Security for the greater good

INTERNATIONAL INFORMATION SECURITY COMMUNITY

Enero de 2024

Factores críticos en la generación del estrés de los CISOs y cómo evitarlos

Tabla de contenidos

1

Resumen Ejecutivo

Resumen Ejecutivo

Durante los primeros meses del año 2023 y viendo que las estadísticas del número de ataques sufridos por empresas españolas seguía creciendo año tras año y que esta circunstancia unida a la presión tanto interna en la propia empresa como de los medios podía influir en la percepción del estrés de los profesionales que nos dedicamos a la ciberseguridad, **Advens e ISMS Forum** se comprometieron a realizar un **estudio sobre el estrés de estos profesionales de la seguridad** de la información, más concretamente, sobre el puesto de responsable de seguridad (CISO) por ser esta figura el máximo responsable dentro de la organización.

Advens propuso esta iniciativa después de descubrir que los estudios realizados al otro lado del Atlántico y del Canal de la Mancha encontraron niveles alarmantes de estrés entre los responsables de seguridad de estos países.

A la vista de dichas conclusiones, ISMS Forum y Advens han elaborado una **encuesta** dirigida al mercado español y a los CISOs españoles asesorados directamente por los miembros del ISMS Forum. Esta encuesta ha sido diseñada por ISMS Forum y Advens, con la ayuda de profesionales, que no son especialistas en la profesión de CISO, pero que son capaces de aportar toda su experiencia en el tratamiento del estrés en contextos exigentes.

La encuesta recopiló respuestas de más de **80 responsables de seguridad**, y se han cubierto todos los sectores de actividad y tamaños de empresas, es decir, una muestra significativa de estas ocupaciones en España.

La encuesta consistió en **dos conjuntos de preguntas**: una serie de 10 preguntas alineadas con un modelo reconocido de medición de la percepción del estrés, la Escala de Estrés Percibido (PSS), y cuyo propósito es determinar el nivel de estrés percibido que experimentan los encuestados de manera individual y personal, y una serie de 22 preguntas para determinar los factores específicos de las tareas diarias de los CISOs que contribuyen al estrés.

Con la escala PSS utilizada, que va de 0 a 40, el estrés se considera positivo o estimulante si el nivel es inferior a 16. Entre los 16 y los 24, se descubren sentimientos ocasionales de impotencia y trastornos emocionales: algunas situaciones se vuelven difíciles de manejar. Por encima de los 22, se alcanza una "zona roja" con mayores riesgos para la salud física y mental, y una sensación de amenaza e impotencia.

La medición del nivel de estrés entre los encuestados condujo a un **nivel promedio de 19,34: esto refleja un alto nivel colectivo de estrés**. 25 personas (30% de los encuestados) se encuentran en la zona verde, y el otro 70% de los encuestados se sitúa en las zonas naranja (30%) o roja (39%) - resultados aproximados - y, por lo tanto, experimentan estrés con efectos negativos. De las 32 personas que se encuentran en la zona roja, 10 están en riesgo de agotamiento. A su vez, otras 10 personas se encuentran incluso en una zona de riesgo de depresión clínica, con una puntuación de 28 o más sobre 40.

Estos niveles de estrés **son preocupantes**. El estrés alto puede ser soportable en un corto período de tiempo. Pero a largo plazo, los niveles más altos pueden tener un impacto grave en la salud mental; y a corto plazo, el estrés repetido puede afectar al rendimiento de los CISOs y, en última instancia, al rendimiento de los sistemas de ciberseguridad.

Por este motivo, recomendamos que se realice una medición periódica del nivel del estrés para determinar si éste conlleva un factor a largo plazo o, por el contrario, es una situación puntual. También habría que volver a medir este estrés a distancia de la situación de pan-

demia, la cual produjo un aumento del mismo sobre un gran número de profesiones. Las empresas IT han estado sometidas a un aumento de las amenazas desde el inicio de la pandemia, y el aislamiento forzado vinculado a las fases de confinamiento puede haber acentuado la sensación de impotencia y desánimo ante las amenazas.

Entre los factores que **más contribuyen al estrés** se encuentran el contexto de adversidad, la dificultad para desconectar y tomar un descanso, la relación con la responsabilidad y la culpa y la sensación de incertidumbre y desconocimiento en el día a día. Además, la función del CISO está en constante evolución. Los más afectados por el estrés experimentan una sensación de impotencia y desánimo ante el poder de los ataques. Otro elemento destacable es que la mayoría de los encuestados están preocupados por la posibilidad de poder perder sus empleos.

En concreto, el **75%** de los encuestados confirma el estrés derivado del contexto de adversidad, ante enemigos que a menudo son invisibles, el **61%** de los encuestados se siente permanentemente alerta, casi una cuarta parte de los participantes no se acostumbra a los peligros e imprevistos del trabajo y el **42%** se siente desanimado por el aumento de la frecuencia y potencia de los ciberataques. En cuanto a las competencias, el **76%** de los encuestados cree que tiene los conocimientos técnicos y metodológicos necesarios, pero solo algo más de la mitad de ellos cree que tiene la capacidad de adaptarse al contexto tan cambiante de la profesión. La gestión del riesgo de ciberseguridad, antes de las acciones de los CISOs, se considera un ejercicio difícil para el **89%** de los encuestados, pero el **74%** de ellos experimenta bastante bien la gestión de crisis. Por último, el **74%** de los encuestados afirma que su trabajo "todavía" adolece de una idea preconcebida bastante negativa, el **75%** sigue sintiéndose incomprendido, o incluso a veces considerado excesivo, y el **62%** cree que una crisis importante podría costarle su trabajo.

Entre las situaciones que aportan factores positivos del análisis del estudio, podemos destacar que los Responsables de Ciberseguridad no se sienten personalmente en peligro, no se preocupan por los secretos a veces delicados que están obligados a guardar, viven bastante bien bajo el hecho de que están del lado de la defensa sin poder tomar represalias y se sienten apoyados por sus seres queridos en momentos extremos de gestión de crisis.

Algunos componentes del trabajo del CISOs son **claramente estresantes**, lo que a veces puede llegar a ser negativo. Si algunos factores parecen difíciles de controlar, como la intensidad de los ataques o su carácter aleatorio, hay ciertos parámetros sobre los que se puede trabajar. Todo esto subraya la riqueza de información de esta encuesta, y también empuja a continuar el ejercicio de análisis, profundizándolo en ciertos temas, y perpetuándolo a través de una medición anual. Dado que las profesiones de ciberseguridad siguen evolucionando, a veces incluso surgiendo en algunas organizaciones, es probable que ciertos factores disminuyan con el tiempo cuando se logre una cierta forma de estabilidad.

En lo que respecta a las respuestas al estrés, se están examinando varias vías que se relacionan con la modificación de las causas del estrés o con la mitigación de las consecuencias. Estas vías pueden formar parte de comunidades como ISMS Forum, a través de talleres de "resiliencia frente al estrés", seminarios ad hoc o la producción de retratos más completos de los profesionales de la Ciberseguridad para entender de manera concreta el tema del estrés en esta profesión, a través de diferentes caminos.

Más allá de las comunidades, el **responsable debe tener en cuenta el estrés**. Debe comenzar tan pronto como se elabore la descripción del puesto, integrarse en el curso de formación y basarse en intercambios con las demás líneas de negocio de la empresa para un mejor conocimiento y comprensión del trabajo, lo que, por cierto, solo puede aumentar la conciencia de los riesgos y el nivel colectivo de preparación frente a un ataque. El mundo académico también tiene un papel que desempeñar en la identificación e integración de los aspectos relacionados con el estrés en la formación de los profesionales de hoy y del mañana.

Comprender y abordar el tema del estrés entre los profesionales de la ciberseguridad es un **enfoque doblemente beneficioso**. Es importante garantizar el entusiasmo, la realización y el equilibrio de las personas afectadas, pero lidiar con el estrés también brinda un enfoque que mejorará el rendimiento. Al trabajar en las causas del estrés, la ciberseguridad progresará. Por un lado, las personas que lo sufren se sentirán mejor equipadas y más apoyadas, y por otro lado, este tema estratégico se integrará mejor en la vida digital de la empresa, con los CISOs debidamente reconocidos y dotados de las palancas adecuadas para llevar a cabo su función.

2

©kittyvector

Introducción

Introducción

El riesgo de ciberseguridad, entendido como cualquier riesgo que surge del uso de tecnologías de información y de comunicaciones y que compromete la confidencialidad, disponibilidad e integridad de datos o servicios, se encuentra en la actualidad en la **parte superior de muchas clasificaciones internacionales de riesgo**. En 2021, la aseguradora Allianz la situó en la primera posición de su barómetro anual de riesgos. Del mismo modo, el Foro Económico Mundial identifica el riesgo de ciberseguridad en su t**op 5 de "peligros claros y presentes"**.

Los reguladores, las aseguradoras y una serie de organismos de supervisión han comprendido claramente la magnitud de este riesgo. Además, con la interdependencia entre las organizaciones, sus proveedores y sus clientes, el riesgo de ciberseguridad se ha vuelto sistémico. Los recientes ataques a empresas renombradas como Air Europa y Sony, son un buen ejemplo de ello.

Pero entonces, ¿se debe recordar que las ciberamenazas se ciernen sobre todas las organizaciones, públicas y privadas, independientemente de su tamaño, dada la creciente dependencia de la tecnología digital y la naturaleza extremadamente lucrativa del cibercrimen?

Desafortunadamente, ¡sí! A pesar de esta naturaleza crítica y estratégica, a pesar de las consecuencias destructivas, está claro que es difícil hacer frente a este riesgo. Este reto es el reto de todas las organizaciones, y está liderado por una mujer o un hombre, quien es el encargado de este área. Bajo el nombre de CISO (Chief Information Security Officer), esta persona se encarga de orquestar todas las acciones que contribuyen al control del riesgo de ciberseguridad.

El auge de la ciberseguridad ha provocado que estos profesionales del sector digital experimenten **grandes cambios**, por no decir trastornos, en los últimos años. Las causas son tan numerosas como los factores de complejidad del control de este riesgo en particular. Las consecuencias para la profesión y para las mujeres y hombres que la asumen son igual de importantes, o, incluso, más.

ISMS Forum y Advens han querido lanzar una gran encuesta sobre el estrés entre CISOs, en diferentes organizaciones. Ante estos cambios que están teniendo lugar en el panorama actual, se consideró importante preguntarse cómo les está yendo a estos profesionales, y si están logrando vivir serenamente en su profesión, que se está transformando, expandiendo y estructurando bajo la presión del creciente fuego de los ciberataques.

Hay **varios elementos que están cambiando en la forma en que se lleva a cabo esta profesión,** que a veces pueden dar una sensación de vértigo, o incluso de desequilibrio. Los profesionales son cada vez más numerosos, aunque a corto plazo los recursos siguen siendo insuficientes. Están surgiendo especialidades, reflejando la riqueza de las profesiones relacionadas con la ciberseguridad, la paleta se ha ampliado con un cursor que se ha movido hacia una mayor detección y respuesta a incidentes. Para algunos, la vida cotidiana está cada vez más marcada por las actividades de seguridad operativa y la gestión de crisis.

El riesgo de seguridad se entiende y se aborda cada vez más por parte de la alta dirección de las empresas, pero el tiempo para asentarse, construir y anticiparse siempre es más costoso.

¿Todos los profesionales de la ciberseguridad están hechos para este tipo de retos y situaciones cada vez más peligrosas? ¿Son capaces de dar el paso atrás necesario para ser buenos estrategas, mientras se enfrentan a una vida cotidiana que requiere cada vez más energía y eficiencia? ¿Les pesa este trabajo o les estimula y excita? ¿Cómo les influye esta situación en la relación con sus seres queridos, sus familias y amigos?

Todos estos son temas que aún **no se han analizado en profundidad,** ya que esta profesión es bastante joven y ha sufrido muchos cambios en los últimos años, y es por ello por lo que Advens e ISMS Forum buscan darle más visibilidad a través de este estudio.

Los medios de comunicación están haciendo una "gran labor" por y para la ciberseguridad. Es el momento de cuidar a quienes nos brindan seguridad y escuchar sus sentimientos sobre este exigente trabajo.

Daniel GARCÍA, ISMS Forum y José Luis DÍAZ, Advens

3

Metodología del estudio

3.1 Introducción

Este estudio nace como reacción a una serie de artículos publicados en medios anglosajones sobre la salud mental de los CISOs, en el Reino Unido y al otro lado del Atlántico. Este contenido, publicado entre principios de 2019 y principios de 2020, planteó el fantasma de los CISOs en medio de una crisis: agotamiento, depresión, consumo excesivo de drogas, alcohol y otras sustancias. ¡Evidentemente la copa estaba llena y la situación era muy grave!

¿Cómo se puede saber lo que realmente significaban estos artículos, con sus títulos a veces pegadizos? ¿Cómo pueden importar estos elementos a Europa o España? ¿Se pueden aplicar las conclusiones a los CISOs españoles? Las culturas corporativas, el derecho laboral, el contexto socio-profesional y muchos otros factores parecen demasiado diferentes como para permitir un "copia/pega" de estos resultados. Sin embargo, la ciberseguridad es un asunto global, y todas las soluciones para hacer frente a los riesgos psicosociales entre los CISOs son buenas.

El tema de la salud mental es interesante y nuevo para la comunidad española. Los temas de la gestión del estrés, la resiliencia emocional y la carga mental están más que nunca en boga desde 2020, el inicio de la pandemia por el COVID y tras los primeros meses de confinamiento.

Así nació este estudio, bajo el impulso de Advens y en colaboración con ISMS Forum, con el objetivo de analizar la situación actual a la que nos enfretamos. ¿Qué pasa con el estrés de los CISOs en España? ¿Hay algún estudio? ¿Qué se puede decir al respecto? La forma más fácil era preguntar a los interesados, y así explotar el poder de convocatoria y el conocimiento y experiencia del ISMS y sus cientos de miembros para tratar de encontrar respuestas y establecer un punto de comienzo para el estudio de la situación.

3.2 El proceso de estudio

Este estudio se ha elaborado en torno a una encuesta dirigida a los CISOs en España. Para llegar a ellos, hemos contado con el apoyo de ISMS Forum. La asociación reúne perfiles de una amplia variedad de orígenes, que trabajan en un sector igualmente variado, en organizaciones de diversos tamaños y desafíos. De este modo, se evitó el sesgo de centrarse únicamente en grupos y empresas multinacionales, por ejemplo.

Es importante destacar un elemento clave del proceso de estudio: la participación de actores externos con conocimientos o experiencia en el manejo del estrés, tanto en la fase de diseño de la encuesta como en el análisis de sus resultados. De hecho, si los iniciadores de este estudio pueden presumir de cierta experiencia en cuestiones de ciberseguridad, no ocurre lo mismo en los temas de salud mental, resistencia al estrés y temas asociados.

La encuesta se basa en dos conjuntos de preguntas, unidas en un solo cuestionario al que los distintos encuestados y voluntarios respondieron en su totalidad.

✓ El primer conjunto de preguntas tiene como objetivo **analizar el nivel de estrés que perciben los CISOs**. Esta percepción es específica de cada persona, las mismas condiciones no desencadenan el mismo nivel de estrés en todos. Por lo tanto, corresponde a cada encuestado estimar una posición en una escala de estrés experimentado, por analogía con la evaluación de la intensidad del dolor en las escalas propuestas por los especialistas en dolor. Esta parte consta de diez preguntas y deriva de un modelo para medir la percepción del estrés, la Escala de Estrés Percibido (PSS). Los resultados de este componente se analizan en la Parte 4.

✓ El segundo conjunto de preguntas consiste en **comprender los detalles del trabajo que podrían ser la causa del estrés que se experimenta**. Se trata de entender qué causa el estrés que se aprecia a través del prisma del trabajo. No se tienen en cuenta factores personales (por ejemplo, situación familiar) o factores profesionales más amplios (relaciones con compañeros o jerarquía, trayectoria profesional, salud de la empresa, etc.). Se analizan una serie de criterios considerados característicos del puesto de Responsable de Ciberseguridad. Las conclusiones provisionales relacionadas con este componente se comparten en la Parte 5.

El estudio busca evaluar la existencia de una preocupación en torno al estrés causado por las características específicas de la profesión de los CISOs; e indirectamente el grado de importancia que la comunidad de la ciberseguridad debe otorgarle. En el caso de un problema comprobado, e independientemente del nivel de intensidad de este estrés, las soluciones no se incluyen en el alcance de este trabajo. Sin embargo, en la Parte 7 se abordan algunas vías y recomendaciones, gracias en particular a la ayuda de las partes externas interesadas.

El cuestionario está compuesto por 32 preguntas en total que se dividen en dos conjuntos diferentes: Las 10 primeras preguntas se entienden como las niveladoras del estrés de la población entrevistada respecto a cómo se han sentido en la gestión de sus tareas y competencias mediante la influencia del estrés, y la percepción de la existencia del estrés en los encuestados.

Las 22 preguntas restantes, que se definen como "estresores", se organizaron según una tipología de 8 familias: coerción y vigilancia, complejidad y evolución, transversalidad, combate y adversidad, incertidumbre y desconocido, gestión de crisis, comunicación y convicción y responsabilidad y culpa. La mayoría de estas 22 preguntas, 17 de 22, destacan los factores que contribuyen al estrés, mientras que 5 de las 22 preguntas se centran en los factores que no parecen aumentar el estrés.

Pregunta	**Las 5 preguntas dentro de las 22 que conforman la segunda parte del estudio que NO contribuyen al estrés de manera afirmativa (La respuesta no es "Sí, absolutamente", sino "No, en absoluto"):**
18	¿Se siente cómodo con el alcance funcional y técnico que debe cubrir el negocio cibernético, que debe garantizar una defensa eficaz en todas partes, a todos los niveles y en todos los terrenos?
30	¿Ha experimentado grandes niveles de adrenalina, presión y/o sensación de urgencia generalmente asociadas a una cibercrisis?
31	¿Aprecia el ejercicio peligroso, el equilibrio permanente entre las decisiones a tomar y la información disponible para poder tomarlas, a lo largo de una crisis?
32	¿Te sientes comprendido o al menos apoyado por tus seres queridos durante los períodos en los que estás lidiando con crisis?
33	¿Cómo se siente comunicando? ¿Es capaz de expresarse de verdad, de empatizar con los demás y de convencerlos?

Para el análisis posterior de resultados en este informe, se han omitido en la parte contribuyente al estrés estas 5 preguntas ya que realmente no impactan de manera afirmativa al estrés, sino más bien lo contrario, de forma negativa. Como consecuencia, se han utilizado las respuestas con el número de porcentajes más elevados que se encontraban a continuación de estas preguntas en la lista de resultados.

Por otro lado, estas son las preguntas que contribuyen afirmativamente al estrés:

Pregunta	Preguntas que contribuyen de manera activa al estrés:
13	¿Sufre la imagen del CISO percepciones negativas e ideas preconcebidas relacionadas con su función que pueden complicar su trabajo e incluso provocar sentimientos de aislamiento?
14	¿Se siente incomprendido o juzgado como "excesivo" cuando hace recomendaciones?
15	¿Le dan pavor las situaciones en las que su trabajo le obliga a estar al tanto de secretos y/o le coloca en situaciones humanamente delicadas o embarazosas?
16	¿Considera que le faltan conocimientos técnicos o metodológicos?
17	¿Le resulta difícil tener que adaptar constantemente sus análisis y estrategias ante un entorno de amenazas complejo en rápida evolución y tener que aprender y reinventarse constantemente?
19	¿Considera que su trabajo es inusual en el sentido de que implica tratar con adversarios que a menudo son "invisibles" y malintencionados, lo cual es inhabitual porque pocas profesiones experimentan
20	¿Le frustra estar únicamente a la defensiva y no poder nunca tomar represalias o contraatacar?
21	¿Se siente desanimado por la creciente frecuencia y potencia de los ciberataques?
22	¿Se siente impotente ante la naturaleza asimétrica del combate, en el que el atacante tiene una clara ventaja sobre el defensor?
23	¿Se siente alguna vez personalmente en peligro ante tal adversidad?
25	¿Le molesta no conocer de antemano, o incluso no conocer nunca, a quienes le atacan o cometen un acto malicioso?

26	¿Está constantemente en alerta, incapaz de desconectar sus pensamientos de su trabajo, por miedo a que se produzca un ciberataque o una situación de alto riesgo?
27	¿Siente que su situación profesional es incierta y que una crisis importante podría costarle el puesto de trabajo?
28	¿Considera que la gestión del ciberriesgo es intelectualmente difícil?
29	¿Ha experimentado grandes niveles de adrenalina, presión y/o sensación de urgencia generalmente asociadas a una cibercrisis?
33	¿Siente que tiene que justificar ante los demás, o incluso ante sí mismo, la utilidad de sus acciones?
34	¿Se siente culpable a los ojos de los que le rodean y/o de sus superiores cuando se produce un incidente y no fue capaz de evitarlo, detectarlo y/o limitar su impacto?

Los resultados de la encuesta no solo fueron analizados por los clientes habituales de ciberseguridad, sino que además han contado con la valoración y evaluación de una serie de ponentes que se presentarán en el siguiente apartado.

3.3 Promotores del estudio

Benjamin Leroux

Benjamin Leroux es Director de Marketing en Advens. Lleva 20 años trabajando en el campo de la ciberseguridad. Comenzó su carrera en Accenture e Idemia y luego trabajó como CISO en el sector financiero. Se unió a Advens en 2012 para desarrollar las ofertas de consultoría y soporte del CISO. Ahora está a cargo de definir y liderar todas las ofertas de Advens y el catálogo de servicios asociado, para hacer que la seguridad sea más accesible, más ágil y eficiente. Benjamin representa a Advens en CESIN, CLUSIF y otros grupos profesionales en Francia.

Benjamin ha estado liderando el estudio del estrés del CISO que se realizó en Francia, y ahora en España tiene toda la información para poder establecer comparaciones con los resultados anteriores.

Gonzalo Asensio

Apasionado por el sector de la Seguridad Digital.

La misión principal de Gonzalo Asensio es ofrecer soluciones y respuestas eficaces al Comité de Alta Dirección y Consejeros para potenciar y proteger el negocio.

Lleva en el sector casi 20 años trabajando en grandes empresas (BANKINTER, TELEFÓNICA, ING, etc) creando y liderando equipos de dirección.

En los últimos años también he desempeñado el rol de Consejero y Asesor de Ciberseguridad, algo que le ilusiona y le reta porque puede compartir su visión y experiencia.

Speaker en los principales eventos del sector (RootedCon, ISMS FORUM, CSA) y profesor de Ciberseguridad en algunas de las mejores empresas de España (IE, UNIVERSIDAD COMPLUTENSE, EDEM, IBERIA, UNIDAD EDITORIAL).

José Luis Díaz

José Luis Díaz es el CEO de Advens en Iberia. 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, Capgemini y Cipher. Se unió a Advens en 2022 para liderar el crecimiento de la compañía en España y contribuir a los objetivos en Europa.

ISMS Forum: Daniel García y Beatríz García

Con formación en periodismo, Daniel García ha contribuido significativamente a ISMS Forum desde 2011, ocupando actualmente el cargo de Director General. Durante este tiempo, ha destacado en la dirección de relaciones públicas e institucionales, así como en la coordinación de iniciativas y proyectos clave para la organización.

Beatriz García, licenciada en Psicología Social por la UCM, desempeña actualmente el cargo de Subdirectora de las áreas de Formación, Certificación y Proyectos en ISMS Forum. Con una trayectoria profesional que abarca más de 15 años en el ámbito laboral y de recursos humanos, ha consolidado su experiencia como líder en la gestión estratégica de proyectos y el fomento del conocimiento en ciberseguridad.

3.4 El Grupo de CISOs

Tras la construcción del análisis de los resultados, se obtuvo la respuesta de 82 CISOs. La distribución de la encuesta ha sido comunicada a través de los CISOs asociados a ISMS Forum, tanto de empresas públicas como privadas. Esta muestra de personas pertenece al mercado español. La muestra consultada consiste en 82 personas pertenecientes a la función de gestión de la ciberseguridad. Ya sean CISOs o Deputy CISOs.

3.5 Estudios similares

El asunto del estrés en la función de seguridad ha sido un tema que ha aumentado su importancia e interés a lo largo de los años. Un estudio relevante por la empresa Nominet Cybersecurity, desde una perspectiva anglosajona, señala datos tan preocupantes como los siguientes:

→ Cerca del 17% de los CISOs **se medican o recurren al alcohol** para tratar con el estrés.

→ 21,9% de los CISOS encuestados **nunca desconectan o se toman un descanso** de sus responsabilidades.

Sobre la base de los anteriores outputs, no podemos obviar que el **vínculo entre la ciberseguridad y la salud es muy estrecho**.

En España, el estudio sobre el estrés ha empezado a abordarse a pequeña escala y sobre posiciones más técnicas. Dicho esto, la revista SIC se hace eco del estudio llevado a cabo por Trend Micro, donde se destaca que el 66% de los profesionales encuestados en España (gestores de alertas en SOCs) declaran que su vida personal se ha visto afectada por la tipología de trabajo que desempeñan.

La aportación que pretende hacer Advens en colaboración con ISMS Forum es arrojar luz en España sobre la situación de estrés de la función del CISO, ofreciendo una perspectiva holística del efecto del estrés, y focalizando el tema en los principales holders de esta cuestión: los Responsables de Ciberseguridad.

4

Conócete a ti mismo:
Evaluación del estrés percibido

4.1 Justificación del estudio

El objetivo inicial del estudio es identificar la existencia, o no, de un problema relacionado con el estrés de los profesionales de la ciberseguridad y relacionado con la naturaleza de su profesión. Si la mayoría de los encuestados no sienten los efectos del estrés negativo, es poco probable que el tema requiera un análisis más profundo.

Por lo tanto, es esencial comenzar por medir el nivel de estrés que sienten los CISOs encuestados. Este es el tema de la primera parte de la investigación. El primer reto para hacerlo fue la elección del método. Como el sujeto está ligado a un estrés sentido, por naturaleza propia de cada entrevistado, fue necesario definir un abordaje racional e idealmente universal, que facilite la comparación e integre los sesgos de percepción.

Para lograrlo, el aporte de las partes interesadas externas fue más que beneficioso y permitió el uso de un método reconocido en el campo de la evaluación del estrés. Este método fue el tema de la primera parte del cuestionario, cuyas preguntas se dan en la sección siguiente, junto con las respuestas a modo de conclusiones gráficas y los resultados detallados en el apéndice.

4.2 Escala de medición del estrés

Desde que los investigadores se interesaron en evaluar el estrés, **los métodos han evolucionado porque la concepción misma del estrés ha cambiado**. En la década de 1980, los investigadores se dieron cuenta de que el impacto de una situación supuestamente estresante no era el mismo para diferentes personas y, sobre todo, que "la evaluación del individuo de esta situación era decisiva sobre su experiencia" (Lindsay y Norman, 1980).

En 1983, Cohen, Kamarck y Mermelstein propusieron un cuestionario de estrés percibido basado en el modelo teórico transaccional: la Escala de Estrés Percibido (PSS), que tiene como objetivo "evaluar el grado en que los encuestados sienten que sus vidas son impredecibles, incontrolables y sobrecargadas". El PSS permite evaluar de forma global si una persona siente o no que tiene la capacidad de afrontar acontecimientos o momentos difíciles de vivir, pero no los concreta. Cohen, Kamarck y Mermelstein (1983) presentan tres versiones, en 14, 10 y 4 ítems, bajo las designaciones PSS14, PSS10 y PSS4.

Estos modelos se han utilizado en muchos países y se han adaptado al mundo profesional. La versión española del PSS10 ha sido objeto de varios estudios y se ha demostrado su fiabilidad/correlación con otros modelos de referencia.

Como parte de este estudio, las 10 preguntas del PSS10 se incluyen entre las 32 preguntas realizadas.

Pregunta	Preguntas PSS10:
1	En el último mes, ¿te has sentido molesto o molesto por eventos imprevistos?
2	Durante el último mes, ¿te has sentido incapaz de controlar los "fundamentos" de tu trabajo/función/rol?
3	En el último mes, ¿te has sentido nervioso o estresado?
4	Durante el último mes, ¿te has sentido plenamente capaz de manejar tus problemas profesionales?
5	Durante el último mes, ¿has sentido que las cosas van como tú quieres?
6	En el último mes, ¿has pensado que no puedes hacer todas las cosas que tienes que hacer?
7	Durante el último mes, ¿has podido controlar (interna y externamente) tu molestia?
8	Durante el último mes, ¿has sentido que tienes el "control"?
9	En el último mes, ¿te has sentido irritado porque las cosas estaban fuera de tu control?
10	Durante el último mes, ¿has descubierto que las dificultades se han ido acumulando hasta el punto en que ya no puedes controlarlas?

Las respuestas a las preguntas se califican entre 0 (Estrés bajo) y 4 (Estrés alto). En el estudio, los puntos se otorgan de acuerdo con la siguiente escala: Nunca = 0, Casi nunca = 1, A veces = 2, Algo a menudo = 3, A menudo = 4. Esto es válido para todas las preguntas excepto para las cuatro cuestiones llamadas "invertidas" (Q6, Q7, Q9, Q10), donde Nunca = 4, Casi Nunca = 3, etc. Al sumar las puntuaciones de las 10 preguntas, se obtiene un total entre 0 y 40 para cada participante.

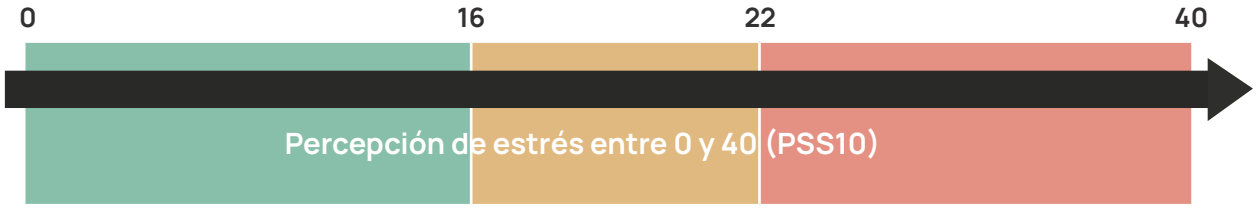
4.3 Análisis del estrés percibido

El resultado mostrado a continuación deriva de la metodología explicada anteriormente, la cual recoge la suma de las 10 primeras preguntas de la percepción del estrés sobre los encuestados, que supone la primera parte del informe.

Preguntas PSS10 :		Promedio de respuestas
1	En el último mes, ¿se ha sentido molesto o irritado por acontecimientos inesperados?	2,46
2	En el último mes, ¿se ha sentido incapaz de controlar lo "básico" de su trabajo?	2,13
3	En el último mes, ¿se ha sentido nervioso o estresado?	2,70
4	En el último mes, ¿se ha sentido plenamente capaz de gestionar sus problemas profesionales?	1,40
5	En el último mes, ¿ha sentido que las cosas iban como usted quería?	1,85
6	En el último mes, ¿ha sentido que no podía hacer frente a todas las cosas que tenía que hacer?	2,56
7	En el último mes, ¿ha sido capaz de controlar (interna y externamente) su irritación?	1,02
8	En el último mes, ¿se ha sentido en control de la situación?	1,45
9	En el último mes, ¿se ha sentido irritado porque los acontecimientos escapaban a su control?	2,00
10	En el último mes, ¿ha notado que las dificultades se acumulaban hasta tal punto que ya no podía controlarlas?	1,76
Total		**19,34**

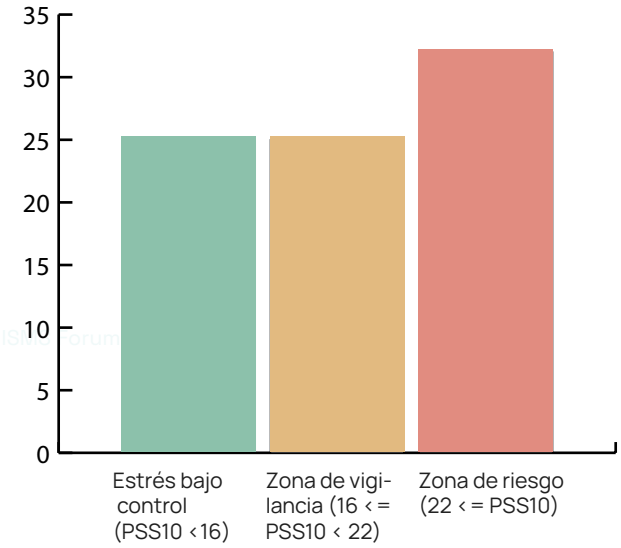
La puntuación media en el panel es de **19,34** puntos. Se trata de un **nivel de vigilancia representativo**. De hecho, como se muestra en los gráficos a continuación, una puntuación de 16/40 representa el punto de inflexión entre la estimulación del estrés y el estrés que comienza a causar disgustos emocionales y conductuales. Una puntuación de 22/40 representa un paso a una zona de riesgo para la salud física y mental.

Zona verde	Entre 0 y < 16	De la calma al estrés "estimulante" o "positivo.
Zona naranja	Entre 16 y < 22	Sentimientos ocasionales de impotencia que conducen a alteraciones emocionales, situaciones que a veces son difíciles de manejar.
Zona Roja	≥ 22	Fuerte sentimiento de impotencia, sensación de amenaza más o menos difusa, riesgos para la salud física y mental (tensión arterial, IMC, eficacia del sistema inmunitario, trastornos del sueño, adicciones, etc.).



El resultado **no es positivo**. Los CISOs se encuentran bajo unos niveles de estrés que han de **vigilarse** y que se repiten de manera ocasional, como si fuese un hábito. Ya de por sí, esto supone que los encuestados encuentran dificultades para enfrentarse a situaciones que les generan alternaciones emocionales, produciendo ese malestar y sensación de pérdida de control que deriva en estrés. Por lo tanto, es una franja que debe tenerse bajo vigilancia. No obstante, el % de encuestados que se encuentran en la zona naranja no es el más elevado. La zona de vigilancia viene a representar a un 30% de los encuestados (25 CISOs), mientras que la zona verde, la cual habla de un estrés que es estimulante y positivo y que por lo tanto no es nocivo y se puede considerar «saludable», representa otro 30% del grupo de encuestados (25 CISOs):

No obstante, la franja más preocupante se encuentra en la zona de riesgo. Los encuestados **representados en el área roja simbolizan el % más alto de todos con un 39%, lo que es equivalente a 32 CISOs. Esto quiere decir que un alto número de participantes se encuentran en una situación que comienza a ser crítica en relación con su salud mental y física y un malestar general que deriva en riesgos de amenaza y situaciones constantes de impotencia.**



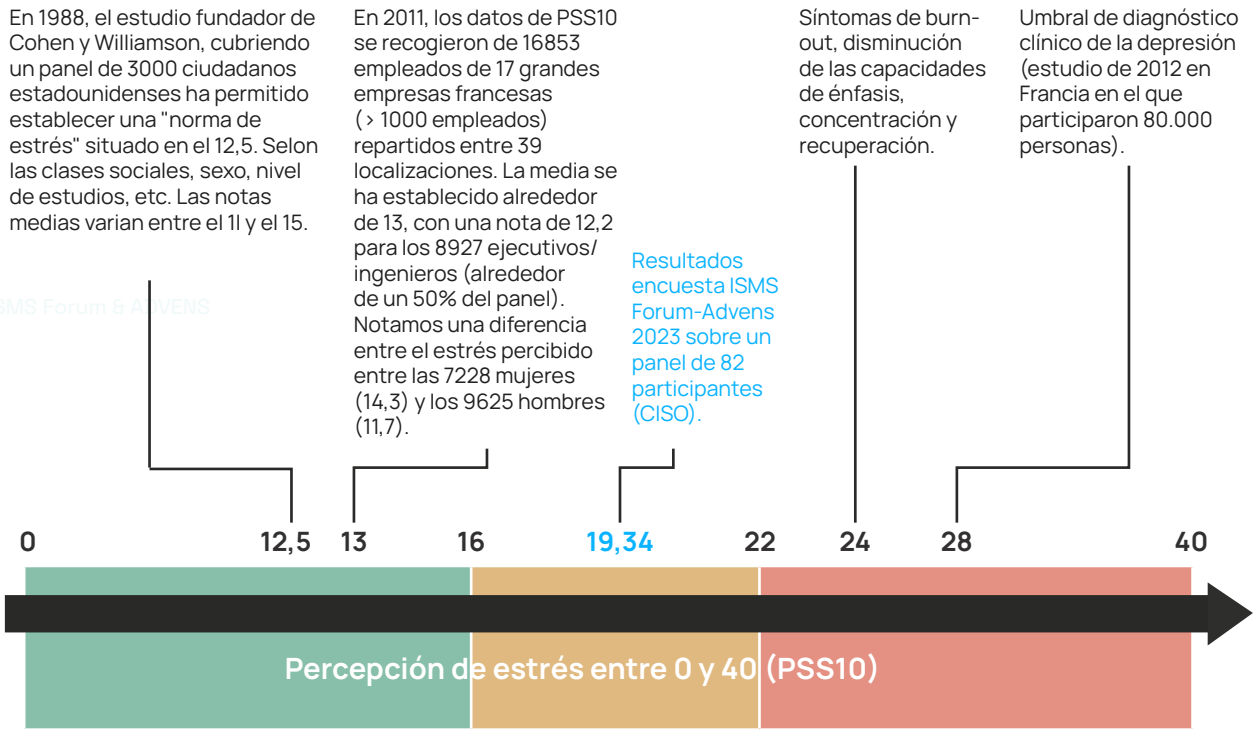
Clasificación resultados por zonas de riesgo

Dentro de los encuestados que se encuentran bajo el color rojo, se puede hacer una distinción entre todos ellos:

Zona de riesgo: la zona de riesgo es como se llama a todo el conjunto que engloba a los encuestados que han obtenido un resultado que está por encima de 22 puntos (incluyendo el mismo). No obstante, dentro de los mismos, hay una zona que representa un nivel de riesgo "leve", bajo el cual se engloban 12 personas, es decir, un 38% del total de las 32 personas (39%) del total de los participantes. Estos encuestados están bajo niveles de estrés importantes que deben comenzar a tenerse en cuenta y a frenar para evitar su avance.

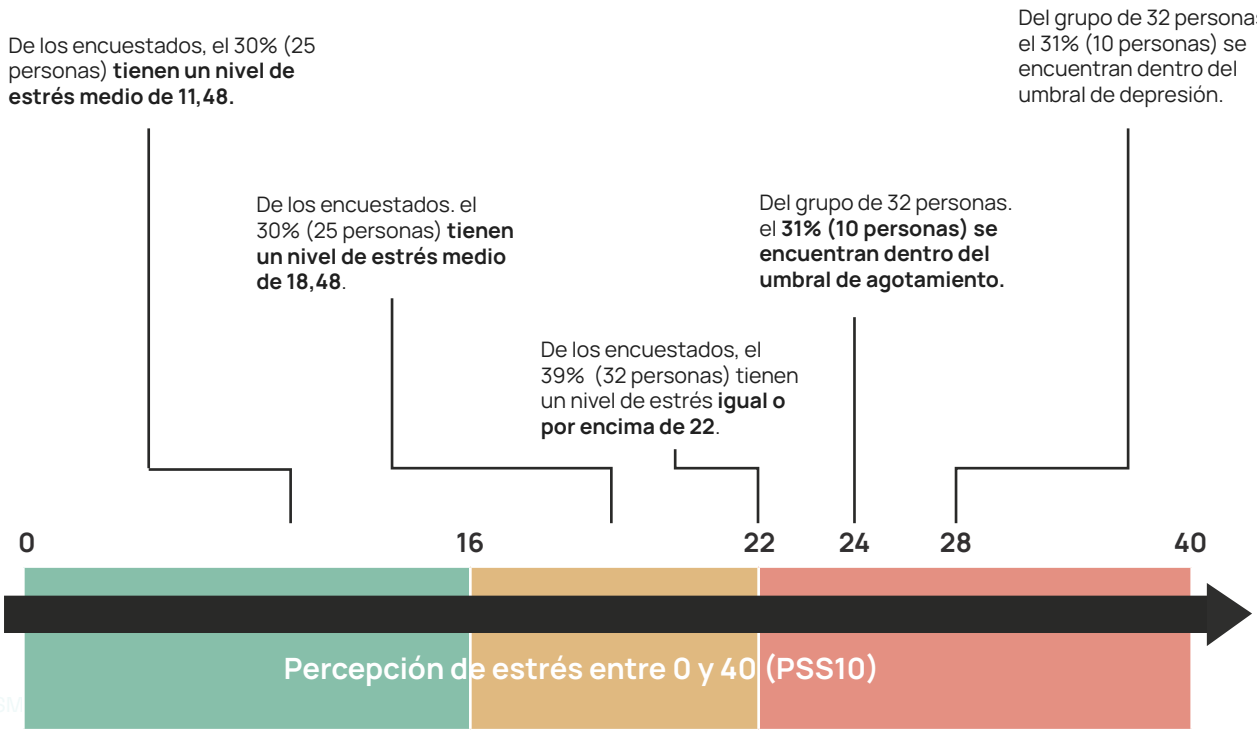
Zona de agotamiento: la zona de agotamiento representa un nivel dentro del riesgo más elevado. Los encuestados recogidos dentro de este rango representan un 31% (10 personas) de las personas dentro de la franja roja y su estado y niveles de estrés son más altos. Están agotados a nivel físico y mental y se engloban dentro de una franja preocupante, donde pueden darse bloqueos y sentimientos constantes y reiterativos de un malestar general.

Zona de depresión: representa el estado más grave. Los encuestados que entran dentro de esta franja representan el 31% de la zona roja (10 personas) y su estado es crítico. Es una franja en la que es recomendable con urgencia acudir a un especialista médico que tome cartas en el asunto para abordar la situación, un panorama completamente desbordante. A continuación, se presentan unas gráficas donde se reflejan los resultados y su significado de una forma más visual y donde se incorpora la historia de todo este proceso metodológico hasta el día de hoy.

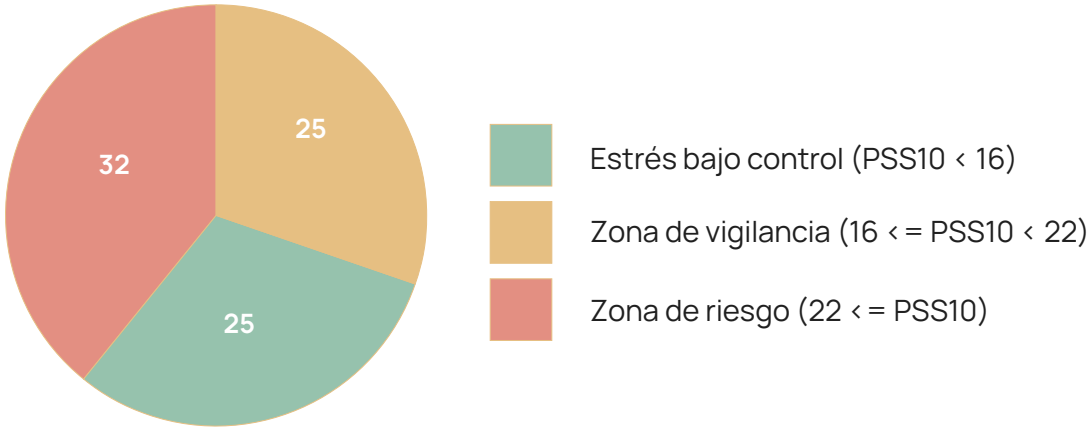


En ambas gráficas se representa el impacto histórico de esta metodología, así como el proceso de realización del mismo cuestionario y sus características.

Se observa un nivel **muy equitativo** en cuanto a la situación de los encuestados respecto a las diferentes franjas; en cualquier caso, el segmento con más peso es aquel igual o superior a 22, lo que destaca que los CISOs empiezan a sufrir un mayor agotamiento mental en el ejercicio de sus funciones, sobresaliendo que el **12,2%** se encuentra en el umbral de depresión.



En estas dos últimas gráficas se reflejan los porcentajes y el número de personas donde se simplifican las explicaciones anteriores zona por zona.



Se observa que el grupo mayoritario, sin constituir este la mayoría absoluta del estudio, es aquel cuyos encuestados se sitúan en el grupo de riesgo (>22). Este es un resultado muy significativo respecto a la muestra, que arroja una latente realidad de la dificultad y ejercicio del rol del CISO. La zona roja está marcada por la mala afección a la salud producida a las personas que pertenecen a este segmento. El 24,4% (20 personas) se sitúan en los umbrales de agotamiento y depresión; una realidad la cual no permite echar la vista a otro lado, y exige ser tratada desde la raíz.

5

Evaluación de los factores estresantes

5.1 Tipología de estresores

Una vez realizado el diagnóstico sobre el nivel de estrés experimentado, el objetivo del estudio es encontrar los factores que contribuyen a este **estrés que son específicos del entorno de la ciberseguridad**.

De hecho, los trabajos de ciberseguridad forman parte de todas las profesiones digitales y, por lo general, se enfrentan a las dificultades comunes de estos oficios. Más allá de estos inconvenientes, que ya han sido ampliamente analizados y comentados, el objetivo de este estudio es centrarse en lo que constituyen las particularidades de las profesiones de ciberseguridad y qué es susceptible de poner a prueba mentalmente a estos profesionales. Por lo tanto, es necesario determinar si los factores específicos de la ciberseguridad realmente están contribuyendo al estrés experimentado y, en caso afirmativo, cuáles son los más agravantes. Esto con el fin de guiar la búsqueda de formas de tratar y reducir el estrés experimentado.

Para ello, se formularon **22 preguntas** que pusieron de manifiesto una serie de criterios específicos de la profesión de Ciberseguridad. Estas preguntas se han agrupado en **8 dominios**:

1. Coerción y vigilancia: el CISO define estrategias de defensa que conducen:

→ Por un lado, a prohibir o bloquear determinadas acciones llevadas a cabo por los empleados (que también son sus compañeros), como medida preventiva, lo que puede hacerle aparecer como censor.

→ Por otro lado, a recopilar y analizar rastros, disponiendo así de los medios para observar las prácticas profesionales y personales de los empleados (porque integran una parte personal en su uso de los recursos informáticos) y anotar las desviaciones de una política interna o de las buenas prácticas, que pueden dar lugar a llamadas al orden o incluso sanciones. El CISO puede aparentar ser un controlador («hermano mayor») y juez.

2. Complejidad y escalabilidad: la riqueza de la tecnología, la integración masiva de servicios en la nube y las múltiples expectativas de los clientes internos y externos hacen de los sistemas de información de las organizaciones contemporáneas, extendidas e hiperconectadas, un terreno complejo para protegerse de las amenazas en constante evolución. Esto conduce a un contexto rico y cambiante, que requiere un cuestionamiento constante de las estrategias a adoptar.

3. Transversalidad: para ser lo suficientemente completa y eficaz, la ciberdefensa debe ser omnipresente. Debe integrarse en toda la empresa y a todos los niveles, en todas las arquitecturas, en todos los componentes técnicos, en todas las líneas de negocio, integrando por supuesto el factor humano.

4. Combate y adversidad: el CISO se enfrenta a una situación rara entre las profesiones de la empresa: la de tener que enfrentarse a adversarios externos e internos de la compañía. Una situación que lo pone en el papel de un luchador. Además, dado el nivel de amenaza actual y la intensidad de la ciberdelincuencia, esta lucha es asimétrica, con un poder de ataque a menudo muy superior a la capacidad de defensa de una organización determinada.

5. Incertidumbre e incógnita: El ejercicio de la defensa se enfrenta a una incertidumbre constante sobre el momento y la forma del próximo incidente. Esto obliga al CISO a estar preparado para cualquier eventualidad y en cualquier momento, ya que nunca puede considerar que está totalmente protegido.

6. Gestión de crisis: La gestión de crisis es un componente importante de la profesión de ciberseguridad. Requiere un alto nivel de disponibilidad y exige proponer y/o tomar decisiones bajo presión y sin tener todos los elementos de apreciación. Se basa en pocos modelos históricos conocidos. El CISO gestiona sus crisis haciendo todo lo posible para evitar los sesgos cognitivos que pueden parasitar o paralizar su acción.

7. Comunicación y convicción: debido a que aborda muchas de las líneas de negocio de la empresa para obtener su apoyo y aporte, el CISO debe saber comunicar y convencer en un campo que puede parecer austero, restrictivo y que requiere un esfuerzo colectivo necesario.

8. Responsabilidad y culpa: el CISO implementa planes de acción que requieren recursos financieros y humanos, y es probable que impongan restricciones operativas. La eficacia de su enfoque es examinada y juzgada. Aunque sus estrategias sean relevantes y de muy buen nivel para hacer frente a los riesgos, la empresa no puede ser completamente inmune a una crisis con un impacto significativo. Por lo tanto, el gerente se enfrenta a dos posibles reacciones de duda y juicio. Si no pasa nada, «¿qué sentido tiene todo esto?» y si hay una crisis importante, «todo ha sido en vano». Un cóctel con un sabor a veces amargo de inutilidad y culpa...

Estos diferentes criterios pueden situar al CISO en un contexto de duda, miedo, inestabilidad y cuestionamiento de sus valores. Por lo tanto, se tuvieron en cuenta en la segunda parte de nuestro estudio sobre la identificación de los factores que contribuyen al estrés.

5.2 Principales factores estresantes

Si nos fijamos en la media de las respuestas a las 22 preguntas relativas a estos criterios, se observa que 17 preguntas obtienen un resultado a favor de una contribución al estrés, mientras que 5 preguntas se refieren a factores que tienen poca influencia en el estrés.

A continuación, se muestra cuáles han sido las **preguntas que más han afectado a los encuestados de manera positiva y negativa al estrés**. Durante el estudio, las 22 preguntas (17 afirmativas y 5 negativas) se han contestado sin diferencias entre ellas. Los siguientes datos demuestras la subjetividad de los encuestados al contestar, donde podemos destacar un TOP 5 de preguntas que han sido respondidas con "No, en absoluto", con porcentajes más altos que no necesariamente tienen que coincidir con las 5 preguntas que metodológicamente explicadas con anterioridad, contribuyen de manera negativa al estrés (un "Sí en absoluto" no contribuye al estrés, mientras que un "No en absoluto"; sí).

En este caso, se puede apreciar que los encuestados han votado como menos contribuyentes a su estrés, un **TOP 5** de preguntas que entran en las 17 que impactan de **manera positiva al estrés**.

Si hablamos de estos últimos factores, se puede observar desde el punto de vista de los CISOs que:

→ Se sienten relativamente cómodos con los secretos que guardan (P15).

→ No necesariamente se sienten frustrados por no poder contraatacar (P20).

→ No se sienten desanimados por la creciente frecuencia de los ciberataques (P21).

→ No se sienten personalmente inseguros en el ejercicio de su profesión (P23).

→ No sienten necesariamente que una crisis de ciberseguridad afecte o ponga en peligro de manera directa su puesto de trabajo (P27).

A continuación, se muestran los datos del **TOP 5 de preguntas que los encuestados han votado con porcentajes más altos de preguntas que sí contribuyen de manera afirmativa al estrés**, es decir, que han sido votadas con "Sí, absolutamente", las cuales se agrupan en las siguientes familias de criterios. (Cabe recordar que cada pregunta del cuestionario va englobada dentro de una familia de criterios. Algunas de estas familias cuentan con más de una pregunta dentro de su dominio).

Las familias de criterios que tienen más probabilidades de contribuir al estrés son:

1. **El alto nivel de incertidumbre y lo desconocido** (cuenta con dos de las preguntas más votadas dentro de su dominio). Es la familia más votada, con una media ponderada de 13,52 puntos.

2. **El contexto de combate y adversidad.** Es la segunda familia más votada, con una media ponderada de 12,34.

3. **Gestión de crisis.** Siendo la tercera familia más votada, con una media ponderada de 8,51. (Cuenta con dos de las preguntas más votadas dentro de su dominio).

Si nos fijamos más en los 3 factores que más estrés generan, se puede observar que **predomina el alto nivel de incertidumbre y lo desconocido**, el cual se ha repetido en dos preguntas en esta familia de criterios. El permanecer en un limbo, y un estado donde no se puede prever qué ocurrirá a ciencia cierta, es un factor que influye de manera muy incisiva en el estrés de los CISOs. A continuación, observamos la **sensación de adversidad**, frente a la cual, los encuestados están constantemente alerta, sin poder desconectar nunca, por miedo a un suceso. Esta situación de inestabilidad se ve agravada por el hecho de que la amenaza está en constante evolución y requiere una defensa igualmente evolutiva, por lo que la **gestión de crisis se vuelve más compleja**, y contribuye a aumentar el efecto de la incertidumbre, y, con ello, el estrés. La profesión navega en territorio hostil, con un contexto de desequilibrio permanente. También debe justificar la utilidad de su acción y no tiene derecho a cometer

errores porque puede llevar al cuestionamiento de su posición, generando un nivel de responsabilidad y culpa elevados. Esta observación busca dar un **mayor reconocimiento a la naturaleza exigente de la profesión**.

Si restringimos esta observación a la población cuyo nivel de estrés está en rojo (puntuación superior a 22), se puede distinguir la aguda sensación de adversidad, pero también se deja entrever un sentimiento de impotencia ante la asimetría del combate y la dificultad de entender y afrontar los riesgos de ciberseguridad. Esta población ya no evoca la necesidad de desconectar, porque están envueltos en el compromiso que el trabajo requiere. Pero se siente impotente ante la magnitud de la tarea. El sentimiento de desaliento se expresa claramente.

Echemos un vistazo a los criterios que generan una opinión clara de "Sí, absolutamente" o "No, en absoluto".

Los factores que más contribuyen al estrés entre los encuestados son:

Los 5 factores principales que más contribuyen al estrés en todos los encuestados:	Número de pregunta
Dificultad del ejercicio de gestión del riesgo.	Pregunta 28
El no conocer al enemigo y no ponerle cara genera una situación de estrés que es propia y característica de esta profesión.	Pregunta 19
La gestión de crisis es compleja y deriva en un aumento de la adrenalina y del estrés a la hora de enfrentarse a un ciberataque.	Pregunta 29
Imposibilidad de desconexión total del trabajo y sus funciones.	Pregunta 26
La situación profesional es incierta, una crisis importante puede costar el puesto de trabajo.	Pregunta 27

Si el análisis se centra en las personas que más sufren, es decir, en la zona roja, los factores más marcados se convierten en:

Los 5 factores principales que más contribuyen al estrés en los encuestados con niveles de estrés en números rojos (> 22):	Número de pregunta
Dificultad del ejercicio de gestión del riesgo.	Pregunta 28
La gestión de crisis es compleja y deriva en un aumento de la adrenalina y del estrés a la hora de enfrentarse a un ciberataque.	Pregunta 29
El no conocer al enemigo y no ponerle cara genera situación de estrés que es propia y característica de esta profesión.	Pregunta 19
La situación profesional es incierta, una crisis importante puede costar el puesto de trabajo.	Pregunta 27
- Falta de concienciación en el entendimiento de la toma de decisiones. - Frustración al no poder ejecutar contramedidas durante los ataques. - Sentimiento constante por sentirse siempre "por detrás" durante los ataques. - Imposibilidad de desconexión total del trabajo y sus funciones.	Pregunta 14, 20, 22, 26

Los primeros 4 factores dominantes son similares para todos los encuestados y para la población en la zona roja. No obstante, los encuestados en la zona roja, en quinto lugar, **barajan 4 preguntas que han sacado el mismo número de puntos, donde solo una de ellas coincide con la de todos los encuestados**. Las preguntas 14,20 y 22 son únicas de los encuestados en zona roja. Por un lado, estos encuestados se sienten excesivamente juzgados cuando hacen algún tipo de recomendación o toma de decisión en comparación al resto de la población. Esto es un factor agregado a la responsabilidad del cargo del CISO. A continuación, la siguiente respuesta refleja también un rasgo característico de dicho puesto, pues recalca que en su cargo únicamente puede tomar acciones defensivas, aunque su deseo ante ciertas circunstancias sea el de efectuar contramedidas. Por último, una característica fundamental en el mundo de la ciberseguridad es la ventaja con la que cuentan los atacantes y la sensación constante de ir un paso por detrás de ellos. Estas últimas tres respuestas han tenido la misma puntuación y se cuentan dentro del factor 5. Podemos comprobar que son más específicas y que a la población en la zona roja que está expuesta a un nivel de estrés mayor le afectan de cara a la ejecución de su trabajo.

Por otro lado, los estresores que mejor se controlan o los factores más favorables son:

Los 5 factores principales mejor controlados por todos los encuestados:	Número de pregunta
Acceso a secretos que pueden ser humanamente difíciles de conocer.	Pregunta 15
Nunca poder tomar represalias contra un ataque.	Pregunta 20
La sensación de estar personalmente en peligro.	Pregunta 23
No conocer a tu(s) oponente(s) en la mayoría de los casos.	Pregunta 25
Contar con el apoyo de los seres queridos durante la gestión de crisis de ciberseguridad.	Pregunta 31

Y considere este análisis para aquellos que están en la zona roja.

Los 5 factores mejor controlados entre los encuestados con niveles de estrés en números rojos (> 22):	Número de pregunta
Nunca poder tomar represalias contra un ataque.	Pregunta 20
Acceso a secretos que pueden ser humanamente difíciles de conocer.	Pregunta 15
No conocer a tu(s) oponente(s) en la mayoría de los casos.	Pregunta 25
Contar con el apoyo de los seres queridos durante la gestión de crisis de ciberseguridad.	Pregunta 31
La sensación de estar personalmente en peligro.	Pregunta 23

Existe una similitud general en las respuestas sobre estos 5 factores, aunque el orden de los factores difiere en una pequeña medida.

5.3 Enfóquese en algunos factores estresantes

A continuación, para sacar los porcentajes y el número de participantes de las preguntas, dividiremos las respuestas en dos bloques:

→ «No, en absoluto» y «Más bien no» serán contabilizados como un bloque genérico que da respuesta a un «no».

→ «Sí, absolutamente» y «Más bien sí» serán contabilizados como un bloque genérico que da respuesta a un «sí».

Un déficit de imagen

El **74%** de los encuestados, afirma que su trabajo «todavía» adolece de una **idea preconcebida bastante negativa** (P13). Por supuesto, hubiera sido interesante saber cuánto valía este indicador hace 5 años. Es probable que el porcentaje fuera significativamente mayor en ese momento. Por supuesto, la profesión es más conocida y entendida hoy en día, pero todavía queda un esfuerzo importante por hacer para comercializar esta función. Aún falta tiempo para convencerlo y promoverlo, y puede que no sea lo que mejor saben hacer los profesionales de la ciberseguridad. Además, un importante **75%** todavía se siente incomprendido, o incluso considerado **excesivo** en ocasiones (P14). Es importante trabajar la imagen, ya que un déficit de imagen en relación con el rol social es, sin duda, una fuente de estrés. Sin embargo, en los últimos años se ha producido un importante cambio de postura que debería mejorar gradualmente el reconocimiento y el coeficiente de comprensión e incluso simpatía dentro de la empresa. Sin embargo, es necesario continuar y acentuar los esfuerzos y, sobre todo, darse cuenta de la importancia de la comunicación en esta profesión.

Y fuera de la empresa, ¿qué dice un niño cuando se le pregunta qué hace su padre o madre cuando trabaja en ciberseguridad? Es difícil predecir si los niños pequeños querrán dedicarse a la ciberseguridad en el futuro, en lugar de querer ser bomberos, astronautas o médicos. Tal vez le falte el uniforme, la bata blanca y el estetoscopio al cuello, el traje para ir al espacio o el casco de bombero. Es difícil encontrar simbolismo material en una profesión que gira en torno a los datos y el ciberespacio, aunque el término "ciberseguridad", que tiene pocos años, es quizás una primera pequeña conquista para fortalecer la imagen de la profesión.

Adicionalmente, la ciberseguridad es un concepto o término que suele aparecer de forma reactiva en caso de sucesos, o en una fase muy tardía de los estudios de un profesional, **por lo que no se adquiere conciencia de su existencia hasta lograr un nivel de madurez alto**.

Comprender las habilidades requeridas

Las opiniones en términos de "hard skills" **destacan de manera muy positiva**. El **76%** de los encuestados consideran que tienen los conocimientos metodológicos y técnicos adecuados para adaptarse a las responsabilidades de su rol, lo cual refleja que se sienten preparados a nivel de aptitudes para enfrentarse a los nuevos problemas de la función (P16), y más de la mitad de ellos **(55%)** cree que tiene la capacidad de adaptarse al contexto altamente cambiante de la profesión (P17). Esto todavía significa que más de dos tercios del panel encuestado confían en sus competencias individuales y en su **capacidad de adaptación al entorno para hacer frente a los retos del mundo de la ciberseguridad.**

A pesar de que la profesión es reciente, España cuenta con un gran catálogo de formación en ciberseguridad. No hay más que ver la última actualización en enero de 2023, del "Catálogo de formaciones en ciberseguridad en España" propulsado por el Instituto de Ciberseguridad Español (INCIBE), donde aparecen reflejados:

→ La impartición de 87 programas de Máster, 4 especializaciones universitarias y 3 grados universitarios.

→ 62 especializaciones de Formación Profesional en ciberseguridad.

→ La existencia de 198 centros que imparten formación en ciberseguridad, reglada o no, repartidos por España.

Los CISOs demuestran haber encontrado un equilibrio que les permita adaptarse al medio y evolucionar con él, a la vez que el panorama va cambiando; así como una predisposición y proactividad por parte de la mayoría de los encuestados a nutrirse diariamente, y no dejar de aprender/adquirir conocimientos. **A pesar de no tener el control pleno de la situación debido a la profesionalización de los ciberataques de manera diaria y constante, los CISOs asumen ese riesgo de manera positiva.**

Experimentar la adversidad

El **74%** de los encuestados confirma que tiene que enfrentarse a enemigos que a menudo son invisibles (P19), lo que sin duda lo convierte en una verdadera singularidad de su trabajo. Fuera del sector de Defensa, son pocas las líneas de negocio que se encuentran en esta postura de lucha contra los enemigos de la compañía; ya sea que estos adversarios sean individuos u organizaciones criminales.

A pesar de que el **80%** de los encuestados no se siente personalmente inseguro (P23) o perturbado por rara vez poder identificar a la otra parte (P25), es innegable que los profesionales de la ciberseguridad se encuentran en una postura inherentemente defensiva.

El **42%** están más o menos desanimados por el aumento en la frecuencia y el poder de los ciberataques (P21) y el **48%**; se sienten frustrados por no poder defenderse (P20). Aunque

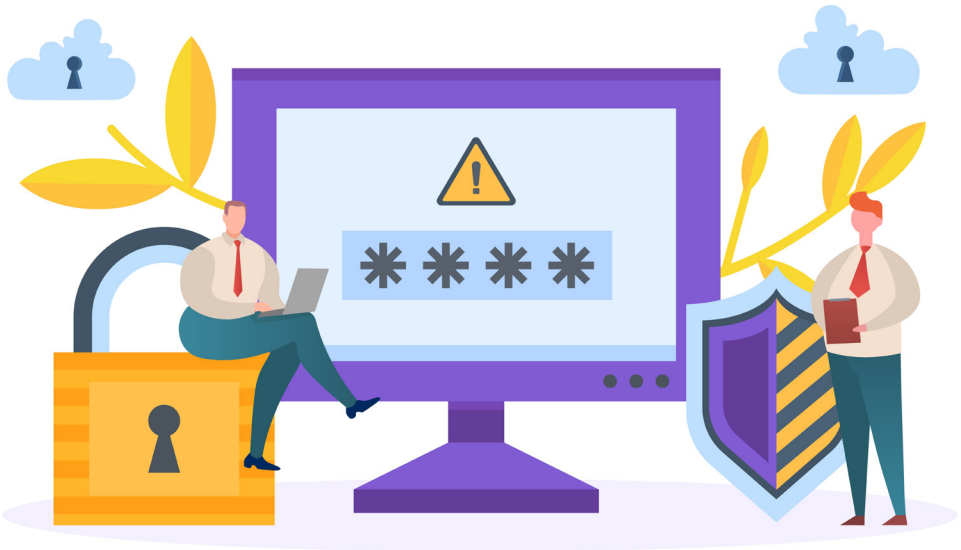
estos porcentajes son minoritarios, representan, en términos absolutos, a casi la mitad de los encuestados. Más del cincuenta por ciento de los participantes del cuestionario **(56%)** se sintió impotente ante la naturaleza asimétrica de la lucha (P22).

El contexto de adversidad es una fuente de estrés muy conocida, acentuada por la intensidad de la agresión potencial y la dificultad de afrontarla. Pero este contexto también puede crear empatía en la relación con los empleados de la empresa, lo que puede aliviar o suavizar la presión percibida. Esta presión puede transferirse invitando a estos empleados a contribuir a la defensa: "la seguridad es asunto de todos". Los trabajadores de la compañía confían en el equipo de ciberseguridad para que los defienda, y este equipo a su vez los invita a participar en esta actividad de defensa.

Desconexión e incertidumbre

La desconexión es una necesidad que se observa cada vez más en las empresas, en diversos sectores profesionales, derivando en la Ley Orgánica 3/2018 mediante el derecho a la desconexión digital. Se trata de trazar una línea entre los momentos profesionales y la vida personal. En realidad, los correos electrónicos nunca se detienen los viernes por la noche y la información más reciente es de fácil acceso, al alcance de la mano, en el teléfono inteligente que miras durante varias horas al día en esta obsesión generacional por asegurarse de no perderse nada. Algunos usan el mismo teléfono inteligente para intercambios comerciales y personales, lo que complica el proceso de clasificación. Los periodos de confinamiento y teletrabajo han difuminado aún más las líneas con respecto a esta frontera. En ciberseguridad, el trabajo requiere que estés constantemente atento a las señales, ya sea que expresen el inicio de un posible ataque, en casa, en la de tu proveedor, en la de tu competidor, o si son fallas cuya puntuación de peligrosidad es importante.

Ya sea porque las señales sean débiles o fuertes, ya sea porque el fuego se extinga rápidamente o no, existe una **sensación permanente de incertidumbre**: cualquier cosa puede suceder en cualquier momento y la gravedad de ello solo se medirá gradualmente. Pero hay que estar ahí, escuchando siempre. Ya sea que estés viendo un buen partido, cenando en casa de un amigo, en la ducha o en cualquier otra circunstacia, la incertidumbre está ahí. El **61%** de los encuestados se sienten alerta (P26), **incapaces de desconectar**. A pesar de que el **59%** de los encuestados puede disfrutar de este trabajo compuesto por peligros e imprevistos (P24), **algo menos de la mitad no se siente confortable**. La sensación de incertidumbre se cita entre las 5 principales causas de estrés. También lo expresan claramente todos los encuestados que consideran que su situación profesional está incluida en esta incertidumbre intrínseca a la profesión. Por lo tanto, no se trata simplemente de que le despierten en medio de la noche para hacer frente a un evento grave, sino de hacerlo considerando que este evento puede costarle su posición, si todos los astros no están correctamente alineados ese día. Así que no hay desconexión para las profesiones de ciberseguridad, abunda la incertidumbre, y todo desemboca en una vida de sorpresas y aventuras que puede acabar con una desconexión definitiva y forzada.



Inestabilidad de la función

Este tema del despido después de una crisis importante y, más en general, el de la inestabilidad del puesto, puede contribuir al nivel de estrés percibido por los CISOs. Sin embargo, los encuestados solo están parcialmente preocupados por el riesgo de perder su trabajo en caso de incidente: el **62%** cree que una crisis importante podría costarles su puesto.

Aun así, tenemos que tomarnos el tiempo para analizar esta cuestión. ¿Cómo se comporta una profesión en la que más de la mitad de sus miembros sienten que pueden "saltar" en caso de incidente? En un momento en el que los ataques van en aumento, pero también en el que los sectores afectados están cada vez más extendidos, esta mayoría puede **representar un riesgo**. Uno se pregunta si este miedo conducirá a comportamientos cuestionables, como ignorar ciertas vulnerabilidades o incidentes, o dedicar más energía a asignar responsabilidades en lugar de construir defensas sólidas. Estos elementos de análisis permanecen en el terreno de la hipótesis debido a la falta de cifras, pero deben ser considerados.

Entonces, ¿cómo podemos mejorar esta situación y evitar posibles desviaciones? La clave está en la percepción de ser el fusible de una cibercrisis. De hecho, **aunque el sector contrate mucho y se enfrente a una escasez de recursos, la pérdida del empleo representa una dificultad, cuyo nivel de gravedad será juzgado por cada persona en función de su situación personal.**

Sin embargo, ¿agradecerá cada una de las organizaciones afectadas a su CISO su trabajo realizado en caso de crisis? ¿Ha sido este el caso de las víctimas recientes de ataques de alto perfil? El tema del reconocimiento, la confianza en la propia posición y en la gestión, probablemente pueda explicar esta distorsión y representa una interesante línea de trabajo para reducir este riesgo, especialmente entre la población más expuesta al estrés.

Además, hay una categoría de profesionales que reproducen una técnica bien conocida de gestión de riesgos: ¡la aceptación! Algunos CISOs han dicho que son conscientes de esto y viven con ello: **en caso de una crisis importante, mi responsable puede decidir prescindir de mis servicios**. Esta es una de las posibilidades que existe en respuesta a una crisis. Y para esta categoría, no parece ser un factor estresante.

Percepción del riesgo de ciberseguridad

La gestión del riesgo de ciberseguridad es un ejercicio difícil para el **89%** de los encuestados. Una amplísima mayoría. Este riesgo está evolucionando mucho, necesita ser reevaluado con frecuencia, y las estrategias que abordan estos riesgos pueden dar giros rápidos y muchos cambios en las prioridades.

Ahora se acepta que el **impacto de un ciberataque puede ser considerable para la empresa y que la probabilidad de ocurrencia ya no es baja**. Sin embargo, mientras la madurez de la empresa avanza en materia de ciberseguridad, la información y los sistemas a proteger son cada vez más difusos. El ejercicio de concentración es arduo, sobre todo porque a menudo es necesario replantearse el tema para tener en cuenta la naturaleza cambiante de este riesgo.

Gestión de crisis

La gestión de crisis de ciberseguridad es un **ejercicio relativamente reciente**. A pesar de que en la actualidad existe una literatura abundante y un cierto número de cursos de formación en este campo, hay pocas referencias sobre el tema, pocos ejemplos de escenarios para construir modelos de respuesta. Varias historias se mantienen confidenciales, lo que dificulta el modelado.

Sin embargo, parece que la presión relacionada con la gestión de cibercrisis es sufrida por el **74%** de los encuestados (P29). Se trata de una puntuación que demuestra una de las caras más importantes y que más malestar generan en el día a día de la función del CISO, que es la gestión de estos ciberincidentes.

Esta administración se lleva a cabo en buenas condiciones personales, ya que el **69%** de los encuestados afirma contar con el apoyo de sus seres queridos (P31).

Por último, la ausencia de referencias sobre la gestión de crisis de ciberseguridad es quizás una ventaja, ya que permite evitar anclar sesgos en una práctica o escenarios que han funcionado bien en el pasado.

INSSB y riesgos psicosociales

1. Tiempo de trabajo.
2. Autonomía.
3. Carga de trabajo cuantitativa y cualitativa.
4. Demandas psicológicas.
5. Variedad/contenido.
6. Participación/Supervisión.
7. Interés por el trabajador.
8. Desempeño del rol.
9. Relaciones y apoyo social.
10. Conciliación laboral-familiar.
11. Equipos de trabajo.

El Instituto Nacional de Seguridad, Salud, y Bienestar (INSSB) en el trabajo emitió una lista de factores de riesgo psicosocial, que se pueden agrupar en las siguientes áreas:

1. Respecto al dominio de **Coacción y vigilancia**, pueden ligarse los riesgos: Carga de trabajo cuantitativa y cualitativa, Interés por el trabajador y Participación/Supervisión.

2. Respecto al dominio de **Complejidad y escalabilidad**, pueden ligarse los riesgos de: Desempeño del rol y autonomía.

3. Respecto al dominio de **Transversalidad**, pueden ligarse los riesgos de: Desempeño del rol, Variedad/contenido y Demandas psicológicas.

4. Respecto al dominio de **Combate y adversidad**, pueden ligarse los riesgos de: Demandas psicológicas, Equipos de trabajo y Participación/Supervisión.

5. Respecto al dominio de **La incertidumbre y lo desconocido**, pueden ligarse los riesgos de: Demandas psicológicas y Participación/Supervisión.

6. Respecto al dominio de **Gestión de crisis**, pueden ligarse los riesgos de: Equipos de trabajo y Demandas psicológicas.

7. Respecto al dominio de **Comunicación y convicción**, puede ligarse el riesgo de: Participación/Supervisión.

8. Respecto al dominio de **Responsabilidad y culpa**, pueden ligarse los riesgos de: Conciliación laboral-familiar, Relaciones y apoyo social y Tiempo de trabajo.

5.4 Comparativa resultados Francia y España

Este estudio, pionero en España, ya había pasado primero por los CISOs franceses. El equipo de Advens en Francia fue el primero en lanzar esta iniciativa en 2021, hace exactamente dos años. Por lo tanto, en este apartado procedemos a realizar una comparativa de los resultados entre ambos países y determinar la situación de estrés en la que se encuentran de media los CISOs franceses y españoles.

Resultados de las preguntas PSS10 de España:

Número de Pregunta		Preguntas PSS10:	Media de respues-tas
Q3	1	En el último mes, ¿se ha sentido molesto o irritado por acontecimientos inesperados?	2,46
Q4	2	En el último mes, ¿se ha sentido incapaz de controlar lo "básico" de su trabajo?	2.13
Q5	3	En el último mes, ¿se ha sentido nervioso o estresado?	2,70
Q6	4	En el último mes, ¿se ha sentido plenamente capaz de gestionar sus problemas profesionales?	1,40
Q7	5	En el último mes, ¿ha sentido que las cosas iban como usted quería?	1,85
Q8	6	En el último mes, ¿ha sentido que no podía hacer frente a todas las cosas que tenía que hacer?	2.56
Q9	7	En el último mes, ¿ha sido capaz de controlar (interna y externamente) su irritación?	1.02
Q10	8	En el último mes, ¿se ha sentido en control de la situación?	1,45
Q11	9	En el último mes, ¿se ha sentido irritado porque los acontecimientos escapaban a su control?	2.00
Q12	10	En el último mes, ¿ha notado que las dificultades se acumulaban hasta tal punto que ya no podía controlarlas?	1,76
		Total	19,34

En este caso la media de las 10 primeras preguntas que analizan el estrés percibido que tiene cada uno desemboca en la cifra: **19,34**.

Resultados de las preguntas PSS10 de Francia:

Número de Pregunta		Preguntas PSS10:	Media de respues-tas
Q3	1	En el último mes, ¿se ha sentido molesto o irritado por acontecimientos inesperados?	2,63
Q4	2	En el último mes, ¿se ha sentido incapaz de controlar lo "básico" de su trabajo?	2,12
Q5	3	En el último mes, ¿se ha sentido nervioso o estresado?	2,58
Q6	4	En el último mes, ¿se ha sentido plenamente capaz de gestionar sus problemas profesionales?	1,04
Q7	5	En el último mes, ¿ha sentido que las cosas iban como usted quería?	1.47
Q8	6	En el último mes, ¿ha sentido que no podía hacer frente a todas las cosas que tenía que hacer?	2.53
Q9	7	En el último mes, ¿ha sido capaz de controlar (interna y externamente) su irritación?	0,93
Q10	8	En el último mes, ¿se ha sentido en control de la situación?	1.4
Q11	9	En el último mes, ¿se ha sentido irritado porque los acontecimientos escapaban a su control?	1,99
Q12	10	En el último mes, ¿ha notado que las dificultades se acumulaban hasta tal punto que ya no podía controlarlas?	1,72
		Total	18,41

En este caso la media de las 10 primeras preguntas que analizan el estrés percibido que tiene cada uno desemboca en la cifra: **18,41**.

En comparativa, se puede apreciar que hay **una diferencia poco significativa de exactamente 0,93 puntos**. Únicamente, ambos resultados se encuentran en la zona de vigilancia (naranja) que esclarece unos niveles de estrés suficientes como para tenerlos en consideración. Es decir, refleja una serie de emociones y sentimientos de importancia que aparecen de manera ocasional y que conducen a alteraciones y cambios de humor de nuestras emociones, dando lugar a situaciones que pueden convertirse en circunstancias difíciles de manejar.

Si analizamos los resultados de ambos países por zonas, se obtiene que:

→ En la zona verde, Francia cuenta con un % más alto de encuestados que se encuentra en un área de estrés controlado, es decir, el estrés se mide con una connotación estimulante o positiva. En España contamos con un % menor.

→ La zona naranja apenas presenta variaciones, teniendo ambos países un rango de porcentajes similar en cuanto al número de personas que se encuentran con sentimientos ocasionales de impotencia que derivan en situaciones difícil de manejar. Esta es la zona en la que se encuentra la media final de ambos países.

→ Por último, la zona roja, donde entran factores tales como fuertes sentimientos de impotencia, sensación de amenaza más o menos difusa, riesgos para la salud física y mental, etc., registra un porcentaje mayor en España, donde la diferencia se encuentra en un 11% más que los resultados de Francia.

6

Concienciación: Reacciones a los resultados

6.1 Perspectiva del Experto

Benjamin Leroux, Director de Marketing de Advens.

Es muy importante para nosotros estudiar el tema del estrés de los responsables de ciberseguridad. Este estudio inició en Francia y quisimos extenderlo a otros países en los que pudiésemos apoyar a las empresas en sus esfuerzos sobre materia de ciberseguridad. Este estudio muestra que el problema es especialmente importante también en España.

Si nos fijamos en la medición del estrés percibido, nos damos cuenta de que más de dos tercios de los CISO se encuentran en una situación difícil. Esto representa un riesgo nuevo que quizás no se había identificado hasta ahora. En primer lugar, es un riesgo para las mujeres y los hombres afectados por este estrés. Ahora sabemos que las consecuencias de un exceso de estrés y una mala gestión pueden ser muy graves: bajo la posibilidad de llegar hasta el agotamiento. Estudiar el tema del estrés debe permitir evitar riesgos para las personas, actuando como un enfoque preventivo.

Más allá de los problemas de las personas, estos resultados muestran una problemática global para España (que también se había observado en Francia) ¿Podemos sentirnos seguros si una gran mayoría de CISOs se encuentran en una situación de riesgo personal? ¿Qué pasaría en caso de un ataque sistémico? Estas situaciones personales pueden desembocar en una grave situación colectiva.

Si intentamos entender el origen de este estrés, nos damos cuenta de que es una de las características del trabajo de un CISO. De hecho, el CISO es uno de los pocos trabajos en una organización que se enfrenta a una amenaza permanente e invisible y, a veces, a recursos desproporcionados. Sin embargo, estos son factores externos que no se pueden cambiar. Por lo tanto, es necesario aceptar esta situación y trabajar en la resiliencia y las habilidades humanas de los profesionales de la ciberseguridad.

Con demasiada frecuencia, estas profesiones se han asociado con trabajos puramente informáticos o técnicos. No obstante, por encima de todo, no dejan de ser trabajos humanos. Por lo tanto, es necesario tomarse el tiempo para reconocer las particularidades que esto genera en términos de habilidades, conocimientos, pero sobre todo en competencias interpersonales.

Esperamos contribuir al reconocimiento de las especificidades de estas profesiones. Esto conducirá a programas de apoyo para les profesionales que les ayuden a hacer frente a estos estresores y así hacerlos más eficientes. Al final, esto tendrá un impacto en toda la sociedad.

6.2 La visión del CISO

Gonzalo Asensio, CISO de Bankinter.

ISMS Forum & ADVENS

Quiero agradecer que en España se empiece a estudiar, analizar y comunicar este tipo de estudios; este en concreto llamado "Factores críticos en la generación del estrés de los CISOs y cómo evitarlos" proporciona bajo mi punto de vista un resumen ejecutivo y detallado realizado por ISMS Forum y Advens sobre el estrés experimentado por los responsables de seguridad de la información (CISOs) en España.

Es importante destacar el motivador del mismo:

"El estudio se llevó a cabo debido al aumento de los ataques cibernéticos y su impacto en la percepción del estrés en los profesionales de ciberseguridad".

Quiero añadir esta frase de un autor desconocido:

"El trabajo apasionado es aquel que combina la dedicación y el entusiasmo con el cuidado de nuestra salud, pues solo así podemos alcanzar el éxito sostenible y disfrutar de una vida plena."

- Autor desconocido.

Los resultados revelaron que el nivel de estrés promedio entre los encuestados era alto, con un resultado de 19,34 en una escala de estrés que va de 0 a 40. El 70% de los encuestados experimentaba estrés con efectos negativos, y un 39% se encontraba en la "zona roja" con mayores riesgos para la salud física y mental.

Sin duda son datos que no me sorprenden pero que me resultan preocupantes debido a que siempre he defendido la idea del CISO 360, en el que cuanto mejor persona, más desarrollo personal inviertes y mejor podrás desarrollar tu difícil labor, que a su vez está llena de pasión y en muchos casos, de altruismo comunitario.

Los factores que más contribuyeron al estrés de los CISOs incluyeron el contexto de adversidad, la dificultad para desconectar y descansar, la responsabilidad y la culpa, y la sensación de incertidumbre y desconocimiento en el día a día. Además, la preocupación por perder el empleo también generó estrés en la mayoría de los encuestados; en este sentido siempre explico mi trabajo de esta forma:

"Mi trabajo es algo "puñetero" o complejo…. Cuando no pasa nada es difícil de justificar y cuando pasa normalmente lo pierdes".

Además, quiero destacar la importancia de abordar los factores estresantes identificados y promover soluciones, tanto a nivel individual como a través de comunidades y en la trayectoria profesional.

Sin duda hay necesidad de abordar el estrés y promover medidas para mitigarlo y proteger la salud mental de todos los profesionales de la ciberseguridad.

Establecer límites y un equilibrio entre el trabajo y la vida personal es fundamental. Los CISOs tenemos que asegurarnos de dedicar tiempo a actividades que nos proporcionen alegría y relajación fuera del entorno laboral.

En este sentido aquí dejo lo que a mí me ha costado años descubrir para encontrar un equilibrio, lo trabajo diariamente y casi seguro que seguiré haciéndolo mientras tenga este trabajo. Es importante hacer hincapié en el hecho de que no soy médico, por lo que si te encuentras bajo una situación desbordante siempre se recomienda acudir a profesionales cualificados.

Por ejemplo, en mi caso os comento algunas de las cosas que me ayudan, como siempre cada cual tiene que encontrar que es lo que le da paz, tranquilidad, felicidad, energía, descanso y concentración:

Paseo montaña: a mí me ayuda mucho parar el ruido exterior, oler el campo y sentirme como en el origen de todo, siempre que tengo un problema en modo bloqueo me voy a dar un paseo y luego reflexiono sobre el mismo de otra forma.

Lectura interesante: es importante leer cosas que no siempre sean nuestro foco, nuestro trabajo… en mi caso me gusta leer sobre desarrollo personal, neurociencia, filosofía, etc.

Baño con sal: El calor del agua y la sal ayudan a la relajación muscular y ese tiempo de calidad te sirve para suavizar la tensión.

Animales: me ayudan a tener una responsabilidad diferente, a ver en corto y medio plazo, me aportan calidez y satisfacción.

Natación: no sólo por la espalda o por las miles de horas que estamos sentados, sino por la desconexión mental y la rebaja de pensamientos simultáneos.

Ayuda a otros (ong, voluntariado): ofrecer tus conocimientos y experiencia en otros es maravilloso y me hace sentir más realizado.

Viajar: sin duda uno de los grandes aliados y retos ya que siempre debemos estar conectados en nuestro trabajo; si podemos organizar viajes con una buena delegación y aviso podremos desconectar.

Cuidar la alimentación: parece una tontería… pero cuando estas estresado comes mal, te llama el dulce, comes por la noche y tienes cierto desorden… no soy partidario de ninguna dieta, sólo soy partidario de escuchar tu cuerpo y poner cierto orden.

Meditar: se dice que debemos de respirar profundamente 10 veces cada hora/dos… yo lo intento, pero el hábito continuo es complicado con nuestro entorno, aún así aprovecho el coche y momentos más apropiados para poder meditar y sólo respirar y sentir el aire (esto me ayuda a la toma de decisiones).

Yobility (Yoga Coaching): Sin duda es lo que mejor me va porque mezcla funcional, estiramiento, movilidad y coaching.

Dormir: importante no ver nada audiovisual que pueda interrumpir o alterar el sueño.

6.3 La perspectiva de Advens

José Luis Díaz, CEO Advens Iberia.

Uno de los temas que siempre me han llamado la atención es conocer de primera mano cómo influye la continua presión por sufrir un ciberataque en el desempeño cotidiano de los CISOs. Visto desde el otro lado, es de suponer que la presión debe ser enorme, con los medios publicando a diario los continuos ciberataques y las consecuencias sufridas por las empresas.

Una vez lanzado el estudio en Francia y viendo la repercusión que ha tenido para la población de CISOs, se planteó en España repetir el estudio entre nuestros responsables de ciberseguridad, pero nos hacía falta un compañero de viaje para la realización del estudio, alguien en contacto continuo con los CISOs, que los conozca bien y que sea capaz de plasmar este conocimiento diferencial.

Cuando propuse este tema de estudio al ISMS Forum, no sabía muy bien a dónde nos llevaría todo. Nuestra intención era aportar un estudio novedoso a los CISOs, un punto de partida para conocer si hay un problema e intentar establecer las bases para ponerle solución. La respuesta por parte de ISMS forum fue muy positiva, recurrir a esta comunidad permitiría contar con un gran número de CISOs, y así disponer de cifras y estadísticas creíbles y realistas. El objetivo principal era hacerse una idea de la situación. La cuestión del estrés de una población expuesta a incidentes y crisis puede parecer retórica. ¿Quién no estaría estresado ante esta amenaza cibernética que decimos todos los días y que cree que no tiene límites? Aun así, pensamos que sería una buena idea profundizar y tratar de averiguar más.

El proceso de estudio fue particularmente importante. Además del uso de una encuesta internacionalmente reconocida (Perceived Stress Scale 10 – Cohen 1983), con la esperanza de llegar al mayor número posible de CISOs, también era necesario tener una visión neutral, e idealmente experta, de estos temas de estrés y salud mental. Nuestra experiencia conjunta ISMS Forum y Advens no cubre específicamente estos temas. Por lo tanto, es necesario proceder con cautela o dejarse guiar por especialistas, lo que es posible gracias a los colaboradores externos que contribuyen.

Todos estos factores nos han permitido medir el nivel de estrés que sienten nuestros CISOS y buscar las causas relacionadas con la naturaleza del trabajo diario. Como resultado, el nivel medio es preocupante (19,34 puntos), con algunos grupos dentro de límites alarmantes (10 personas dentro del grupo de agotamiento y otras 10; dentro del umbral de depresión).

El estudio de los factores generadores de estrés resultó igual de interesante para dar paso al siguiente debate: **la búsqueda de soluciones para controlar o incluso reducir este estrés**. También en este caso, el método que se ha seguido puede ser cuestionado. El estrés puede provenir de una situación personal, que sabemos que la pandemia ha hecho más compleja aún o bien puede estar relacionado con el entorno del empleador, la capa directiva o las relaciones interpersonales en el trabajo. Todos estos factores son importantes, pero están más allá del alcance de este estudio y habría sido complejo adentrarse más allá.

Por lo tanto, parece que varios componentes del trabajo del CISO producen estrés. Si excluimos factores externos, que son difíciles de influir (como la aleatoriedad de un ataque o la adversidad de la lucha contra la amenaza), todavía hay muchos factores como la responsabilidad, la dificultad para desconectar, el miedo a actuar o la complejidad de la función de CISO en sí misma.

Ahora es necesario tomarse el tiempo necesario para analizar estas conclusiones iniciales con el fin de definir las acciones más relevantes. Es fácil identificar un conjunto de acciones destinadas a que la gente hable sobre el tema, a que se atreva a abordarlo. Y muy rápidamente pensaremos en acciones para reducir el nivel de estrés, en particular explicando aún mejor el trabajo, sus particularidades y sus dependencias con los otros trabajos de la empresa.

Este enfoque pedagógico debería permitir un mejor reconocimiento del papel del CISO y, en el proceso, debería contribuir a una mejor comprensión del riesgo de ciberseguridad. Ya podemos ver un primer resultado de "ganar, ganar". Por un lado, el CISO mejora su reconocimiento y comprensión de sus acciones, y podrá beneficiarse del apoyo de otros actores de la empresa. Por otro lado, los empleados están mejor equipados para comprender la amenaza y reducir potencialmente el comportamiento de riesgo.

Este primer ejemplo ilustra plenamente la ambición de la próxima etapa de nuestro trabajo. Identificar las áreas que permiten, por un lado, reducir el nivel de estrés o contenerlo en un estado de estrés positivo y estimulante y, por otro lado, reforzar la eficacia de los sistemas de ciberseguridad, en particular a través de una mejor integración en las líneas de negocio de la empresa y un enfoque más positivo y preventivo.

6.4 La perspectiva de ISMS Forum

Daniel García, Director General y Beatríz García, Subdirectora de las áreas de Formación, Certificación y Proyectos.

ISMS Forum, comprometida con el avance del conocimiento en seguridad de la información, ha encontrado en la colaboración con Advens una oportunidad única para explorar el terreno psicolaboral de los profesionales de ciberseguridad en España. Con una sólida trayectoria en la creación de guías, estudios e infografías que amplían la comprensión y evalúan la madurez

de las empresas en este ámbito, ISMS Forum abraza la iniciativa de entender y abordar el estrés en el puesto de Responsable de Seguridad de la Información (CISO).

Vivimos en una era digital donde la ciberseguridad se ha convertido en una columna vertebral de la estabilidad empresarial y la protección de datos sensibles. Mientras la tecnología avanza a pasos agigantados, los responsables de ciberseguridad se enfrentan a desafíos que van más allá de la pura técnica y lo corporativo.

En este contexto, surge la necesidad de abordar la salud mental y emocional de los profesionales de ciberseguridad. La rapidez con la que evolucionan las amenazas cibernéticas y la creciente sofisticación de los ataques hacen que los responsables de ciberseguridad estén sometidos a una presión constante.

Este estudio pionero busca arrojar luz sobre los factores psicológicos y emocionales que afectan a estos expertos, reconociendo que su bienestar es esencial para la resiliencia y eficacia en la protección de la ciberseguridad. En un momento en el que la ciberseguridad está más en el foco que nunca, es crucial comprender que el cuidado de la salud mental de estos profesionales no es solo una consideración humana esencial, sino también un paso estratégico hacia un panorama de ciberseguridad más sólido y resiliente.

7

©kittyvector

Profundizando y observando

La encuesta ha abierto un campo de preguntas sobre la carga mental de las profesiones relacionadas con la ciberseguridad. Sin embargo, una sola encuesta no es suficiente para llevar a cabo acciones a largo plazo para prevenir y tratar los riesgos psicosociales de esta profesión.

Es importante profundizar en ciertos temas, confirmar las hipótesis planteadas durante esta encuesta y, sobre todo, medir la evolución de este estrés a lo largo del tiempo. Al comprender el origen del estrés y la evolución de la situación de los CISOs, deberíamos ser capaces de apoyar mejor esta evolución y tratar de brindar una ayuda concreta a los profesionales.

Por lo tanto, se propone establecer una observación anual del estrés, mediante el seguimiento de algunos indicadores clave a lo largo del tiempo, y completar la encuesta actual profundizando en ciertos temas.

Para ello, se plantea organizar algunos debates en el seno de la comunidad de ISMS Forum, con el fin de construir conjuntamente estos indicadores y este enfoque en profundidad.

8

©kittyvector

De las palabras a la acción: primeras ideas sobre las soluciones

8.1 ¿Qué debe hacer?

El objetivo del estudio no fue trabajar en soluciones para el manejo del estrés, como se presentó anteriormente. Su objetivo era formar una convicción sobre el problema y sus orígenes. Los resultados son indiscutibles: La mayoría de los profesionales de la ciberseguridad se enfrentan al estrés con efectos negativos, y ciertas características intrínsecas a su trabajo y al contexto en el que se lleva a cabo contribuyen a este nivel de estrés potencialmente peligroso.

Una vez establecida esta observación, y demostrada por las cifras, no podemos echar la vista a un lado. Por una parte, porque no está en los hábitos de los iniciadores del estudio, ni de los especialistas que contribuyeron al mismo; y por la otra, porque la situación es peligrosa: ¿Cómo se puede proteger adecuadamente a una empresa y su entorno digital si usted mismo no se siente protegido? ¿Se puede potenciar la profesión trabajando sobre el estrés y sus causas? ¿Cómo podemos ayudarnos a nosotros mismos, a la comunidad y a la sociedad?

Ya no es necesario demostrar la importancia de la ciberseguridad. La importancia de "asegurar" a las mujeres y hombres que lo orquestan día tras día debe ser a su vez indiscutible. Dicho esto, ¿qué se puede hacer para trabajar en este tema, que es nuevo para los expertos en ciberseguridad, pero cada vez más entendido por los especialistas en salud mental y, por extensión, por los recursos humanos, la gestión, etc.?

Con la ayuda de las partes interesadas externas, y a lo largo de las diversas perspectivas, ya están surgiendo algunas soluciones. A continuación, se analizan, dependiendo de si se centran en las prácticas de los profesionales en cuestión; o si se centran en los ecosistemas organizativos, académicos o, incluso, sociales.

El objetivo de estas propuestas es abordar las consecuencias o causas del estrés mediante la identificación de acciones que puedan reducirlo.

8.2 Dentro de las comunidades

Dentro de las comunidades profesionales, con el ejemplo de lo que está haciendo una asociación como ISMS Forum, pueden surgir varias soluciones de las prácticas utilizadas para hacer frente al estrés en el lugar de trabajo, a escala global o a nivel de ciertas profesiones o perfiles de profesiones, como por ejemplo, los CISOs.

El objetivo de estas acciones es doble: El primer componente tiene como objetivo continuar con la concientización y el reconocimiento del problema, mientras que el segundo plantea trabajar en prácticas para reducir el estrés. En esta etapa de las reflexiones, se proponen cuatro vías que serán trabajadas por Advens e ISMS Forum.

ISMS Forum & ADVENS

Idea 1: Seminarios web sobre resiliencia al estrés

El uso de seminarios web se ha utilizado ampliamente en los últimos meses, especialmente durante los confinamientos. Ahora es dominado por todos y se puede utilizar para este tema aún nuevo.

Se trata, por tanto, de utilizar este formato de forma regular para ofrecer un espacio de intercambio y trabajo colectivo, y así estimular una amplia dinámica común dentro de la profesión. El tema general podría ser el "Cuidado", donde **su objetivo es designar bajo una palabra clave los diferentes métodos, dispositivos y respuestas que se pueden proporcionar a situaciones de vulnerabilidad personal de los CISOs**.

El contenido de este seminario web se basa en particular en la contribución de la teoría y el conocimiento, el intercambio de casos prácticos y la retroalimentación. Al igual que en este estudio, la intervención de especialistas será beneficiosa para asegurar su calidad y efectividad.

Por ejemplo, se deben considerar los siguientes temas:

→ Cambiar la postura frente al estrés (neurociencia) en el contexto de una ciberamenaza.

→ Encontrar el nivel adecuado de tensión (liderazgo adaptativo) para el nivel de madurez de la ciberseguridad de su organización.

→ Lidiar con «demasiado».

→ Etc.

Idea 2: Talleres en profundidad

El objetivo de los talleres en profundidad es trabajar en grupos más pequeños (de 8 a 10 participantes), a lo largo del tiempo y, por ejemplo, en una dinámica interempresarial. Cada grupo tiene una duración de seis meses. Durante este período, los participantes se apoyan mutuamente en la adquisición de habilidades (cognitivas, emocionales y conductuales). El objetivo de cada persona es fortalecer su postura individual frente al estrés y ganar agilidad emocional.

Existe una brecha entre la evolución de la ciencia cognitiva y del comportamiento en las últimas dos décadas y su aplicación en el mundo real por parte de la mayoría de nosotros. Este tipo de talleres puede aportar soluciones muy concretas para los participantes, sobre temas que a menudo se descuidan o incluso se desconocen.

Así es como todos podrán crecer y fortalecerse frente al estrés. **De hecho, la inteligencia colectiva utilizada para fortalecer a los individuos ya ha demostrado ampliamente su eficacia.**

Idea 3: Seminarios presenciales

Se trataría de organizar una jornada de conferencias e intercambios sobre el tema del estrés en las profesiones de Ciberseguridad. Su objetivo sería sensibilizar a la profesión.

También podría abrirse a otros actores, como los superiores jerárquicos de los CISOs (CIO, CFO, Secretarios Generales, CEO, etc.), con el fin de **sensibilizar e integrar a estas profesiones en el pensamiento y el trabajo sobre la gestión del estrés.**

Idea 4: Retratos y experiencias de CISOs

ISMS Forum & ADVENS

El objetivo es elaborar retratos de los miembros de ISMS Forum. Hoy en día, la ciberseguridad se describe a través de un conjunto de actividades y prácticas. Se trata de completar esta visión de la profesión acercando las experiencias de las personas que la ejercen a diario, en toda su complejidad y sutileza. De este modo, se propondrá a los miembros de ISMS Forum que lo deseen transmitir lo que es esta profesión y lo que representa para ellos, en sus ambiciones, en sus dudas y en sus pruebas. Estos retratos individuales, además de la encuesta estadística general, sin duda arrojarán luz sobre los pequeños datos, los cuales pueden resultar interesantes para médicos e investigadores, con el fin de identificar situaciones y escenarios atípicos e interesantes que los promedios probablemente pasarán por alto. Por supuesto, no solo se centrarán en el estrés, sino en el hecho de que esta dimensión estará inevitablemente presente.

8.3 En la trayectoria profesional

Más allá de los círculos profesionales de los CISOs, el campo de posibilidades es mucho más amplio. El tema de la **gestión del estrés ha sido muy abordado** por otras profesiones, utilizando numerosos dispositivos y herramientas ¡Las pistas propuestas en esta etapa son solo puntuales y no garantizan ninguna integridad! Su objetivo es abrir las reflexiones para la máxima creatividad, pero también para la eficiencia en las soluciones, en la reacción y también en la prevención.

Idea 1: De la descripción del puesto

Hoy en día, las descripciones de los puestos de trabajo no tienen en cuenta el tema del estrés. Podría haber una serie de elementos en las descripciones de los diferentes cargos que aborden las causas del estrés tal y como surgieron en la encuesta. La comunidad de ISMS Forum podría trabajar en ejemplos de descripciones de puestos, que tengan en cuenta las lecciones aprendidas de la encuesta, ya sea para informar y hacer que se reconozca el requerimiento de la profesión en términos de carga mental, o para integrar estos elementos en la descripción de las actividades. Por ejemplo, parece útil recordar, en la descripción del puesto, la naturaleza conexa del mismo al hecho de que este puesto conduce a la realización de acciones útiles, a veces restrictivas, y que no evitarán todos los escenarios, sino que limitarán los riesgos. También es necesario recordar **la naturaleza evolutiva que requiere una adaptación constante e integrar el seguimiento y el ajuste a los cambios como una actividad en sí misma del negocio y no como un elemento a soportar.**

Idea 2: Integración en el curso de formación

Lo primero que hay que hacer puede parecer obvio: **es confiar en el responsable** y en su departamento de RRHH para ayudar al CISO a fortalecer sus habilidades en términos de resiliencia a los factores estresantes. En la actualidad, muchos catálogos de formación corporativa incluyen estas cuestiones.

Esto se puede lograr de forma sencilla integrando al CISO en el itinerario formativo adecuado. Dada la naturaleza a veces "estandarizada" de estos elementos, esto puede implicar una evolución del estatus del CISO, para acercarlo a una población desde el punto de vista de la Gestión de Personas más cercana a las profesiones de gestión, la toma de decisiones y el impacto general a nivel estructural.

Podemos imaginar que, para los CISOs, **la transición a la condición de alto directivo puede ir acompañada en determinadas estructuras de esta oferta de formación centrada en el estrés, el desarrollo personal y el liderazgo.**

Para las estructuras menos maduras, es una oportunidad para que los responsables de la formación se doten de contenidos y competencias adaptadas a esta cuestión, que van más allá del estricto marco de la ciberseguridad.

Idea 3: Reconocimiento y apoyo en la empresa

La segunda vía se refiere al reconocimiento y apoyo de los profesionales de la ciberseguridad por parte de sus colegas y de otros profesionales dentro de su organización. Este enfoque se deriva de los mecanismos puestos en marcha en el mundo de la salud.

Si bien el objetivo es fácil de expresar, los mecanismos para lograrlo son más complejos. Pueden **cambiar drásticamente dependiendo de la organización, su cultura y sus modalidades internas**. El objetivo es explicar y promover el trabajo de los equipos de ciberseguridad para que se reconozcan sus particularidades y sus aportaciones a la organización.

Esto se puede hacer a través de acciones internas de "marketing", promoción y comunicación, pero también, más simplemente, a través de momentos de diálogo entre el CISO y sus homólogos dentro de otros cargos de la organización.

Idea 4: Divulgación orientada a la acción

La tercera vía se relaciona con la anterior en su finalidad: **el reconocimiento y el apoyo**. El objetivo es garantizar que el mayor número posible de empleados de la organización conozcan las particularidades y dificultades del rol del CISO. Se trata, por tanto, **de desarrollar la empatía hacia el equipo de seguridad.**

Esto puede tener un doble nivel de impacto. En primer lugar, porque la organización generalmente se dará cuenta del estrés potencial de su CISO y debe tener un movimiento natural de apoyo y reconocimiento. En segundo lugar, porque aumentará el nivel general de concienciación sobre ciberseguridad, a través de una mejor comprensión de sus problemas, y por lo tanto fortalecerá el nivel de protección de la organización.

Esto nos lleva de nuevo a los objetivos de la concienciación de los empleados. Sin embargo, para alcanzar ambos retos, es necesario concienciar sobre los riesgos, por supuesto; pero también y sobre todo sobre las posturas, mecanismos y acciones que hay que poner en marcha para controlar estos riesgos. Esta concienciación "orientada a la acción" debe implicar a las personas a las que se dirige para ponerlas en el lugar de los profesionales de la ciberseguridad mientras dure una acción de sensibilización. Pero también, y, sobre todo, dotarlos de los medios para actuar con el fin de hacer frente de forma sostenible y eficaz a las amenazas dirigidas a los seres humanos. Podemos imaginar acciones en forma de inmersión en el día a día de los equipos de seguridad operativa o juegos de rol, por ejemplo. La difusión de contenidos educativos accesibles a todos, que expliquen los mecanismos de ataque y defensa, también puede ser beneficiosa.

Podemos esperar entonces un **círculo virtuoso**: el refuerzo de la defensa por parte de los empleados reducirá el nivel de riesgo y el número de crisis y, por lo tanto, debería permitir un mejor equilibrio de la carga mental de los equipos de ciberseguridad.

9

Conclusión:
lo humano, una y otra vez

Este estudio se inició sobre la base de una pregunta simple: ¿ Los responsables de ciberseguridad en España, están sujetos a un nivel de estrés particularmente alto? El cuestionario cumplimentado por 82 profesionales dio respuesta. El análisis de estos resultados, con la ayuda de especialistas, permitió comprender el nivel de gravedad de la situación, pero también identificar algunas de las causas de este estrés en los propios componentes del trabajo.

Sí, los CISO están bajo estrés. El 69% de todos los CISOs encuestados sienten estrés; y el 32% del total de los encuestados se sitúan en una zona de riesgo.

Sí, el trabajo contribuye a este estrés. Es una profesión marcada por la adversidad, caracterizada por una situación de lucha incesante contra un enemigo que muchas veces es virtual e invisible, con recursos a veces mayores que los de la defensa, o al menos beneficiándose del elemento sorpresa o asimetría que hace que baste con que el atacante encuentre una sola puerta abierta. Es un trabajo exigente en el sentido estricto de la palabra, porque está sujeto a pruebas. Es frágil porque el reconocimiento no está sistemáticamente alineado con la importancia de los temas de ciberseguridad para que la organización esté protegida.

Por lo tanto, debemos utilizar los resultados de este trabajo para mejorar la situación, para mejorar la vida cotidiana de quienes protegen la vida digital de las empresas todos los días. Es una obligación para cada uno de estos profesionales vivir mejor su profesión y prosperar. Más allá del desarrollo personal, también es la clave del éxito profesional. Gestionar mejor el estrés también significa ayudarte a rendir mejor, a afrontar los peligros y las crisis con más serenidad, protegiendo al mismo tiempo tu espacio y tu tiempo personal, es decir, gestionando el sutil equilibrio entre la vida profesional y la personal, que está cada vez más entrelazada. Esta mejora incluirá una mejor explicación y valoración del trabajo de los CISOs. La promoción del puesto, un tema muy discutido, debe mejorarse. Explicar las características del trabajo, valorar la diversidad de temas, desmitificar los métodos operativos de los atacantes, especificar lo que todos en la organización pueden aportar, etc.: todas ellas acciones que pueden mejorar el reconocimiento y aumentar el apoyo que los profesionales de la ciberseguridad tienen derecho a esperar.

Gracias a profesionales de ciberseguridad formados en materia de estrés, toda la ciberseguridad será más eficiente. Las empresas y las organizaciones públicas estarán mejor protegidas y serán más eficaces a la hora de centrarse en sus propios retos.

El factor humano ha sido estudiado a menudo en la Ciberseguridad, ya que se considera o bien como un factor recurrente en brechas e incidentes, o más recientemente, de forma más positiva, como una fuente de contribución a la ciberdefensa. Los programas de sensibilización son claves, cada uno aporta su contexto profesional, su deseo de innovación o su propia experiencia. Desafortunadamente, se han descuidado otros factores: los que desempeñan el trabajo de ciberseguridad: El factor humano. Es hora de abordarlos, de mejorar su vida cotidiana y contribuir a una sociedad digital más segura y equilibrada.

10

Apéndices – Cuestionario y datos del estudio

10.1 Apéndice 1 – Cuestionario largo

Tal como se presenta en el documento, el cuestionario del estudio consta de dos partes.

La primera se basa en las 10 preguntas de la "PSS10" (Escala de Estrés Percibido)

	Preguntas PSS10:
1	En el último mes, ¿se ha sentido molesto o irritado por acontecimientos inesperados?
2	Durante el último mes, ¿te has sentido incapaz de controlar los "fundamentos" de tu trabajo/función/rol?
3	En el último mes, ¿te has sentido nervioso o estresado?
4	Durante el último mes, ¿te has sentido plenamente capaz de manejar tus problemas profesionales?
5	Durante el último mes, ¿has sentido que las cosas van como tú quieres?
6	En el último mes, ¿has pensado que no puedes hacer todas las cosas que tienes que hacer?
7	Durante el último mes, ¿has podido controlar (interna y externamente) tu molestia?
8	Durante el último mes, ¿has sentido que tienes el "control"?
9	En el último mes, ¿te has sentido irritado porque las cosas estaban fuera de tu control?
10	Durante el último mes, ¿has descubierto que las dificultades se han ido acumulando hasta el punto en que ya no puedes controlarlas?

La segunda se basa en preguntas elaboradas por Advens y ISMS Forum específicamente para el estudio.

	Preguntas sobre los factores estresantes relacionados con la profesión de CISO:
13	¿Sufre la imagen del CISO percepciones negativas e ideas preconcebidas relacionadas con su función que pueden complicar su trabajo e incluso provocar sentimientos de aislamiento?
14	¿Se siente incomprendido o juzgado como "excesivo" cuando hace recomendaciones?
15	¿Le dan pavor las situaciones en las que su trabajo le obliga a estar al tanto de secretos y/o le coloca en situaciones humanamente delicadas o embarazosas?
16	¿Considera que le faltan conocimientos técnicos o metodológicos?
17	¿Le resulta difícil tener que adaptar constantemente sus análisis y estrategias ante un entorno de amenazas complejo en rápida evolución y tener que aprender y reinventarse constantemente?
18	¿Se siente cómodo con el alcance funcional y técnico del negocio cibernético, que debe garantizar una defensa eficaz a todos los niveles y en todos los terrenos?
19	¿Considera que su trabajo es inusual en el sentido de que implica tratar con adversarios que a menudo son "invisibles" y malintencionados, lo cual es inhabitual porque pocas profesiones experiment...
20	¿Le frustra estar únicamente a la defensiva y no poder nunca tomar represalias o contraatacar?
21	¿Se siente desanimado por la creciente frecuencia y potencia de los ciberataques?
22	¿Se siente impotente ante la naturaleza asimétrica del combate, en el que el atacante tiene una clara ventaja sobre el defensor?
23	¿Se siente alguna vez personalmente en peligro ante tal adversidad?
24	¿Le gusta lo inesperado y lo imprevisible?
25	¿Le molesta no conocer de antemano, o incluso no conocer nunca, a quienes le atacan o cometen un acto malicioso?
26	¿Está constantemente en alerta, incapaz de desconectar sus pensamientos de su trabajo, por miedo a que se produzca un ciberataque o una situación de alto riesgo?

27	¿Siente que su situación profesional es incierta y que una crisis importante podría costarle el puesto de trabajo?
28	¿Considera que la gestión del ciberriesgo es intelectualmente difícil?
29	¿Ha experimentado grandes niveles de adrenalina, presión y/o sensación de urgencia generalmente asociadas a una cibercrisis?
30	¿Disfruta del peligroso equilibrio entre las decisiones que hay que tomar y la información disponible para tomarlas, a lo largo de una crisis?
31	¿Se siente comprendido o al menos apoyado por sus allegados durante los periodos de gestión de crisis?
32	¿Cómo se siente comunicando? ¿Es capaz de expresarse de verdad, de empatizar con los demás y de convencerlos?
33	¿Siente que tiene que justificar ante los demás, o incluso ante sí mismo, la utilidad de sus acciones?
34	¿Se siente culpable a los ojos de los que le rodean y/o de sus superiores cuando se produce un incidente y no fue capaz de evitarlo, detectarlo y/o limitar su impacto?

10.2 Apéndice 2 – Resumen de resultados – Estresores

Familia	Pregunta	No, en absoluto	Más bien no	Más bien sí	Sí, absoluta-mente
Coerción y vigilancia	P13: ¿Sufres de la imagen y, a veces, de las ideas preconcebidas negativas que rodean a tu trabajo, lo que puede complicar tu tarea o incluso causar una sensación de aislamiento? ¿Sufre la imagen del CISO percepciones negativas e ideas preconcebidas relaciona-das con su función que pueden complicar su trabajo e incluso provocar sentimientos de aislamiento?	3,66%	21,95%	54,88%	19,51%
Coerción y vigilancia	P14: ¿ Se siente incomprendido o juzgado como "excesivo" cuando hacerecomenda-ciones?	1,22%	23,17%	53,66%	21,95%
Coerción y vigilancia	P15: ¿Le dan pavor las situaciones en las que su trabajo le obliga a estar al tanto de secretos y/o le coloca en situaciones humanamente delicadas o embarazosas?	43,90%	39,02%	12,20%	4,88%
Complejidad y escalabilidad	P16: ¿Considera que le faltan conocimientos técnicos o metodológicos?	17,07%	58,54%	23,17%	1,22%
Complejidad y escalabilidad	P17: ¿Le resulta difícil tener que adaptar constantemente sus análisis y estrategias ante un entorno de amenazas complejo en rápida evolución y tener queaprender y rein-ventarse constantemente?	15,85%	29,27%	43,90%	10,98%
Transversali-dad	P18: ¿Se siente cómodo con el alcance fun-cional y técnico del negocio cibernético, que debe garantizar una defensa eficaz a todos los niveles y en todos los terrenos?	2,44%	31,71%	46,34%	19,51%
Lucha y adversidad	P19: ¿Considera que su trabajo es inusual en el sentido de que implica tratar con adversarios que a menudo son "invisibles" y malinten-cionados, lo cual es inhabitual porque pocas profesiones experimentan este tipo de adversidad?	6,10%	19,51%	37,80%	36,59%

		No, en absoluto	Más bien no	Más bien sí	Sí, absolutamente
Lucha y adversidad	P20: ¿Le frustra estar únicamente a la defensiva y no poder nunca tomar represalias o contraatacar?	25,61%	26,83%	31,71%	15,85%
Lucha y adversidad	P21: ¿Se siente desanimado por la creciente frecuencia y potencia de los ciberataques?	20,73%	36,59%	30,49%	12,20%
Lucha adversidad	P22: ¿Se siente impotente ante la naturaleza asimétrica de la pelea, con el atacante teniendo una clara ventaja sobre el defensor?	7,32%	36,59%	36,59%	19,51%
Lucha adversidad	P23: ¿Se siente alguna vez personalmente en peligro ante tal adversidad?	34,15%	46,34%	15,85%	3,66%

		No, en absoluto	Más bien no	Más bien sí	Sí, absolutamente
La incertidumbre y lo desconocido	P24: ¿Le gusta lo inesperado y lo imprevisible?	12,20%	46,34%	31,71%	9,76%
La incertidumbre y lo desconocido	¿Le molesta no conocer de antemano, o incluso no conocer nunca, a quienes le atacan o cometen un acto malicioso?	17,07%	40,24	35,37%	7,32%
La incertidumbre y lo desconocido	P26: ¿Está constantemente alerta, incapaz de desconectar sus pensamientos de su trabajo, por miedo a que se produzca un ciberataque o una situación de alto riesgo?	8,54%	30,49%	37,80%	23,17%
La incertidumbre y lo desconocido	P27: ¿ Siente que su situación profesional es incierta y que una crisis importante podría costarle el puesto de trabajo?	20,73%	17,07%	34,15%	28,05%
La incertidumbre y lo desconocido	P28: ¿Considera que la gestión del ciberriesgoes intelectualmente difícil?	1,22%	9,76%	41,46%	47,56%

Gestión de crisis	P29: ¿Ha experimentado grandes niveles de adrenalina, presión y/o sensación de urgencia generalmente asociados a una cibercrisis?	4,88%	20,73%	37,80%	36,59%
Gestión de crisis	P30: ¿ Disfruta del peligroso equilibrio entre las decisiones que hay que tomar y la información disponible para tomarlas, a lo largo de una crisis?	15,85%	31,71%	37,80%	14,63%
Gestión de crisis	P31: ¿Se siente comprendido o al menos apoyado por sus allegados durante los periodos de gestión de crisis?	6,10%	24,39%	39,02%	30,49%
Comunicación y convicción	P32: ¿Cómo se siente comunicando? ¿Es capaz de expresarse de verdad, de empatizar con los demás y de convencerlos?	1,22%	10,98%	63,41%	24,39%
Responsabilidad culpabilidad	P33: ¿Siente que tieneque justificar ante los demás, o incluso ante sí mismo, la utilidad de sus acciones?	6,10%	19,51%	50,00%	24,39%
Responsabilidad y culpabilidad	P34: ¿Se siente culpable a los ojos de los que le rodean y/o de sus superiores cuando se produce un incidente y no fue capaz de evitarlo, detectarlo y/o limitar su impacto?	14,63%	26,83%	46,34%	12,20%

Security for the greater good

¿Desea hablar sobre sus problemas de ciberseguridad?

¡Contáctenos!

www.advens.es

Calle de Agustín de Foxá 4, 28036, Madrid