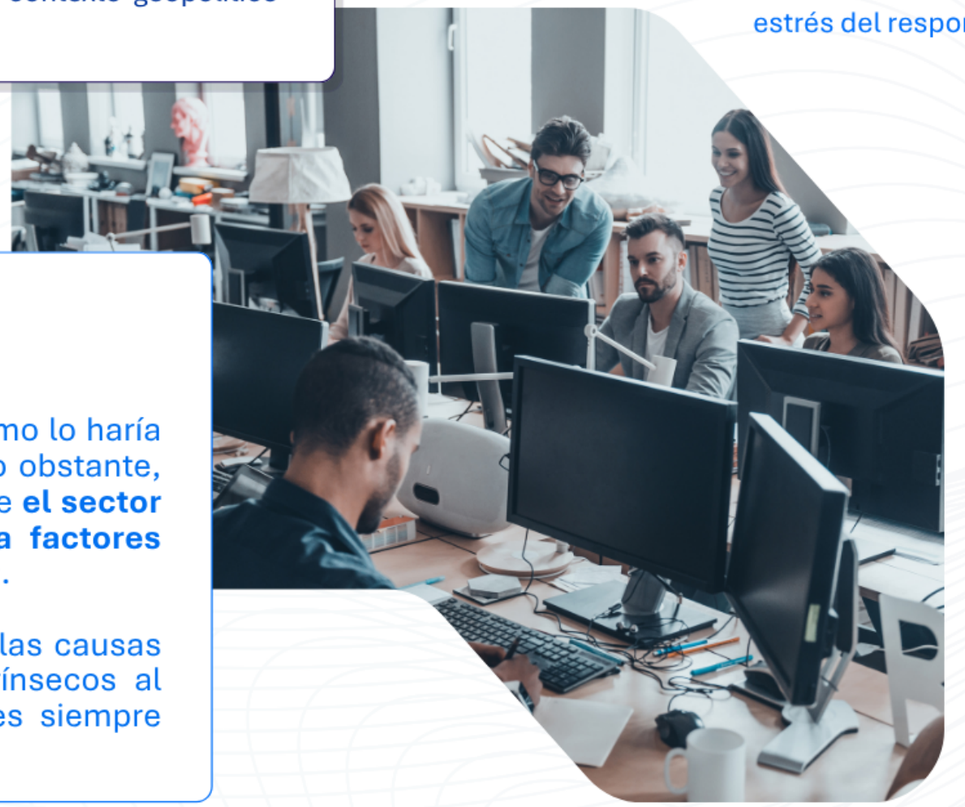
Sin embargo, el estrés es, ante todo, un síntoma. Comprender sus causas es condición necesaria para avanzar en su tratamiento. **El objetivo de este estudio, al igual que el de la edición anterior, no es identificar ni eliminar una causa única.**

Se trata más bien de medir la **intensidad del estrés**, evaluar **cómo se manifiesta en el ejercicio de la profesión** e identificar **posibles vías de mejora.**

La carga invisible del CISO

En el contexto profesional, el estrés puede entenderse como el resultado de un desajuste entre la percepción que el profesional tiene de su propio valor y las expectativas que la dirección y los compañeros proyectan sobre ese valor. Este desajuste se expresa con claridad en la función del CISO: se le percibe como un superhéroe capaz de protegerlo todo, cuando él mismo es consciente de que la tarea desborda con creces la capacidad de una sola persona.

Se espera de él una postura estratégica, pero la realidad le arrastra con frecuencia al terreno operativo, dificultando la distancia necesaria para pensar a largo plazo. Y, como cualquier directivo, debe navegar un continuo de complejidad: organizaciones complejas, en una sociedad compleja, en un contexto geopolítico que no deja de complicarse.



→ ***« Los atacantes siempre serán atacantes »***

Esta discrepancia alimenta el estrés, como lo haría en cualquier otro ámbito profesional. No obstante, este estudio ha puesto de manifiesto que **el sector de la ciberseguridad está expuesto a factores adicionales que amplifican esa presión**.

De ahí la importancia de trabajar sobre las causas del desajuste, porque los factores intrínsecos al puesto no van a cambiar: los atacantes siempre serán atacantes.

Las verdaderas causas del estrés

No están en la tecnología, sino en la gestión, las prioridades y las relaciones.

Las causas del estrés no hay que buscarlas en la técnica. Hay que buscarlas en la gestión y el liderazgo. Elegir las prioridades adecuadas, no dispersarse, gestionar las expectativas de los interlocutores internos y externos, acompañar al equipo ante cargas de trabajo elevadas, involucrar a las demás direcciones en la hoja de ruta de ciberseguridad, convencer a la alta dirección: todos estos son retos cuya superación puede tener un impacto extraordinariamente positivo en el nivel de estrés del responsable de ciberseguridad.

Y para afrontarlos no se necesitan nuevas competencias en métodos de ataque, criptografía postcuántica o seguridad de la inteligencia artificial. Las herramientas necesarias están en otro lugar: en las habilidades interpersonales, de comunicación y de dirección propias de cualquier puesto de responsabilidad. Quizás sea esta la consecuencia más natural de la evolución y maduración de la función ciber dentro de las organizaciones.

4.0 UNA PALABRA PARA CONCLUIR

Trabajar en la segunda edición de este estudio ha sido, una vez más, un ejercicio apasionante. El estrés en la ciberseguridad es un tema que no se agota: cada dato abre una conversación, cada cifra esconde una historia personal. Y eso es precisamente lo que lo hace tan valioso — nos obliga a mirar más allá de la tecnología y a recordar que, al final del día, quien sostiene la defensa digital de una organización es una persona.

Con sus límites, su desgaste y también su capacidad de adaptación. Ojalá este trabajo sirva para que más profesionales, más directivos y más organizaciones se detengan a pensar en lo que implica ejercer esta profesión, no solo en términos técnicos, sino en lo que exige a nivel emocional, relacional y de liderazgo.

Para Advens y para ISMS Forum, explorar la dimensión humana de la ciberseguridad no es un ejercicio colateral: forma parte de lo que somos.

La vulnerabilidad es nuestro territorio.
Protegemos a quienes están expuestos a ella, nos enfrentamos a quienes intentan explotarla y la entendemos como lo que realmente es: no una debilidad, sino una fuente de valor, tanto individual como colectivo.

Si el tema del estrés le interesa o si ahora está convencido de que no puede hacer frente a este estrés (el suyo, el de algunos miembros de su equipo, el de sus compañeros, etc.), aquí tiene algunas medidas que puede tomar sin más demora. Se pueden llevar a cabo de forma individual o colectiva:

- **Medición del estrés:** utilizo la escala PSS y el cuestionario de 10 preguntas para evaluar el nivel de estrés percibido.
- **Retroalimentación**: repaso las situaciones vividas recientemente en las que mi nivel de estrés ha sido incontrolable.
- **Plan de acción:** intento identificar el punto común de estas situaciones (gestión de crisis, supervisión y dirección, postura de liderazgo, exceso de trabajo, etc.) y elaboro un plan de acción específico, con asistencia especializada si es necesario (dirección de RR. HH. de mi organización, ISMS Forum, Advens, profesionales del tema, etc.).
- No hay que esperar a que haya una urgencia (riesgos psicosociales) y hay que saber acudir rápidamente al ámbito médico y/o a los servicios de RR. HH. de la empresa.

Presentación de los ponentes

José Luis Díaz

Es el CEO de Advens España & Portugal. Es ingeniero de telecomunicaciones, posee un EMBA por el IESE Business School.
Con más de 20 años de experiencia en ciberseguridad, comenzó su carrera en PwC como consultor de ciberseguridad y posteriormente ha desempeñado puestos de responsabilidad en Everis y Capgemini.
Se unió a Advens en 2022 para liderar el crecimiento de la compañía en Iberia y contribuir a los objetivos de crecimiento en Europa.

Moisés López

Desde 2025, lidera el área de consultoría de GRC & BC en Advens Iberia, con titulación de ingeniero de sistemas de telecomunicaciones, más de 15 años de experiencia en ciberseguridad y certificaciones tales como CISM, CRISC, AMBCI o CDPSE desarrolla su carrera en varios campos de especialización como la Continuidad de Negocio, Seguridad de la información, Protección de datos, Gestión de Riesgos y Ciberseguridad tanto en consultoría como auditoría. Involucrado en la gestión de equipos y proyectos y en actividades de gestión interna y preventa.

Roberto Baratta

Roberto es ingeniero informático, master en gestión de redes y en comercio electrónico. Es también graduado en seguridad corporativa y en gestión de la seguridad. Tiene amplia experiencia en la gestión de ciberseguridad en entornos complejos y su relación con Riesgo Tecnológico, liderando en varios ámbitos nacionales, europeos e internacionales programas y planes de Ciberseguridad, Resiliencia y Riesgos Tecnológicos en entornos financieros. Asesora a consejos de administración y ejercer de analista y asesor en diferentes ámbitos en varios continentes. Es presidente de ISMS donde lidera las actividades de la asociación y la representa a todos los niveles.

Daniel García

Es licenciado en Periodismo, cuenta con dos másteres oficiales en Periodismo Económico y en Gestión e Investigación de la Comunicación Empresarial. Dispone de una sólida trayectoria en el ámbito de la comunicación, la dirección estratégica y el desarrollo de negocio. Vinculado a ISMS Forum desde hace más de una década, ejerce actualmente como director general, siendo el máximo responsable de la estrategia global de la asociación, su posicionamiento institucional y la definición de las líneas de crecimiento y sostenibilidad económica. A lo largo de su carrera ha impulsado alianzas estratégicas y acuerdos de colaboración con entidades públicas y privadas, liderando la relación con socios, patrocinadores y partners, así como la puesta en marcha de iniciativas de impacto orientadas a la concienciación, la regulación y el fortalecimiento del ecosistema de la seguridad de la información.

Beatriz García

Es licenciada en Psicología Social y con formación de posgrado en Dirección y Gestión de Proyectos, ocupa el cargo de subdirectora y responsable de la Unidad de Proyectos de ISMS Forum. Cuenta con una amplia experiencia en la planificación, dirección y ejecución de proyectos complejos, así como en la coordinación de equipos multidisciplinares y la gestión operativa de iniciativas estratégicas.
Su trayectoria profesional se ha desarrollado de forma transversal en el ámbito de los Recursos Humanos, la gestión del talento y el liderazgo de equipos, aportando una visión organizativa y orientada a personas en la ejecución de los proyectos. Su responsabilidad se centra en el diseño metodológico, la gestión integral y el seguimiento técnico de los proyectos de la asociación, incluyendo programas de formación, certificación, ejercicios estratégicos y proyectos colaborativos con expertos.

Benjamin Leroux

Benjamin Leroux es director de marketing de Advens, donde anteriormente ocupó el cargo de RSSI. Lleva más de 20 años trabajando en el ámbito de la ciberseguridad.

Anexos

Escala de medición del estrés

Desde que los investigadores comenzaron a interesarse por la **evaluación del estrés**, los métodos han evolucionado, ya que el concepto mismo de estrés ha cambiado.

En los años 80, los investigadores se dieron cuenta de que **el impacto de una situación supuestamente estresante no era el mismo para todas las personas** y, sobre todo, que «la valoración que el individuo hacía de esa situación era determinante para su experiencia» (Lindsay y Norman, 1980).

En 1983, **Cohen, Kamarck y Mermelstein** propusieron un cuestionario sobre el estrés percibido basado en el modelo teórico transaccional: la Escala de Estrés Percibido (PSS) tiene como objetivo «evaluar el grado en que los encuestados consideran que su vida es impredecible, incontrolable y sobrecargada».

La PSS permite evaluar de manera global si una persona considera que tiene la capacidad de afrontar o no acontecimientos o momentos difíciles, sin especificarlos. Cohen, Kamarck y Mermelstein (1983) **presentan tres versiones, de 14, 10 y 4 ítems, denominadas PSS14, PSS10 y PSS4**.

Estos modelos **se han utilizado en numerosos países y se han adaptado al ámbito profesional.** La versión española de la PSS10 ha sido objeto de varios estudios y se ha demostrado su fiabilidad y correlación con otros modelos de referencia.

Apéndice

Cuestionario completo y datos del estudio

Referencia metodológica

A1 — Preguntas PSS10

Nº	Pregunta
1	En el último mes, ¿se ha sentido molesto o irritado por acontecimientos inesperados?
2	Durante el último mes, ¿se ha sentido incapaz de controlar los «fundamentos» de su profesión/función/papel?
3	Durante el último mes, ¿se ha sentido nervioso o estresado?
4 (inv.)	Durante el último mes, ¿se ha sentido plenamente capaz de gestionar sus problemas profesionales?
5 (inv.)	Durante el último mes, ¿ha sentido que las cosas iban como usted quería?
6	Durante el último mes, ¿ha pensado que no podía asumir todas las cosas que tenía que hacer?
7 (inv.)	Durante el último mes, ¿ha sido capaz de controlar (interior y exteriormente) su irritación?
8 (inv.)	Durante el último mes, ¿ha sentido que «tenía el control de la situación»?
9	Durante el último mes, ¿se ha sentido irritado porque los acontecimientos escapaban a su control?
10	Durante el último mes, ¿ha sentido que las dificultades se acumulaban hasta tal punto que ya no podía controlarlas?

(inv.) = preguntas de formulación positiva, puntuadas de forma invertida en el cálculo del score PSS.

A2 — Resumen de resultados: factores estresantes

Familia	Pregunta	No/Más bien no	Sí/Más bien sí
Coacción y vigilancia	P13 — Imagen y prejuicios negativos sobre la función	69%	31%
Coacción y vigilancia	P14 — Incomprendido o considerado 'excesivo'	43%	57%
Coacción y vigilancia	P15 — Preocupación por los secretos que maneja	79%	21%
Complejidad	P16 — Falta de experiencia técnica o metodológica	83%	17%
Complejidad	P17 — Dificultad para adaptar análisis ante amenazas cambiantes	61%	39%
Transversalidad	P18 — Cómodo con el alcance funcional y técnico	28%	72%
Combate y adversidad	P19 — Profesión singular: adversarios invisibles	9%	91%
Combate y adversidad	P20 — Frustración por no poder contraatacar	65%	35%
Combate y adversidad	P21 — Desanimado por la frecuencia de ciberataques	68%	32%
Combate y adversidad	P22 — Impotente ante el combate asimétrico	40%	60%
Combate y adversidad	P23 — Se siente personalmente en peligro	80%	20%
Incertidumbre	P24 — Le gustan los imprevistos de la profesión	68%	32%
Incertidumbre	P25 — Perturbado por no conocer a sus atacantes	59%	41%
Incertidumbre	P26 — Constantemente alerta, sin poder desconectar	45%	55%
Incertidumbre	P27 — Situación profesional incierta	41%	59%
Incertidumbre	P28 — Gestión del ciberriesgo intelectualmente difícil	13%	87%
Gestión de crisis	P29 — Cómodo con la adrenalina de las crisis	43%	57%
Gestión de crisis	P30 — Disfruta del equilibrio decisiones/información en crisis	41%	59%
Gestión de crisis	P31 — Apoyado por sus seres queridos en las crisis	13%	87%
Comunicación	P32 — Capaz de expresarse y convencer	15%	85%
Responsabilidad	P33 — Tiene que justificar la utilidad de sus acciones	35%	65%
Responsabilidad	P34 — Culpabilidad cuando se produce un incidente	57%	43%

Contacto

Advens España

www.advens.es

Calle de Agustín de Foxá 4, 28036 Madrid

ISMS Forum

www.ismsforum.es

C. del Segre, 29, 1ºB, Chamartín, 28002 Madrid