La SEI
School of Economic Intelligence
Escuela de Inteligencia Económica
Universidad Autónoma de Madrid

2018

Volumen 1 nº 2, pp. 11-22

ISSN 2659-9791

UAM

- DRAFTS OF ECONOMIC INTELLIGENCE -

EL FACTOR HUMANO EN LA FUGA DE INFORMACIÓN PRIVILEGIADA Y SU RELACIÓN CON LA PERSONALIDAD

Andrea Zamorano Salardón*

Resumen/Summary

La mayor parte de las pérdidas relacionadas con la fuga de información en las empresas tiene que ver con personas dentro de la misma. El objetivo del presente ensayo es considerar los distintos aspectos de estas personas denominadas *insider*, tales como su definición, tipología, motivaciones y métodos de detección actuales. Posteriormente se estudiará su posible relación con los rasgos básicos de personalidad. De esta forma se pretende realizar una primera aproximación a la detección temprana de *insiders* potenciales basándonos en test de personalidad y en el perfilado indirecto. Para ello, se han analizado diversos artículos de investigación de distintas disciplinas y así tener una visión más amplia del problema.

Palabras clave/*Key words*: Información privilegiada, *insider*, personalidad, relación.

1. Introducción

Gran parte de la información que manejan las empresas es de carácter confidencial, por lo que es necesario mantener la seguridad de estos datos mediante diferentes técnicas como, por ejemplo, la encriptación del tráfico de la red. Esta es una de las múltiples formas de prevenir la pérdida de datos debida a los ataques externos. Sin embargo, la mayor parte de las pérdidas derivadas de la fuga de información privilegiada se deben a personas dentro de la compañía. Frente al 30% de los ataques que provienen de personas ajenas a la empresa, nada menos que el 70% restante es perpetrado por empleados propios de la entidad (Peltier, 2006). Este es un problema que, además, ha ido en aumento en muchas de ellas y que, cuanto más tiempo pasa sin que se detecte a la persona que filtra la información, mayor es el daño que produce (Wall, 2013) Por tanto, la detección de dichas personas es clave para frenar la sangría de información y el daño económico que provoca.

En términos generales, a la persona que filtra información desde dentro de una entidad se le suele denominar *insider* (Nurse et al., 2014b). Si bien todos somos potencialmente capaces de filtrar información de forma más o menos intencionada, no todos tenemos la misma probabilidad de hacerlo dadas las circunstancias apropiadas para ello. ¿Existen personas más proclives a filtrar dicha información? ¿Bajo qué circunstancias?

1.1. Relevancia

La mayor parte de la literatura que existe hasta el momento en relación con este problema trata acerca de cómo detectarlo a posteriori del filtrado de la información. Sin embargo, pocos son los que tratan del concepto del *insider trading* en relación con factores psicológicos asociados, y menos de su detección temprana.

Por tanto, el objetivo de esta revisión es buscar un punto común en la investigación que se ha realizado hasta la actualidad, y plantear cómo los diversos factores a los que

* *Escuela de Inteligencia Económica (La_SEI). Universidad Autónoma de Madrid (Spain)* Correo de contacto: andreazamoranos@hotmail.com

apunta pueden relacionarse con la psicología de cara a una detección temprana del *insider*.

1.2. Insider Trading

Para poder hablar acerca del *insider trading* es necesario empezar por el análisis de la palabra *insider*, un anglicismo que hemos adoptado y que no tiene una traducción exacta al castellano. Las acepciones que se encuentran en el diccionario online Diccionary.com (2018) son:

1. Persona miembro de un grupo, organización, sociedad, etc.

2. Persona perteneciente a un círculo limitado de personas que entienden los hechos de una situación o comparten conocimiento privado.

3. Persona que tiene especial ventaja o influencia.

4. Persona en posesión de información corporativa, generalmente no disponible al público, como director, contable u otro empleado de la compañía.

Por otra parte, existen ciertas acepciones de términos en castellano que pueden acercarse de alguna forma a la visión más negativa de un *insider*, como incidir ("caer o incurrir en una falta, un error, un extremo, etc."), traidor ("que comete traición; que es más perjudicial de lo que parece") o traición ("falta que se comete quebrantando la fidelidad o lealtad que se debe guardar o temer"). Para completar este último significado, resulta oportuno tener en cuenta asimismo el de lealtad: "cumplimiento de lo que exigen las leyes de la fidelidad y las del honor y hombría de bien" (Real Academia Española, 2017).

1.3. Información privilegiada

Si la figura del *insider* tiene relevancia, es justo por la información sensible que filtra. Entendemos la información privilegiada como aquella información que no se ha ofrecido de manera pública y que podría afectar, beneficiando o perjudicando, a los accionistas, clientes (Huerta, 2001) o competidores de la empresa en cuestión.

Por tanto, aunando todas las definiciones y siguiendo a Huerta (2001), se puede considerar que un *insider* es la persona que tiene acceso a los activos de la empresa y los emplea para obtener algún tipo de beneficio bien personal, bien de terceros, sea o no patrimonial. Además, según Prado (2002), tiene una serie de atributos: ha de ser, aparte de desconocida, precisa y determinada de forma que no dé lugar a confusión; debe referirse a ciertos aspectos de la empresa que tengan repercusión en el mercado, y debe ser capaz de traer consecuencias en términos de modificación de aspectos económicos de la compañía (a lo que denominan "idoneidad").

2. Metodología

Tal y como se menciona en todos los motivos anteriores, el *insider trading* es un tema de gran relevancia en la sociedad actual. Para poder llevar a cabo el objetivo de relacionar el factor psicológico con los diferentes aspectos del *insider* se ha realizado una revisión bibliográfica sobre la literatura previa.

2.1. Materiales

Para llevar a cabo esta revisión se han empleado 28 artículos de investigación, 6 libros y 2 páginas web.

2.2. Procedimiento

Se ha realizado una búsqueda bibliográfica utilizando diversas bases de datos para la obtención de la información, como ProQuest. También se ha buscado en Google Académico, donde aparecen la mayor parte de los artículos empleados, así como en Google para encontrar la página de la Real Academia Española (RAE). Por último, se han aprovechado los estudios mencionados en las investigaciones para hacer búsquedas concretas de algunos artículos.

Para que esta búsqueda fuera lo más exhaustiva posible se ha acotado utilizando las siguientes palabras clave: insider, insider trading, personality, types of insider, insider personality, información privilegiada, data leakage.

La mayor parte de las búsquedas se han realizado en inglés para obtener un mayor volumen de artículos, aunque en algunos casos también se han introducido en castellano.

Se organizó en función de la temática y del contenido de cada artículo, de forma que el texto adquiriera coherencia en su disposición.

3. Resultados

Los resultados de la búsqueda fueron muy dispares. La mayor parte de los artículos, 23 en total, estaban relacionados con la ingeniería informática, donde se explicaban diferentes métodos que emplean los *insider* para obtener la información privilegiada y cómo combatirlos. Por otra parte, pocos eran aquellos que hablaban de la psicología del *insider* y de su personalidad, habiendo encontrado 14 relevantes para el estudio, si bien algunos no proporcionan una visión profunda de estos aspectos. No obstante, es posible que, por razones de acceso restringido a la información, no se hayan encontrado más artículos de este tipo. Además, con el fin de enriquecer la visión del problema, se contó con 4 artículos pertenecientes a las disciplinas de la Economía y el Derecho.

En este apartado se analizarán los diversos aspectos a tener en cuenta respecto a estas personas, como pueden ser su tipología, sus motivaciones o sus métodos de detección. También se expondrá el modelo de personalidad de Eysenck, uno de los más universales, si bien no el más completo. Sin embargo, teniendo en cuenta la complejidad del problema, es el modelo más sencillo que nos permite realizar una primera aproximación a la detección temprana de los *insider*.

Es necesario hablar de todos estos aspectos, puesto que esta prevención y detección se facilita si tenemos en cuenta el factor psicológico. Existen muchos atributos psicológicos a tener en cuenta a la hora de detectar un *insider* tales como la búsqueda de sensaciones (Marcus y Schuler, 2004) el egocentrismo, arrogancia, temeridad, manipulación, frialdad, autoengaño y posición defensiva; la llamada Tríada Oscura (Turner y Gelles, 2006) que se tratará posteriormente, o la inmadurez, amoralidad, perspectiva no ética, tendencia a la fantasía, inquietud e impulsividad, y falta de consciencia que propone el Centro de Protección de la Infraestructura Nacional de Reino Unido (Nurse et al., 2014b).

No obstante, es preciso poner todas estas teorías en relación con las diferentes características del *insider*, ya que cada una tiene sentido en función de éstas, tal y como se expone a continuación.

3.1. Tipología

Los *insider* pueden clasificarse en distintas categorías en función de su naturaleza. Es importante plantearse cuál es el tipo de *insider* del que hablamos ya que, en función de sus características, es más probable que se relacione con un factor psicológico u otro, tal como se mencionaba anteriormente.

No todos los casos de fuga de información privilegiada a causa de personal de la empresa se deben a sujetos con una clara intencionalidad de hacer daño a dicha entidad. A veces estas acciones se llevan a cabo de forma no intencionada, o incluso pensando en reportar un beneficio. Es por eso que los *insider* se dividen en negligentes, bienintencionados y malignos.

El *insider* negligente o benevolente es aquel trabajador que, por una utilización descuidada de las tecnologías, filtra o pierde esta información accidentalmente en su error (Nurseb et al., 2014b).

Es en el estudio de Wall (2013) donde se hace una diferencia dentro de este grupo, entre los *insider* negligentes y los bienintencionados. Mientras que los negligentes se ciñen a las acciones ya mencionadas, los segundos son trabajadores que se saltan las medidas de seguridad para que su trabajo sea más eficiente y así reportar un mayor beneficio a la empresa. Sin embargo, lo que no tienen en cuenta es que estos datos quedan expuestos, facilitando el ataque posterior de terceras personas que quieran emplear esta información de forma dañina contra la organización.

Por otra parte, nos encontramos con los *insider* malignos, aquellos que son conscientes de que perjudican a la empresa filtrando los datos en cuestión (Nurse et al., 2014b).

Estos *insider* malignos, sabiendo cuál es su objetivo, pueden acceder a la información mediante diferentes métodos: mal uso del acceso, puente de defensa y falla en el control de acceso (Bellovin, 2008).

El mal uso del acceso es el más complejo de detectar. Se trata de trabajadores que, legalmente, pueden acceder a los datos en cuestión para después emplearla en su propio beneficio. Los *insider* que consiguen información privilegiada mediante este método reciben el nombre de traidores. No obstante, también existen trabajadores no autorizados que acceden mediante la suplantación de estas personas acreditadas, los denominados enmascarados (Maestre y García, 2014).

El puente de defensa hace referencia a aquellas medidas de seguridad centradas en evitar ataques externos. Esto provoca que no se detecten aquellos perpetrados por *insider* al encontrarse dentro de la propia entidad.

Por último, también pueden actuar aprovechando un fallo en el sistema. Cuando esto ocurre, es necesario apoyarse en otros métodos de detección porque el sistema ha dejado de funcionar, sin poder reportar cualquier tipo de anomalía provocada por un *insider*.

Sin embargo, se puede conseguir información sin necesidad de acceder a ella directamente. Aquí es donde entran tanto el *tippe trading* como la ingeniería social, conceptos que están muy relacionados. Este primero hace referencia al comúnmente denominado "soplo". Es un método muy común, ya que se trata de una práctica sencilla que, por lo general, ni siquiera reporta un beneficio monetario, al menos inmediato, para la persona que filtra la información (Huerta, 2001).

Por otra parte, nos encontramos con el problema de la práctica denominada ingeniería social. Según Peltier (2006), los ingenieros sociales son personas que buscan conseguir información de una empresa gracias a sus trabajadores. Para ello emplean diferentes técnicas, si bien algunas basadas en la tecnología, otras muchas basadas en el contacto directo con las personas.

Estos ingenieros sociales suponen una gran amenaza para las compañías, ya que las posibilidades de detectarlos son

muy inferiores a las de otro tipo de atacante, en parte debido a sus métodos y en parte por su capacidad de llevar sus acciones a cabo sin levantar sospechas. Suelen basarse en ciertas características de los trabajadores para escoger a sus posteriores informantes; Thomas (2006) identifica cuatro principales, a saber: el deseo de ser útiles, tendencia a confiar en la gente, miedo a meterse en problemas y la disposición a ahorrarse tiempo o esfuerzo.

Aquellas técnicas relacionadas con la psicología tienen mucho que ver con el ámbito de la persuasión y la influencia, ya que son capaces de obtener información de diferentes personas. Existen dos rutas mediante las que pueden conseguirlo: la directa y la indirecta. La ruta directa hace referencia a las preguntas llanas por los datos que se quieren obtener, mientras que la indirecta es algo más complicada. Trata de inducir un estado psicológico en el objetivo que le haga más vulnerable. De esta forma, el trabajador puede compartir la información por diferentes razones como el miedo, la culpa o la confianza con su interlocutor.

Es por eso que, revisando los distintos aspectos relacionados con el fenómeno del insider trading, se pueden plantear diferentes cuestiones a tener en cuenta poniendo la psicología de la personalidad en el punto de mira. Por ejemplo, la relevancia de realizar tests de personalidad en los procesos de selección, bien para todas las vacantes o sólo para aquellas que sean críticas por el manejo de información sensible.

Uno de los interrogantes de este problema es: una vez han recabado todos los datos necesarios, ¿qué es lo que planean hacer con ellos?

Nurse et al. (2014b) plantean dos tipos de actividades a realizar con la información privilegiada conseguida: fraude y robo de la propiedad intelectual.

Entienden por fraude como todas aquellas acciones llevadas a cabo con la intención de obtener algún tipo de beneficio económico. Dicho beneficio puede producirse gracias a la apropiación directa del capital de la compañía o gracias a la difusión de la información.

Por otra parte, el robo de la propiedad intelectual se refiere a la apropiación de información relacionada, principalmente, con los productos o los clientes. En estos casos los ataques suelen realizarse de manera más sofisticada, tratándose, por lo general, de personal técnico autorizado. Esto quiere decir que no solo tienen acceso a estos datos, sino que también saben cómo utilizar los recursos tecnológicos implicados.

Moore et al. (2011) proponen dos modelos mediante los cuales un insider puede actuar robando parte de la propiedad intelectual de la empresa: el del Intitulado Independiente y el del Líder Ambicioso.

Los llamados intitulados independientes son trabajadores de una empresa que se convierten en insider de forma que trabajan solos, robando información para su propio beneficio. Aproximadamente tres cuartos de este tipo de amenazas obtienen datos confidenciales en los que ellos mismos han estado trabajando y que han ayudado a construir. Es por esto que creen que tienen derecho a recolectar este tipo de información, a pesar de que incluso hayan firmado algún tipo de acuerdo en que se definían dichos datos como propiedad intelectual de la empresa.

En muchos casos, este tipo de amenaza se genera a raíz de la insatisfacción con la compañía, lo que produce que el trabajador busque otras ofertas en empresas de la competencia. Cuando consiguen un contrato con la otra entidad es cuando deciden actuar, robando la información, bien para emplearla en su nuevo puesto, bien en caso de que algún día pueda necesitarla.

El patrón de ambos modelos es bastante similar, aunque difieren en algunas características. El modelo del Líder Ambicioso hace referencia a aquellos trabajadores que deciden robar información confidencial para desarrollar su propio producto, para trabajar con una empresa competidora, o para venderla. Las acciones que se llevan a cabo son más complejas, por lo que necesita trabajar en colaboración con otros compañeros, que normalmente deciden unirse a este líder por las consecuencias positivas que acarrearía la resolución satisfactoria del plan.

Otro de los aspectos diferentes respecto al anterior modelo es la motivación: en este caso, la mayoría no actúa por insatisfacción con la compañía, sino por la ambición, por las recompensas que se podrían obtener. Esto se puede aplicar tanto al líder como al resto del equipo, como se menciona en el párrafo anterior.

Tal y como se ha observado, existen diferentes tipos de *insider* y de prácticas, a diferencia de lo que podría pensarse en un principio debido a la influencia de las películas y libros relacionados con el fenómeno del *insider trading* malicioso. Por eso es importante saber qué es lo que llevaría a cada tipo a cometer estas infracciones.

3.2. Motivaciones

Con esta información en mente cabe preguntarse, ¿qué motivaría a un empleado a filtrar la información privilegiada de su propia empresa?

Según Huth, Chadwick, Claycomb y You (2013) las dos motivaciones más comunes son la venganza y la obtención de un beneficio. Sin embargo, Pfleeger (2008) identifica muchos más motivos por los cuales un trabajador puede convertirse en un *insider*, a saber:

- Cometer un error inintencionado.

• Intentar conseguir las tareas requeridas, por ejemplo, cuando el sistema no permite una acción particular o al *insider* se le bloquea el acceso a ciertos datos, el *insider* podría tratar de acceder mediante rodeos para conseguir lo mismo.

• Intentar hacer que el sistema haga algo para lo que no está diseñado, como una forma de innovación para hacer a dicho sistema más útil o manejable.

• Intentar hacer algo inocentemente más allá del límite autorizado, sin saber que la acción está prohibida.

• Revisar el sistema para detectar debilidades, vulnerabilidades o errores, sin intención de reportar problemas.

• Investigar, matar el tiempo mirando datos.

• Expresar aburrimiento, venganza o disgusto.

• Percibirlo como un reto: tratar al sistema como un juego a burlar.

• Actuar con la intención de causar daño, por razones tales como la fama, la avaricia, demostrar capacidad, la lealtad dividida o el engaño. (pp.6, 7).

Este análisis muestra la diversidad de motivos por los que un trabajador podría llegar a filtrar información de la empresa, tanto por una actitud negativa hacia la misma como por una actitud positiva. No obstante, que el *insider trading* no se haya realizado de manera intencionada no implica que dicha actividad sea más fácil de detectar. Es por eso que se debe contar con varios métodos de detección.

3.3. Detección de insiders

La mayor parte de los estudios se basan en modos de detectarlos en lugar de buscar cómo prevenirlos. Actualmente se trabaja, principalmente, con técnicas de *machine learning* o aprendizaje automático (Khorshed, Ali y Wasimi, 2011). "El aprendizaje automático es una rama de la inteligencia artificial que emplea un software de reconocimiento de patrones que analiza grandes cantidades de datos para predecir algún comportamiento (…)" (Mena, 2011, p.1). En definitiva, estas técnicas se basan en el patrón de conducta de los usuarios de las aplicaciones de forma que se pueda ir amoldando a su comportamiento para así conseguir el objetivo en cuestión. Algunos ejemplos pueden ser relativos a la publicidad: en función de las páginas y los productos que se visiten en internet, nos aparecerán artículos de unas características u otras. Sin embargo, en muchas ocasiones no se pueden prevenir las acciones de los *insider* hasta que no se ha perpetrado un ataque, tal y como señalan Khorshed et al. (2011).

Una de las prácticas que se emplean trata de desencriptar el tráfico en la red para poder analizarlo en busca de amenazas (Koch y Dreo Rodosek, 2010). El problema es la gran cantidad de dificultades que presenta, ya sea por comodidad o por cuestiones legales.

Además, muchas veces los *insider* son capaces de acceder, bien por estar autorizados, bien porque conocen el funcionamiento de los dispositivos electrónicos de las empresas.

Sin embargo, también tiene una parte positiva, puesto que el uso de este tipo de canales encriptados permite elaborar patrones de comportamiento que pueden ser comparados con conductas anómalas. Esto supondría una advertencia de cara a la detección de un posible *insider*.

Aparte de los métodos convencionales, hay autores como Sharif, Faiz y Raza (2008); Rybnik, Panasiuk y Saeed (2009); o Melnikov y Schönwälder (2010), que proponen otro tipo de procedimientos de detección basados en el comportamiento de los sujetos a la hora de emplear los ordenadores.

Garfinkel, Beebe, Liu y Maasberg (2013) propusieron una hipótesis diferente a las ya planteadas sobre los patrones de acceso a la información. En este caso, la referencia es el almacenamiento: los *insider* maliciosos tendrán una serie de datos en sus archivos que no tendrán ni sus compañeros ni otras personas que pasaron por la empresa a lo largo del tiempo.

Willison y Warkentin (2013), ponen en relevancia una característica del almacenamiento de datos de este tipo de *insider*. Suelen tener toda la información robada en un solo lugar, de forma que les resulte más fácil exportarla. Esto es lo que hace que sea diferente del sistema de almacenamiento de cualquier otro compañero o de lo que cabría esperar.

Sin embargo, para poder detectar a cada caso particular de *insider* es necesario tener en cuenta su tipología, puesto que el procedimiento difiere en función de la misma. Los traidores deben ser detectados gracias a la implantación de señuelos y trampas, puesto que ya conocen el funcionamiento del sistema. Los enmascarados deben detectarse mediante el análisis de los patrones de conducta en el plano informático; es decir, un enmascarado está suplantando una identidad, por lo que se podrá detectar en la medida en que el comportamiento sea diferente del usuario original (frecuencia de clics, movimientos del ratón, búsquedas…) (Maestre y García, 2014). De esto hablan Gunter, Liebovitz y Malin (2011) con el EBAM o gestión de acceso basado en la experiencia, que se basa en el patrón de utilización de ciertas características del sistema.

3.3.1. El factor humano en la detección

Hay otros autores que defienden la importancia del factor humano en la prevención y detección de *insider* potenciales.

Silvius y Dols (2012) elaboraron un test para medir el comportamiento de incumplimiento mediante cinco dimensiones: descuido, inconsciente, control estricto de tecnologías, cultura y mala alineación entre tecnologías y necesidades; empleando entre dos y tres ítems para cada una. Además, añadieron otra escala compuesta de siete ítems para comprobar si en algún momento el trabajador había realizado este tipo de comportamiento a lo largo de su trayectoria; y otra con cinco ítems sobre el trabajador y su entorno de trabajo.

El cuestionario fue completado por trabajadores de grandes empresas de Holanda y Bélgica, y sus resultados mostraban que, aunque la mayoría de los trabajadores sabían y cumplían con la normativa de seguridad, alguna vez habían pasado por alto estas medidas para conseguir terminar sus tareas. También fueron muchos los que admitieron no tener problema en saltarse las normas de seguridad si su jefe se lo pidiera.

Sin embargo, no se encontró apenas correlación entre los factores medidos y el uso de dispositivos USB sin seguridad, el envío de información confidencial al correo personal o el teletrabajo, permitiendo suponer que los trabajadores aún no están concienciados del peligro que pueden suponer estos aspectos para la seguridad de la información de la empresa.

Casi todos los métodos de detección se basan en las nuevas tecnologías (*machine learning*, almacenamiento de información, patrón de comportamiento informático), pero no se pueden dejar de lado otros caminos que pueden acercar, de manera complementaria a lo que ya se hace, a la identificación de un *insider*. Es por eso que no se debe desestimar una posible vía en los aspectos psicológicos.

3.4. Factores psicológicos y personalidad

Actualmente se cuenta con mucha información acerca de los diferentes tipos de *insider*, su patrón de actuación y formas de detección. También se ha tratado de dar explicación en función de ciertos indicadores psicológicos. Por ejemplo, Terpstra, Rozell y Robinson (1993) realizaron un estudio en el que se observó una correlación negativa entre comportamiento ético y competitividad y locus de control externo. Por otra parte, encontraron correlación positiva entre dicho comportamiento y la edad, así como con el sexo femenino. También se ha relacionado este comportamiento con la llamada Tríada Oscura, compuesta por las dimensiones de maquiavelismo, psicopatía y narcisismo (Paulhus y Williams, 2002).

Nurse et al. (2014b) hacen hincapié en la importancia de ciertas variables psicológicas a la hora de presentar un motivo para llevar a cabo acciones relacionadas con el *insider trading*, tal y como se ha mencionado anteriormente. Estos autores ponen de manifiesto la relevancia no solo de las características, sino de los estados psicológicos. De esta forma, las personas más propensas a cometer un ataque serían aquellas que estuvieran bajo un mayor nivel de estrés (Turner y Gelles, 2006). También tienen una gran importancia los posibles eventos que, por su carga emocional, supongan un desencadenante de este tipo de conducta (Claycomb et al., 2012). Por ejemplo, la circulación de ciertos rumores que, en caso de ser ciertos, podrían comprometer la estabilidad del puesto de trabajo del empleado.

Otro factor de riesgo es el historial de comportamiento (Nurse et al., 2014a), entendiendo como tal los desórdenes mentales, adicciones, o la actitud respecto al lugar de trabajo y sus normas (CPNI, 2013, citado en Nurse et al., 2014b). Por una parte, hay trabajadores que no siguen dichas reglas o no son conscientes de las mismas, lo que puede hacer que se conviertan en un *insider* negligente. Por otra parte, muchos de los ataques intencionados son perpetrados por los llamados empleados disgustados. Esta figura es la del trabajador que siente que no se le ha tratado de manera justa dentro de la empresa y, por tanto, decide utilizar información privilegiada para perjudicarla (Holton, 2009).

Sin embargo, los autores aclaran que todas estas características están ligadas a un tipo de ataque específico, y que no se pueden tomar al pie de la letra de forma aislada. Son únicamente indicadores que pueden ayudarnos a predecir la tendencia de una persona a convertirse en un *insider* malicioso.

Siguiendo esta línea, Gunter et al. (2011) han teorizado acerca de un sistema que permitiera asignar a los trabajadores un cierto nivel de confianza, para así poder relacionarlo con el control de acceso a la información. Es decir, aquellos cuyo nivel de confianza sea mayor serán los que tengan acceso a los datos privilegiados de la empresa.

Sin embargo, en nuestra revisión no hemos detectado que se haya indagado sobre si existe o no un patrón de personalidad o rasgos psicológicos que hagan a una persona más propensa a convertirse en este tipo de amenaza según uno de los modelos clásicos. La única evidencia que se ha encontrado es la mayor representación de carreras relacionadas con la programación y los ordenadores por parte de individuos introvertidos (Pocius, 1991).

También Brown, Greitzer y Watkins (2013) llevaron a cabo un estudio experimental relacionando factores lingüísticos con el Big Five, y estudiaron posteriormente el patrón de tres *insider* maliciosos. Tomaron una muestra de 6.3 millones de palabras, agrupadas en 52116 mensajes de 150 ejecutivos. Tras analizar dichos mensajes, concluyeron que el neuroticismo, la cordialidad y la responsabilidad guardaban relación con la frecuencia de aparición de ciertas categorías de palabras. Encontraron la correlación más positiva entre

neuroticismo y la expresión de emociones negativas, ansiedad e ira; así como entre cordialidad y la mayor utilización de la primera persona del plural, los números y expresiones referentes al ocio. Por otra parte, responsabilidad correlaciona negativamente con la mayor expresión de emociones negativas e ira. Tras encontrar estos resultados, midieron los rasgos de tres casos de *insider* malicioso. Dos de ellos presentaron una alta puntuación en neuroticismo, pero otra extremadamente baja en responsabilidad; el tercero obtuvo un nivel medio en ambos rasgos, pero su puntuación en cordialidad fue bastante baja.

Sin embargo, esta información no es suficiente para poder sacar conclusiones, por lo que para realizar una primera aproximación al problema de la fuga de información privilegiada desde la psicología de la personalidad se ha empleado el modelo de personalidad de Eysenck, ya que es el más sencillo de cara a relacionarlo posteriormente con los distintos tipos de *insider*. Este modelo reconoce tres rasgos básicos de personalidad: extraversión, neuroticismo y psicoticismo (Eysenck, 1970).

Extraversión: lo que caracteriza a una alta puntuación en este rasgo es la infra-activación del córtex cerebral. Es por esto que las personas más extravertidas tenderán a buscar estimulación en el medio que les rodea mediante la realización de diversas actividades que permitan aumentar su arousal cortical. De esto se deriva la mayor probabilidad que sean más habladores y se rodeen de más gente que las personas introvertidas. También suelen ser más asertivos y dominantes en sus relaciones.

Neuroticismo: este rasgo hace referencia a la inestabilidad emocional. Se rige por el sistema límbico: el hipotálamo conecta con el Sistema Nervioso Autónomo, lo que permite la reacción emocional; el hipocampo, por su parte, almacena recuerdos emocionales.

Las personas con una alta puntuación en neuroticismo reaccionarán emocionalmente de manera más intensa ante los estímulos, por lo que serán personas que se conmuevan con mayor facilidad y tenderán a darle mayor importancia a cualquier situación durante más tiempo.

Además, esta emocionalidad hace que el neuroticismo actúe como modulador de los otros dos rasgos, suavizando las reacciones cuando la puntuación es baja, pero intensificándolas cuando es alta (de Juan y García, 2004).

Psicoticismo: es el continuo que comprende las puntuaciones relativas a la dureza afectiva. A pesar de que, en general, se vincula con la poca activación amigdalar, dentro de este rasgo existen tres subdimensiones relacionadas con otras partes concretas del cerebro: psicoticismo primario, secundario y Disociativo (Corr, 2010).

El primero es el que está más directamente relacionado con la baja actividad de la amígdala. Se asocia con el eje afectivo-interpersonal, por lo que presenta características como la independencia afectiva, la baja empatía o la frialdad. En general, todo lo relativo al desapego afectivo.

El psicoticismo secundario tiene que ver con un exceso de dopamina, lo que correlaciona negativamente con la activación del córtex orbitofrontal. Esta área es la encargada de llevar a cabo las decisiones tomadas, por lo que una baja activación provocará comportamientos impulsivos, agresivos y temerarios.

Por último, las personas con un alto psicoticismo disociativo se caracterizan por su excentricidad tanto en su físico como en su forma de pensar y lenguaje, por su desconfianza y por sus extrañas relaciones sociales. La baja activación dorsolateral parece ser la responsable de las puntuaciones altas en esta subdimensión, ya que está implicada en la valoración de la situación y permite elegir entre diferentes opciones.

3.4.1. Personalidad y motivación.

Por otra parte, el estudio de Gray (1981) enlaza los factores de personalidad de Eysenk con tres sistemas motivacionales: Behavioral Activation System (BAS), Behavioral Inhibition System (BIS) y el Fly-Fight System (FFS).

Behavioral Activation System: se trata de un sistema motivacional guiado por un drive apetitivo, por lo que busca un refuerzo positivo. El rasgo asociado a este sistema es la extraversión y el psicoticismo secundario, por lo que las personas que puntúen alto tenderán a realizar acciones encaminadas a la consecución del mencionado refuerzo. Además, las personas con un mayor predominio del BAS son aquellas con alta puntuación tanto en extraversión y psicoticismo como en neuroticismo, puesto que este último rasgo intensificaría las consecuencias de los otros dos.

Behavioral Inhibition System: se rige por un drive evitativo, siendo contrario al BAS. Está orientado a evitar una consecuencia negativa, un daño, por lo que busca un refuerzo negativo. Es por eso que es el sistema que predomina en las personas introvertidas, sobre todo si tienen un neuroticismo alto. No sólo porque actúe como modulador, tal y como se ha mencionado anteriormente, sino porque está relacionado con la ansiedad anticipatoria.

Fly-Fight System: este sistema corresponde al llamado "instinto de supervivencia", orientado a salvar la propia vida mediante conductas de huida (fly) y ataque (fight). El rasgo más representativo del FFS es el psicoticismo. Una persona con alto psicoticismo, al presentar una mayor temeridad, tenderá a llevar a cabo conductas de ataque ante una situa-

ción de peligro. Sin embargo, las personas con bajo psicoticismo presentarán una tasa mayor de conductas de huida ante las mismas situaciones.

Estos tres sistemas actúan en conjunto en cada individuo, presentando una activación diferente en función de los rasgos básicos de personalidad en cada caso. No obstante, que predomine un sistema motivacional sobre los otros no quiere decir que simplemente actúe ese, sino que lo hará con mayor fuerza. Un claro ejemplo es el de las personas con alta puntuación en los tres rasgos: la impulsividad del psicoticismo junto a la búsqueda de sensaciones de la extraversión hace que se busque un refuerzo positivo (BAS), a lo que se suma la intensidad proporcionada por el neuroticismo. Pero, por otra parte, ese mismo neuroticismo hace que aparezca el sentimiento de ansiedad, y de culpa en caso de llevar a cabo la acción finalmente (BIS).

Teniendo en cuenta toda la información recabada acerca de los factores psicológicos y cómo se pueden relacionar con un tipo concreto de *insider*, se podría hipotetizar acerca de un posible vínculo entre estos rasgos de personalidad y el riesgo de filtrar datos privilegiados. Es por eso que, en el siguiente apartado, se expondrán las diferentes hipótesis y las posibles aplicaciones que podría tener una futura investigación siguiendo esta línea.

4. Conclusiones

Una vez revisados los puntos importantes acerca del *insider trading* y la personalidad, queda por exponer la aplicación que pueda tener la posible relación entre ellos. Unido a todos los métodos de detección anteriores, el conocimiento del patrón de personalidad de los trabajadores de una empresa podría ayudar a identificar quiénes son más susceptibles de convertirse en un *insider* y, más concretamente, de qué tipo. Cabe destacar que estos indicadores tienen que ver con un mayor o menor riesgo de cometer *insider trading*, sin que ello implique certeza de comisión de la actividad; es decir, que alguien presente una mayor tendencia no quiere decir que vaya a filtrar información necesariamente, al igual que un menor riesgo no exime de esa posibilidad.

Tras analizar la bibliografía, se ha encontrado una gran convergencia de ciertos aspectos de la personalidad que corresponden al perfil de *insider* malicioso. Un buen candidato a la hora de detectar el riesgo de este tipo de actividad podría ser el psicoticismo, ya que sus características coinciden, en gran medida, con los aspectos ya expuestos. Tal y como se ha mencionado anteriormente, los expertos coinciden en que la ausencia de valores morales es uno de los orígenes de la práctica del *insider trading* (Díaz, 2015); así como otros factores como la Tríada Oscura (Maasberg, Warren y Beebe., 2015). Si relacionamos todo esto con los rasgos propuestos por Eysenck, se puede observar una gran similitud con el concepto de psicoticismo primario.

Si se une este rasgo a una alta estabilidad emocional, podríamos estar ante un ingeniero social, puesto que son personas que tienen una gran dureza afectiva al perseguir la obtención de información privilegiada mediante métodos poco éticos, sin importarles lo que puedan llegar a sentir los trabajadores objetivo.

Por otra parte, un empleado con puntuaciones altas tanto en neuroticismo como en psicoticismo podría ser más propenso a cometer acciones de *insider trading* debido a un motivo de venganza. Probablemente este filtrado de información se produciría poco después a un evento desencadenante de este deseo, ya que las personas con este tipo de patrón de personalidad suelen ser muy impulsivas, algo que se agravaría si se le suma una alta extraversión.

En el caso de los *insider* negligentes no tenemos información que relacione la fuga de datos privilegiados con algún factor psicológico. No obstante, analizando las características de este tipo de *insider* junto con las de los rasgos de personalidad, se podría hipotetizar acerca de la relación entre una mayor tendencia a presentar conductas referentes a la fuga de información y altas puntuaciones en estabilidad emocional y extraversión. Es probable que este tipo de personas no piensen en el peligro que pueden conllevar sus acciones o, que simplemente, se salten el protocolo de seguridad para evitar aburrirse.

Sin embargo, los bienintencionados probablemente tendrán un mayor neuroticismo, al estar relacionado con el sentido de la responsabilidad y la autoexigencia. Si, además, se junta con un psicoticismo primario por encima de la media, el riesgo podría verse incrementado al existir un factor relacionado con el egocentrismo. No obstante, su actitud respecto a la empresa debería ser positiva, de forma que quisiera rendir más para reportarle un beneficio.

Resumiendo estas ideas, se pueden plasmar en cinco hipótesis diferenciadas:

1. Las personas con altas puntuaciones en psicoticismo presentarán una mayor tendencia a cometer acciones correspondientes a las que llevaría a cabo un *insider* malicioso.

2. Los ingenieros sociales tendrán alta puntuación en psicoticismo, pero baja en neuroticismo.

3. Los empleados más impulsivos, relacionados con altas puntuaciones en los tres rasgos, serán más proclives a filtrar información privilegiada de su empresa poco después de un evento que les genere un deseo de venganza.

4. Una persona con baja puntuación en neuroticismo, pero alta en extraversión, podría comprometer la seguridad de

los datos de su compañía con mayor probabilidad al no seguir la normativa.

5. Los empleados con actitud positiva hacia su empresa que presenten un alto neuroticismo y puntuaciones por encima de la media en psicoticismo tendrán mayor riesgo de cometer acciones relacionadas con las de un *insider* bienintencionado.

Aplicaciones

El perfilado de la personalidad de los trabajadores de una empresa puede servir, como ya se ha mencionado, para detectar *insider* potenciales y prevenir posibles ataques internos perpetrados por estos empleados. Sin embargo, cabe preguntarse: ¿cómo?

En primer lugar, en un proceso de selección. Hay ciertos puestos de trabajo que requieren un especial cuidado a la hora de escoger a la persona idónea por la responsabilidad que conlleva. Dicha responsabilidad puede tener relación con el manejo de información privilegiada. Es por eso que, a la hora de evaluar a un candidato, se podría implantar en el proceso una fase consistente en un test de personalidad. Esto podría ayudar a saber de antemano quiénes serían más susceptibles de convertirse en un tipo específico de *insider*. Esta información podría facilitar tanto la propia selección para detectar ciertas conductas como seguimiento del nuevo trabajador.

Este problema también puede abordarse desde el departamento de formación. Se podrían organizar jornadas relacionadas con el *insider trading* desde dos puntos de vista. Por un lado, desde la educación en las normas relacionadas con la seguridad de los datos de la compañía, intentando así reducir los casos de fuga de información por *insider* tanto negligentes como bienintencionados. Por otro lado, fomentando la lealtad hacia la entidad. En este caso, se podría dividir a los distintos empleados por grupos en función de su patrón de personalidad, de forma que se pueda adaptar el discurso a los interlocutores.

Estas jornadas formativas también pueden enfocarse desde otra perspectiva: cómo evitar ser víctima de los ingenieros sociales. En función de la tendencia psicológica de cada empleado, se pueden aprovechar estos grupos ya mencionados para hacer hincapié en aquellos aspectos que podrían hacer que, en un determinado momento, sean más susceptibles de comunicar datos privilegiados a este tipo de personas. Por ejemplo, un grupo con puntuaciones bajas en extraversión y psicoticismo, pero altas en neuroticismo, es probable que decidan comunicar información por motivos de culpa o de lealtad hacia una persona determinada; mientras que una persona con un psicoticismo muy alto podría hacerlo por demostrar su valía.

Por otra parte, en las reuniones de seguimiento que se realizan en las empresas, se puede hacer hincapié en aspectos que podrían tener que ver con un posterior intento de *insider trading*, como puede ser la satisfacción con el trato por parte de la compañía o con las tareas a desempeñar. Una vez detectado el problema, se podría intentar satisfacer las necesidades del empleado que hacen que el riesgo de fuga de información se incremente. Por ejemplo, si las funciones que ha de llevar a cabo son extremadamente aburridas para él y esta persona tiene un alto psicoticismo, tal vez darle tareas que requieran una mayor carga de trabajo y le gusten más contribuya a reducir la posibilidad de que indague acerca de cómo conseguir datos privilegiados, ya sea por puro aburrimiento o por sentir que la empresa infravalora sus capacidades.

Además de tener aplicaciones para la detección temprana de los *insider* potenciales, también podría ayudar a optimizar el proceso de localización del empleado una vez ha filtrado la información privilegiada, con el fin de detener esta fuga y tomar las medidas pertinentes. En este caso, la empresa debería fijarse en el rastro informático que el *insider* haya podido dejar, ya que podría ser indicativo de un mayor o menor nivel de neuroticismo. Al igual que en los análisis criminológicos de escenarios de crímenes y criminales el escenario puede ser organizado, desorganizado o mixto (Burgess, Burgess, Douglas y Ressler, 1997).

Un escenario organizado es aquel que muestra signos de haber sido manipulado después de la comisión del delito, normalmente para ocultar sus acciones o dificultar la actuación posterior de las autoridades pertinentes. El escenario desorganizado es el que no ha sido manipulado, por lo que presenta evidencias de los actos llevados a cabo. Finalmente, el escenario mixto es el que muestra ciertos signos de manipulación.

Es probable que estos conceptos se puedan aplicar a los rastros informáticos después del acceso y/o difusión de información privilegiada en el caso del *insider* malicioso. Ciertas personas optarán por volver a su puesto de trabajo o a sus labores anteriores lo antes posible de forma que nadie pueda sorprenderlos en esta tarea, mientras que otras tardarán más en hacerlo con el fin de eliminar cualquier tipo de evidencia de la misma.

Esto también es posible relacionarlo con la personalidad de una persona, concretamente con el neuroticismo. Puntuaciones altas en este rasgo implican una mayor ansiedad anticipatoria ante los sucesos, por lo que serán personas que tiendan a dejar un escenario desorganizado o mixto esperando que nadie note sus acciones. Por otra parte, personas con un menor nivel de neuroticismo serán más propensos a tardar más en finalizar el *insider trading* al invertir tiempo

en tratar de eliminar cualquier tipo de rastro que pueda involucrarle con este filtrado de información, dejando un escenario organizado.

Por tanto, esta información podría ayudar a reducir el foco de observación, acotándolo a ciertos trabajadores. No obstante, esto solo se debe tratar como un indicador, siendo totalmente inviable utilizarlo aisladamente o como única prueba, ya que la disposición del escenario es un continuo y puede depender de otros factores tales como la habilidad del empleado. Es decir, puede ocurrir que una persona intente manipular por completo el rastro de información referente al *insider trading*, pero no le sea posible debido a una carencia de conocimientos relacionados con el sistema informático.

A pesar de todas las hipótesis planteadas, en este estudio se han encontrado algunas limitaciones. En primer lugar, la tipología de la bibliografía encontrada: gran parte de la misma pertenece al campo de la ingeniería informática, lo que dificultó la comprensión de ciertos artículos y técnicas expuestas en los mismos. Por otra parte, al no haber encontrado literatura que relacionase el estudio de Eysenck con el *insider trading*, no se ha podido contar con un referente. Es por esto que las hipótesis son tentativas, y puede abrir la puerta a nuevas investigaciones experimentales.

En conclusión, no cabe duda de que la fuga de información privilegiada es un gran problema para las empresas hoy día. Por eso es necesario atajarlo de la manera más eficiente y eficaz posible, lo cual solo se puede conseguir desde una perspectiva multidisciplinar. Es preciso unir toda la investigación con la que contribuye la ingeniería informática con todo lo que puede aportar la psicología, de forma que se pueda alcanzar este objetivo de reducir los casos de *insider trading*. Esto no solo reportaría un beneficio a las compañías, sino también a sus trabajadores.

5. Referencias

Bellovin, S. M. (2008). The Insider Attack Problem Nature and Scope. En Bellovin, S. M., Hershkop, S., Keromytis, A. D., Salvatore, J., Smith, S. W., Sinclair, S. y Stolfo, J. (Eds.), *Insider Attack and Cyber Security: Beyond the Hacker* (pp. 1-2). Nueva York: Springer.

Burgess, A., Burgess, A., Douglas, J., y Ressler, R. (1997) *Crime Classification Manual*. San Francisco: Jossey-Bass, Inc.

Claycomb, W. R., Huth, C. L., Flynn, L., McIntire, D. M., Lewellen, T. B., y Center, C. I. T. (2012). Chronological examination of insider threat sabotage: preliminary observations. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, *3*(4), 4–20.

Corr, P. J. (2010) The psychoticism–psychopathy continuum: A neuropsychological model of core deficits. *Personality and Individual Differences, 40, 695-703*.

de Juan Espinosa, M., y García Rodríguez, L.F. 2004. *Nuestra personalidad: En qué y por qué somos diferentes*. Madrid. Biblioteca Nueva.

Díaz, M. (2015). Estudio Empírico Sobre El Insider Trading En España. *Contribuciones a la Economía*. Recuperado de http://eumed.net/ce/2015/1/insider-trading.html

Eysenck, H. J. (1970). *The structure of human personality* (3.ª Ed.). Londres: Mathuen.

Garfinkel, S. L., Beebe, N., Liu, L., y Maasberg, M. (2013). Detecting threatening insiders with lightweight media forensics. *Technologies for Homeland Security (HST)* (86-92).

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

Gunter C., Liebovitz D., and Malin B. (2011) Experience-Based Access Management: A Life-Cycle Framework for Identity and Access Management Systems. *IEEE Security and Privacy Magazine*, *9*(5), 48-55.

Holton, C. (2009). Identifying disgruntled employee systems fraud risk through text mining: A simple solution for a multi-billion dollar problem. *Decision Support Systems*, *46*(4), 853-864.

Huerta, P. (2001). El Insider Trading y el uso de la información privilegiada. *Derecho y Sociedad*, *17*, 171-179.

Huth, C. L., Chadwick, D. W., Claycomb, W. R., y You, I. (2013). Guest editorial: A brief overview of data leakage and insider threats. *Information Systems Frontiers*, *15*(1), 1-4.

insider. (n.d.). *Dictionary.com Unabridged*. Retrieved March 17, 2018 from Dictionary.com website http://www.dictionary.com/browse/insider

Khorshed, M. T., Ali, A. S., y Wasimi, S. A. (2011). Monitoring insiders activities in cloud computing using rule based learning. *Trust, Security and Privacy in Computing and Communications (TrustCom)* (757-764).

Koch, R., y Dreo Rodosek, G. (2010). User identification in encrypted network communications. *Network and Service Management (CNSM)* (246-249).

Maasberg, M., Warren, J., y Beebe, N. L. (2015). The dark side of the insider: detecting the insider threat through examination of dark triad personality traits. *System Sciences (HICSS)* (3518-3526).

Maestre, J., y García, L. J. (septiembre, 2014). *Sistema de Deteccion de Atacantes Emascarados Basado en Técnicas de Alineamiento de Secuencias*. Trabajo presentado en la conferencia RECSI XIII: Actas de la XIII Reunión Española sobre Criptología y Seguridad de la Información. Alicante.

Marcus B. and Schuler H. (2004). Antecedents of counterproductive behavior at work: a general perspective. *Journal of Applied Psychology*, 89 (4), 647.

Melnikov, N., y Schönwälder, J. (2010). Cybermetrics: user identification through network flow analysis. *IFIP International Conference on Autonomous Infrastructure, Management and Security* (167-170).

Mena, J. (2011). *Machine learning forensics for law enforcement, security, and intelligence* (p. 1). Nueva York: Auerbach Publications.

Moore, A. P., Cappelli, D., Caron, T. C., Shaw, E. D., Spooner, D., y Trzeciak, R. F. (2011). A preliminary model of insider theft of intellectual property. *Carnegie Mellon University*.

Nurse, J. R., Buckley, O., Legg, P. A., Goldsmith, M., Creese, S., Wright, G. R., y Whitty, M. (2014). Understanding insider threat: A framework for characterising attacks. *Security and Privacy Workshops (SPW)* (214-228) (a).

Nurse, J. R., Legg, P. A., Buckley, O., Agrafiotis, I., Wright, G., Whitty, M., ... y Creese, S. (2014). A critical reflection on the threat from human insiders–its nature, industry perceptions, and detection approaches. *International Conference on Human Aspects of Information Security, Privacy, and Trust* (270-281) (b).

Sharif, M., Faiz, T., y Raza, M. (2008). Time signatures-an implementation of keystroke and click patterns for practical and secure authentication. In *Digital Information Management* (559-562).

Silvius, A. G., y Dols, T. (2012). Factors influencing Non-Compliance behavior towards Information Security Policies. *CONF-IRM* (39).

Turner, J. T. y Gelles, M. (2012). *Threat assessment: A risk management approach*. Routledge.

Rybnik, M., Panasiuk, P., y Saeed, K. (2009). User authentication with keystroke dynamics using fixed text. *Biometrics and Kansei Engineering* (70-75).

Paulhus D. L. y Williams K. M. (2002). The Dark Triad of Personality: Narcissism, Machiavellianism, and Psychopathy. *Journal of Research in Personality*, *36*(6), 556–563.

Peltier, T. R. (2006). Social engineering: Concepts and solutions. *Information Security Journal*, *15*(5), 13.

Pfleeger, C. P. (2008). Reflections on the Insider Threat. En Bellovin, S. M., Hershkop, S., Keromytis, A. D., Salvatore, J., Smith, S. W., Sinclair, S. y Stolfo, J. (Eds.), *Insider Attack and Cyber Security: Beyond the Hacker* (pp. 1-2). Nueva York: Springer.

Pocius, K. E. (1991). Personality factors in human-computer interaction: A review of the literature. *Computers in Human Behavior*, *7*(3), 103-135.

Prado, A. (2002). Acerca del concepto de información privilegiada en el mercado de valores chileno: su alcance, contenido y límites. *Revista Chilena de Derecho*, *30*, 237.

Real Academia Española. (2017). *Diccionario de la lengua española* (22.ª ed.). Consultado en http://dle.rae.es/?w=diccionario

Terpstra, D. E., Rozell, E. J., y Robinson, R. K. (1993). The influence of personality and demographic variables on ethical decisions related to insider trading. *The Journal of Psychology*, *127*(4), 375-389.

Wall, D. S. (2013). Enemies within: Redefining the insider threat in organizational security policy. *Security journal*, *26*(2), 107-124.

Willison, R., y Warkentin, M. (2013). Beyond Deterrence: An Expanded View of Employee Computer Abuse. *MIS Quarterly*, *37*(1), 1–20.

Real Academia Española (2018). Definición de Red Social. Recuperado de http://dle.rae.es/?id=VXs6SD8 [Fecha de acceso 8 abril 2018].

Ross, C., Orr, E. S., Sisic, M., Arseneault, J. M., Simmering, M. G., y Orr, R. R. (2009). Personality and motivations associated with Facebook use. *Computers in human behavior*, *25*(2), 578-586. doi: 10.1016/j.chb.2008.12.024

Ryan, T., y Xenos, S. (2011). Who uses Facebook? An investigation into the relationship between the Big Five, shyness, narcissism, loneliness, and Facebook usage. *Computers in human behavior*, *27*(5), 1658-1664. doi: 10.1016/j.chb.2011.02.004

Swider, B. W., y Zimmerman, R. D. (2010). Born to burnout: A meta-analytic path model of personality, job burnout, and work outcomes. *Journal of Vocational Behavior*, *76*(3), 487-506. doi: 10.1016/j.jvb.2010.01.003

Wald, R., Khoshgoftaar, T., y Sumner, C. (2012). Machine prediction of personality from Facebook profiles. *2012*

IEEE 13th International Conference on Information Reuse and Integration, 109-115. doi: 10.1109/IRI.2012.6302998

We Are Social. (2018). *Digital in 2018: World's internet users pass the 4 billion mark - We Are Social.* [online] Recuperado de: https://wearesocial.com/blog/2018/01/global-digital-report-2018 [Fecha de acceso 8 abril 2018].