Kymatio®

ACTIVA TUS FIREWALLS HUMANOS

SaaS de gestión del riesgo enfocado en el factor humano, su concienciación y entrenamiento ante ciberataques

White Paper

CIBERRIESGO HUMANO:

¿QUÉ FACTORES MEDIR PARA PROTEGER TU ORGANIZACIÓN?

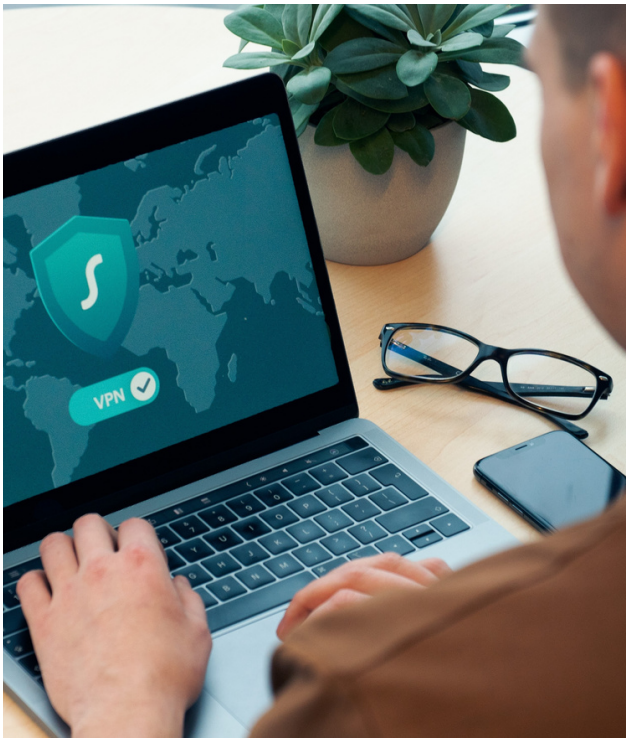
www.kymatio.com

CIBERRIESGO HUMANO: ¿QUÉ FACTORES MEDIR PARA PROTEGER TU ORGANIZACIÓN?

La seguridad de la información es un aspecto clave para las organizaciones. Un incidente puede traer graves consecuencias, tanto a nivel económico como reputacional y legal. El coste medio asociado estuvo en **4.35 millones de dólares** en 2022, según el informe realizado por el Instituto Ponemon e IBM Security (2022), y para las pequeñas y medianas empresas puede implicar incluso el cierre de la compañía.

Las organizaciones son cada vez más conscientes de la necesidad de implementar medidas dirigidas a prevenir estos incidentes, centrando sus esfuerzos en fortalecer su postura de ciberseguridad.

Por supuesto, hay soluciones básicas para la protección de la información de ataques externos, como puede ser la instalación de firewalls y antivirus que filtren los datos que pretenden llegar a los dispositivos corporativos. En esta línea, son muchas las medidas que se pueden tomar a nivel tecnológico para prevenir incidentes, pero, para poder estar realmente protegidos, es necesario prestar atención a otro factor más: **el humano.**



Detrás de cada ordenador, móvil, tableta, etc., se encuentra una persona. Como todo, no hay un ser humano infalible, por lo que es posible que se cometan acciones que deriven en un incidente. Esto es lo que se conoce como ciberriesgo humano.

FACTORES DETRÁS DE UN INCIDENTE DE ORIGEN HUMANO

Son muchas las razones por las que se puede producir un incidente de estas características. Sin embargo, todas y cada una de ellas tienen algo en común: lo nefasto de sus consecuencias. Por eso es imprescindible conocer qué es lo que hay detrás para poder poner solución antes de que suceda un incidente, gestionando este tipo de riesgo de manera holística y no solo parcial.

FALTA DE CONCIENCIACIÓN

La primera razón es la más obvia de todas: la **falta de concienciación**. En muchas ocasiones, los empleados no son conscientes de la importancia que ellos mismos tienen en la seguridad de la organización. Es posible que piensen que este es un área correspondiente de los equipos de seguridad de la Información o de IT, obviando el papel que cada uno desempeña de manera individual. Por eso, el **desarrollo de una cultura de ciberseguridad** dentro de la organización es un punto imprescindible.

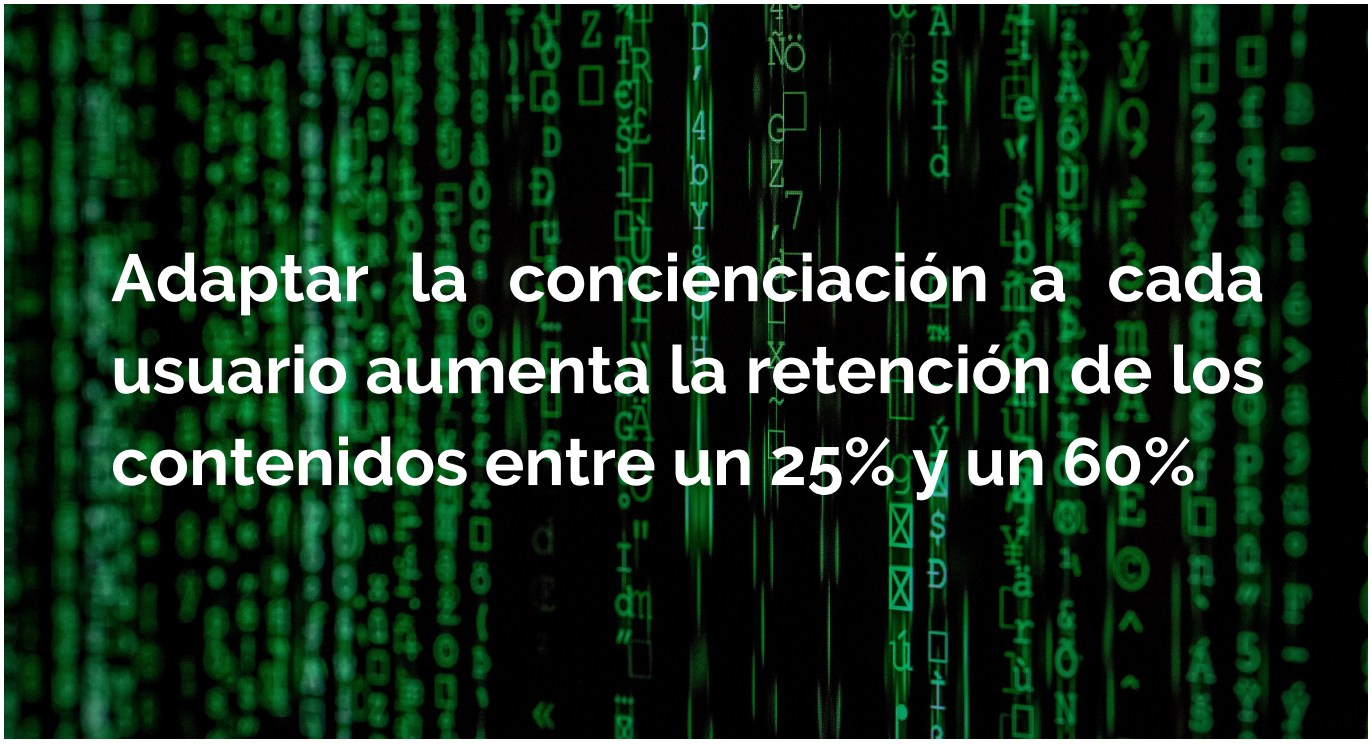
Otras veces, incluso si se es consciente del rol individual que cada uno desempeña en este ámbito, el nivel de concienciación respecto a las buenas o malas praxis no es lo suficientemente alto. Son varias las temáticas a tener en cuenta, entre las que se encuentran:

- **Comunicaciones:** El envío de información a través de internet es una operación que realizamos a diario de una forma u otra. En muchos casos, estos datos que queremos mandar son sensibles, ya sea a nivel personal (como los datos bancarios a la hora de hacer una compra online) o profesional. Saber cómo hacerlo de manera segura es muy importante para evitar incidentes de seguridad.

- **Cumplimiento:** Si bien las organizaciones suelen tener un equipo dedicado a las tareas legales relacionadas con el cumplimiento normativo, cada empleado tiene su responsabilidad individual sobre la información que maneja. Sin embargo, no todos son conscientes de este hecho o de cuál es su labor, por lo que se trata de un área a reforzar.

- **Protección de datos:** Aunque hay muchos empleados que conocen la importancia de la información que tienen entre manos, no es el caso de todos. También puede ocurrir que, aunque sepan que deben protegerla, no sepan cómo hacerlo. Concienciarles en estos aspectos es fundamental para mantener la seguridad.

- **Malware:** Uno de los principales peligros a los que se enfrenta cualquier usuario de internet es la proliferación de software malicioso. Si bien los antivirus y firewalls son capaces de filtrar una gran cantidad de ellos, no siempre es posible, entre otras razones porque, al igual que estos programas de defensa, los ciberdelincuentes también se actualizan. Por eso es importante que los empleados sepan de los tipos de malware que pueden encontrarse y las maneras en las que podrían quedar infectados sus dispositivos.



- **Gestión de contraseñas:** Todos nuestros dispositivos y cuentas están protegidos por una contraseña. Se trata de la llave de acceso a toda nuestra información y a las distintas funcionalidades de las que hacemos uso bajo nuestra propia responsabilidad. Por esta razón, saber cuáles son las mejores prácticas para proteger nuestras cuentas y dispositivos es fundamental.

- **Ingeniería social:** Es uno de los principales métodos de ataque que emplean los ciberdelincuentes hoy en día debido a su gran efectividad. "Hackear" a las personas ha demostrado ser, en muchos casos, más efectivo que hackear ordenadores y otros dispositivos, por lo que es imprescindible concienciar a los empleados sobre la existencia de esta práctica y las distintas formas que puede adoptar.

- **Seguridad en el puesto de trabajo:** La seguridad de la información no puede concebirse de forma aislada, sin tener en cuenta el entorno donde se desempeñan las actividades relacionadas con ella. Ya sea en la oficina, en casa o en cualquier otro lugar, saber cómo se debe actuar en cada lugar es algo que todos los empleados deben interiorizar.

Mantener un buen estado de alerta es fundamental para proteger la información con la que tratamos, y para ello es necesario abordar todas estas temáticas de manera no solo teórica, sino también práctica, para que puedan llevar a la realidad los conocimientos adquiridos.

BIENESTAR

Por supuesto, sin concienciación queda un agujero muy grande que cubrir para evitar la entrada en escena de ciberdelincuentes, así como la prevención de errores. Sin embargo, no es el único factor a tener en cuenta.

El siguiente punto a tratar es uno que, tradicionalmente, se ha asignado al departamento de Recursos Humanos: el **bienestar de los empleados.** Y, si bien es cierto que esta área de la organización es la que más se involucra, también atañe de manera directa a Seguridad de la Información.

Es obvio que el bienestar de todas las personas que trabajan en una organización debería ser una de las máximas de la Dirección por el mero hecho de ser personas; no obstante, el mantenimiento de la seguridad es otra razón más que añadir a la lista.

Esta estrecha relación se da por varias causas. Para un empleado que se encuentra a disgusto en su organización, su interés en lo que pueda ocurrir en ella más allá de lo que le afecta directamente se ve reducido. Lo más probable es que en su mente no ocupe lugar la seguridad de la información, sino esos plazos que tiene que cumplir y la falta de tiempo para ello, la presión recibida por parte de sus responsables o cualquier otro aspecto que le esté generando ese malestar. Esto aumenta la probabilidad de que se produzca una **negligencia** que derive en un incidente. Paralelamente, también crece la probabilidad de materialización de **incidentes intencionados**, una posibilidad que no debemos dejar a un lado.

Mención especial merece el **síndrome de burnout.** Reconocido por la Organización Mundial de la Salud (OMS) como una enfermedad laboral, consta de tres dimensiones: cansancio emocional, despersonalización y una baja percepción de autorrealización (Maslach y Jackson, 1981). Según la OMS (1994):

> El agotamiento físico se evidencia por falta de energía, fatiga crónica, debilidad, cansancio, mayor susceptibilidad a la enfermedad, dolores de cabeza frecuentes, náuseas, tensión muscular, dolores de espalda, diversas molestias somáticas y trastornos del sueño. El agotamiento emocional puede implicar sentimientos de depresión, impotencia, desesperanza, aumento de la tensión y los conflictos en el hogar, aumento de los estados afectivos negativos (p. ej., ira, impaciencia e irritabilidad) y disminución de los estados positivos (p. ej., amabilidad, consideración, cortesía).
>
> El agotamiento mental puede implicar insatisfacción y actitudes negativas hacia uno mismo, hacia el trabajo y hacia la vida en general. Finalmente, también se ha observado un aumento en los comportamientos de retiro del trabajo (por ejemplo, ausentismo y rotación). (p. 1)

En un estudio realizado por Global Web Index y Asana (2021) con más de 10.500 participantes procedentes de siete países, se encontró que **un 67% de los empleados de organizaciones medianas y un 53% de empresas pequeñas habían experimentado burnout.** No faltan razones para decir que estos datos son, cuanto menos, alarmantes.

Trabajar en la evitación de este síndrome y en el bienestar general de los empleados no solo conseguirá hacer del entorno de trabajo un lugar más feliz para todos, sino que también traerá consigo un aumento de la **productividad** (Wright and Cropanzano, 1997, 2000), una reducción de la **rotación** y sus costes asociados (Wright y Bonett, 2007; Cascio, 2003 en Page y Vella-Brodrick, 2009) y lo que nos atañe en este documento: una **disminución de la probabilidad de incidentes de seguridad de la información.**

DIFERENCIAS INDIVIDUALES

Muy relacionado con el punto anterior se encuentra el tercer factor a tener en cuenta: las **diferencias de cada empleado a nivel individual.** Estas diferencias van más allá del conocimiento de las normativas y protocolos, tienen que ver con nuestra forma de ser y de relacionarnos con el mundo que nos rodea.

Ante una misma situación, dos personas pueden reaccionar de manera totalmente diferente. Por ello, cabe deducir que **su relación con la ciberseguridad también difiere.**

Nuestra personalidad determina en gran medida cómo actuaremos en los distintos entornos. Por ejemplo, algunos tienen una gran facilidad para confiar en los demás, mientras que otros son más reservados y requieren de más tiempo para abrirse. Otro ejemplo sería la emocionalidad que cada uno le confiere a cada situación: algunas personas son capaces de mantener la calma incluso ante situaciones extremadamente adversas, mientras que otras son más propensas a sentir estrés, enfado y otras emociones con facilidad (Costa y McCrae, 1985).

Puede que, a priori, esto no parezca muy relacionado con la seguridad de la información, pero **nada más lejos de la realidad**. Esas personas que tienden a confiar en los demás podrían llegar a **compartir información o caer en malas prácticas** (como cesión de claves de acceso) por pensar que su interlocutor no tiene malas intenciones. Del mismo modo, una persona relajada, que tienda a ver la vida desde un punto de vista más laxo y distendido, podría no darle a la seguridad la importancia que merece, **prestando poca atención** y teniendo pensamientos del tipo "esto no me va a pasar a mí" o "estos procedimientos son exagerados". En el otro polo del continuo nos encontramos con personas que se **estresan con facilidad**. En estos casos, cuando existe mucha carga de trabajo lo normal es priorizar la finalización de las tareas sobre la seguridad y, además, ese estrés puede facilitar que se produzcan **errores** que deriven en un incidente.

Cada persona tiene su **predisposición**, y saber cuáles son les permitirá poner atención en estos aspectos que, de otra manera, pasarían desapercibidos.

Esto tiene especial relevancia cuando hablamos de **ingeniería social**. Las motivaciones de las personas son diferentes y, mientras algunos se mueven por la búsqueda de beneficios, otros lo hacen por la evitación de consecuencias negativas (Gray, 1981). De esta forma, puede que nos encontremos detectando correctamente un tipo de ataque, pero no así otros. Conocer cuáles son esos puntos en los que podemos ser más vulnerables es muy importante para mantenernos alerta en todo momento.

¿CÓMO INTEGRAR ESTO EN UN PROGRAMA DE GESTIÓN DEL RIESGO?

Habiendo puesto todos estos factores relevantes sobre la mesa, queda patente que el enfoque actual para la gestión del riesgo **no es suficiente.**

En primer lugar, es necesario integrar en él el **elemento humano** e ir más allá de las soluciones tecnológicas que, hasta el momento, se habían considerado suficientes.

Por supuesto, son cada vez más las organizaciones que deciden dar un paso más e introducir programas de concienciación en su plan director de seguridad. Sin embargo, a menudo estos **se quedan cortos** respecto a las necesidades reales para fortalecer a la plantilla de una manera verdaderamente eficaz.

En la mayor parte de los casos, esto se debe a la **aproximación a la concienciación**. Por lo general, se realizan largos cursos anuales o semestrales para todos los empleados por igual. Por sus características, se hacen tediosos y resultan poco eficaces, por no mencionar que solo cubren el primer punto tratado en este documento.

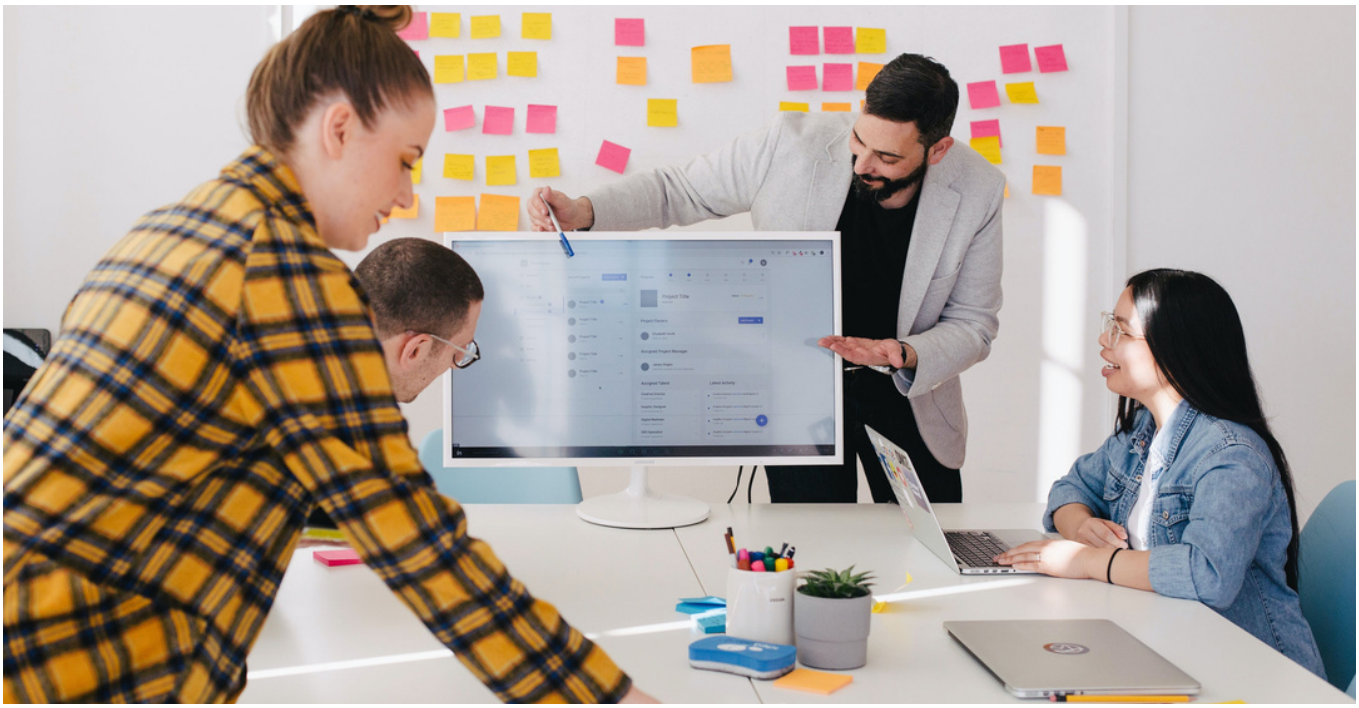
Para poder gestionar con éxito el riesgo asociado al factor humano, se deben contemplar todos los aspectos explicados de manera holística, algo que, por lo general, no ocurre. Una buena gestión pasa por los siguientes puntos:

- **Concienciación periódica** mediante sesiones teóricas en las diferentes áreas de la seguridad de la información.

- Poner estos conocimientos en **práctica** a través de **simulaciones de ataque** que permitan comprobar cómo se comportarían los empleados en un escenario real.

- **Obtención de métricas.** Uno de los grandes problemas de la concienciación actual es que no se obtiene ningún tipo de dato que permita saber si está surtiendo el efecto deseado o no. Contar con unas métricas que proporcionen esta información permitirá no solo llevar un registro sobre la evolución del riesgo, sino también ajustar los itinerarios en función de las necesidades.

- **Medición del bienestar de los empleados.** Como se ha explicado anteriormente, el bienestar no está separado de la seguridad, sino todo lo contrario. Saber cómo se encuentran los empleados y trabajar por mejorar este aspecto repercutirá de manera muy positiva tanto a la propia plantilla como a la organización.



- **Personalizar la experiencia y el programa de concienciación** según las necesidades de cada individuo. Para esto se necesitará una herramienta **automatizada**, de forma que no sea necesario invertir un tiempo excesivo en la elaboración de distintos itinerarios ajustados a cada persona.

- **Hacerlo divertido.** Para que los empleados quieran participar y puedan aprovechar todo lo que el programa puede aportar, es necesario introducir un componente de gamificación.

Si bien estos puntos son un breve resumen de los aspectos a tener en cuenta, en este whitepaper explicamos de manera más extensa por qué los enfoques de concienciación actuales no funcionan y cuál es la mejor aproximación.

CONCLUSIÓN

La gestión del riesgo asociado al factor humano sigue siendo uno de los principales desafíos para las organizaciones. Mientras no se aborde de **manera integral**, tal y como se está haciendo hasta el momento, estarán condenadas a seguir exponiéndose y, en los casos más desafortunados, sufriendo incidentes de seguridad.

Está claro que **no es una misión fácil** para los equipos de seguridad. Se trata de una tarea compleja y, debido a ello, consume mucho tiempo. Por eso es necesario contar con una **herramienta que automatice este proceso** para así poder ir un paso más allá en la protección de la información de las organizaciones.

SOBRE KYMATIO®

Kymatio® es una solución SaaS que automatiza la concienciación de los empleados y la evaluación de su estado de alerta de forma desatendida y personalizada, al tiempo que proporciona una herramienta de gestión de riesgo asociado al elemento humano, con métricas, evolución en el tiempo y planes de acción.

Utilizando la neuropsicología y la ciberseguridad como base de su tecnología, la IA de Kymatio® interactúa con las personas, ofreciéndoles una concienciación personalizada y adecuada a sus necesidades, manteniendo el nivel de alerta y fortaleciendo las áreas en las que pueden ser más vulnerables.

Dicho programa de concienciación ofrece píldoras de concienciación que fortalecen al empleado en las áreas que verdaderamente necesita, incluyendo contenido multimedia que ayuda a la retención de contenidos. Esto se consigue gracias a las evaluaciones periódicas que realiza el empleado al interactuar con la plataforma.

Al mismo tiempo, proporciona a las organizaciones visibilidad en tiempo real sobre el riesgo humano en función de distintas métricas como el nivel de concienciación, las funciones y acceso a la información, el nivel de bienestar, respuesta a simulaciones de ataque de phishing o vigilancia sobre exposición online de credenciales de empleados.

Para saber más, contacta con nosotros en **contact@kymatio.com** o pídenos una reunión en **https://calendly.com/kymatio**

SOBRE LA AUTORA

ANDREA ZAMORANO

Cyberpsychology Manager en Kymatio®, investiga el lado humano de la ciberseguridad y desarrolla los algoritmos necesarios para que la plataforma sea capaz de medir con precisión los factores implicados, de forma que se pueda evaluar el riesgo y presentar las recomendaciones personalizadas en función de las necesidades de cada uno. También es docente en la Escuela de Inteligencia Económica de la UAM (La_SEI) como experta en perfilado indirecto de personalidad. Es psicóloga de formación, habiendo estudiado en la Universidad Autónoma de Madrid, y posteriormente se graduó del Máster en Inteligencia Económica y Relaciones Internacionales por La_SEI. También cuenta con un título de Experto en Organización y Recursos Humanos por la Universidad Autónoma de Madrid.

BIBLIOGRAFÍA

Cascio, W. F. (2003). Managing human resource: Productivity, quality of work life, profits. New York: McGraw-Hill.

Costa, P. T., & McCrae, R. R. (1985). The NEO personality inventory. Odessa, FL: Psychological Assessment Resources.

Global Web Index, Asana (2021). ANATOMY OF WORK SPECIAL REPORT: Keeping employees engaged in a burned-out world. Recuperado de: https://asana.com/es/resources/anatomy-of-work-summary

Gray, J. A. (1981). A critique of Eysenck's theory of personality. In Eysenck H. J., A model for personality (pp. 246-276). Springer, Berlin, Heidelberg.

Maslach, C., & Jackson, S. E. (1981). The measurement of experienced burnout. Journal of organizational behavior, 2(2), 99-113.

Page, K. M., & Vella-Brodrick, D. A. (2009). The 'what','why'and 'how'of employee well-being: A new model. Social indicators research, 90, 441-458.

Ponemon Institute, IBM Security (2022). Informe del Coste de la vulneración de datos 2022. Recuperado de: https://www.ibm.com/es-es/reports/data-breach

World Health Organization. (1994). Guidelines for the primary prevention of mental, neurological and psychosocial disorders. 5. Staff burnout (No. WHO/MNH/MND/94.21. Unpublished). World Health Organization.

Wright, T. A., & Bonett, D. G. (2007). Job satisfaction and psychological well-being as nonadditive predictors of workplace turnover. Journal of Management, 33, 141–160.

Wright, T. A., & Cropanzano, R. (1997, August). WELL-BEING, SATISFACTION AND JOB PERFORMANCE: ANOTHER LOOK AT THE HAPPY/PRODUCTIVE WORKER THESIS. In Academy of Management Proceedings (Vol. 1997, No. 1, pp. 364-368). Briarcliff Manor, NY 10510: Academy of Management.

Wright, T. A., & Cropanzano, R. (2000). Psychological well-being and job satisfaction as predictors of job performance. Journal of Occupational Health Psychology, 5, 84–94.