



Borja González, abogado de Gómez-Acebo & Pombo



Bruce Goslin, socio de K2 Global



Félix Alarcón, director de RR.HH. de Wolters Kluwer



Guzmán de Aguilar, socio director de Piniés & Aguilar



José Antonio Carazo, director de Capital Humano



Lucía Andrés, directora asociada del Career Management Centre del IE Business School

# Una cultura fuerte es la mejor protección de la información confidencial

La seguridad de la información es una de las grandes preocupaciones de las empresas actualmente. Perder información puede suponer un daño comercial, pero también reflejará en el mercado una mala imagen para la empresa. Existen medidas legales y tecnológicas para proteger la información, pero las políticas de transparencia y confianza en los empleados pueden hacer más difícil el control. Un grupo de profesionales reunidos por Capital Humano, en colaboración con K2 Global Consulting, han debatido sobre este tema. Estas son sus conclusiones.

Redacción de Capital Humano.





COMENTE ESTE  
ARTÍCULO EN

[www.capitalhumano.es](http://www.capitalhumano.es)

## FICHA TÉCNICA

**Autor:** Redacción de Capital Humano

**Título:** Una cultura fuerte es la mejor protección de la información confidencial.

**Resumen:** ¿Qué es lo que se puede hacer evitar la pérdida de información sensible en una empresa? ¿Se puede dejar de poner a disposición de los empleados toda la información suficiente para que puedan desarrollar su trabajo? ¿Qué información y qué formación se les debe dar? ¿Cómo se puede crear una cultura de la responsabilidad dentro de las empresas para que no haya filtraciones? Para tratar de resolver estas y otras cuestiones Capital Humano ha organizado un coloquio con profesionales, en colaboración con la consultora K2 Global. Los participantes destacaron que la seguridad de la información se ha convertido en un aspecto crítico, no solo por proteger la información sensible, sino para evitar la mala imagen en el mercado que produce el que una empresa no sea capaz de evitar las fugas de información estratégica. Para evitar que esto suceda hay mecanismos de prevención y control tanto legales como tecnológicos, pero no siempre son suficientes. La cultura de la organización puede ser el mejor mecanismo de seguridad.

**Descriptores:** Cultura Corporativa / Reputación / Información para la Gestión

**Localizador en el buscador de la web:** DT0000181652



Ignacio Mazo, socio  
director de BTS



Lorena Martínez, directora  
asociada del Career Management  
Centre del IE Business  
School



Miguel Ángel Zull, socio de Boyden



Rafael Cabarcos, experto  
en RR.HH.



Ramón Bartolomé, socio de Boyden



**L**a seguridad de la información se ha convertido en un aspecto crítico de las empresas. No solamente por proteger su información sensible y evitar su uso por los competidores, sino por evitar la mala imagen que puede producir en el mercado el hecho de que una empresa no sea capaz de evitar las fugas de información estratégica. Para evitar que esto suceda hay mecanismos de prevención y control tanto legales como tecnológicos, pero no

siempre son suficientes. Las normas y los protocolos de actuación son importantes, pero tanto o más lo son los comportamientos de los empleados. Y esto es una cuestión cultural.

¿Qué es lo que se puede hacer para evitar una situación de riesgo en la pérdida de la información? ¿Se puede dejar de poner a disposición de los empleados toda la información suficiente para que puedan desarrollar >

- su trabajo? ¿Y si no se les da podrán hacer su trabajo? ¿Qué información y qué formación se debe dar a los empleados? ¿Cómo se puede crear una cultura de la responsabilidad dentro de las empresas para que no haya filtraciones? Para tratar de resolver estas y otras cuestiones Capital Humano ha organizado, en colaboración con la consultora K2 Global<sup>1</sup>, un coloquio en el que han participado profesionales de la empresa y la consultoría.

Los participantes en el coloquio fueron: Bruce Goslin, socio de K2 Global; Félix Alarcón, director de Recursos Humanos de Wolters Kluwer; Rafael Cabarcos, experto

1 K2 Global Consulting ofrece servicios de consultoría y asesoría de riesgos para corporaciones multinacionales, Estados soberanos y clientes particulares. Sus principales líneas de negocio incluyen estrategias y soluciones contra el fraude y la corrupción, asesoramiento en transacciones, resolución de disputas y estrategias de seguridad. K2 Global Consulting forma parte de K2 Global Partners LLC, una empresa privada fundada en el 2009 por Jules Kroll y Jeremy Kroll. K2 está enfocada en nuevos negocios en el ámbito de gestión de riesgos e incluye también Kroll Bond Ratings, una nueva agencia de calificación crediticia especializada en los productos financieros estructurados.

en RR.HH; Ignacio Mazo, socio director de BTS; Ramón Bartolomé y Miguel Ángel Zuñil, socios de Boyden; Borja González, abogado de Gómez-Acebo & Pombo; Lorena Martínez y Lucía Andrés, directoras asociadas del Career Management Centre del IE Business School; y Guzmán de Aguilar, socio director de Piniés & Aguilar. La moderación de los debates correspondió a José Antonio Carazo, director de Capital Humano.

## PREVENCIÓN Y CONTROL

Abrió el debate Bruce Goslin, asegurando que la gestión de la seguridad tiene varios aspectos: "Uno es si tenemos que intervenir en una empresa en la que ha habido una fuga de información que haya provocado la pérdida una ventaja comercial. Otra cuestión es que la fuga de información se produzca cuando una persona deja una



empresa, se va a la competencia y empieza a rivalizar con la información que se ha podido llevar. Con frecuencia nos encontramos con situaciones complicadas porque las empresas esperan hasta el último minuto para protegerse. Muchas empresas ponen cláusulas a sus directivos sobre la propiedad de la información o para impedirles durante un tiempo trabajar en el mismo sector o utilizar sus contactos. Hay ciertas medidas que permiten controlar hasta cierto punto”, argumentó.

En su experiencia, la aproximación de su firma a estos incidentes es muy investigativa: quiénes fueron los responsables, cómo lo hicieron, qué recursos legales o financieros hay para la empresa afectada, cómo podemos parar la actividad para que no haya más fugas, cómo podemos actuar con las personas que se llevaron la información...

Miguel Ángel Zuñil, socio de Boyden, empezó por plantear si existen políticas que definen lo que es información sensible y si existe algún protocolo de protección. “Cuanto mayor sea lo que entendamos por información sensible mayor será el espectro que tendremos que proteger y, por tanto, mayor será el

alcance del blindaje para que esa información quede protegida e impedir que la empresa pueda verse perjudicada sin impedir el normal desarrollo de su actividad. El tema es saber qué vamos a proteger”, puntualizó.

A esta cuestión, Borja González, abogado de Gómez-Acebo & Pombo, comentó que “desde el punto de vista jurídico-laboral hay un aspecto fundamental para controlar que no haya fuga de información y es respetar el derecho a la intimidad. Lo que se suele hacer es establecer políticas de uso de los medios informáticos y los trabajadores tienen que estar informados de esas políticas, de cómo les puede controlar la compañía. Esta es la parte de la prevención. Luego hay que definir qué es información confidencial y establecer las cláusulas que correspondan en los contratos. Por mi experiencia la mayor parte de las cláusulas que se suelen incluir en los contratos no son válidas. Hay unos requisitos legales que no se suelen tener en cuenta, como que debe haber una compensación, que tiene que

haber un efectivo interés por parte de la compañía, que tiene que fijarse una duración máxima. Son tres aspectos legales que se deben tener en cuenta para el control de la información confidencial por parte de la compañía”. Y llamó la atención sobre la dificultad de plantear ante un tribunal un conflicto por uso de información confidencial: “No es tan crítico categorizar la información como definir qué es confidencial”.

## INFORMACIÓN Y TRANSPARENCIA

Para Ignacio Mazo, socio director de BTS, es fundamental definir por parte de la empresa qué es información confidencial y sensible. “Para que una compañía consiga éxitos tiene que ser capaz de ejecutar una estrategia y para ejecutar esta estrategia tiene que ser conocida como

mínimo por parte de sus empleados. Hay que establecer una jerarquía de datos, información y conocimiento. El dato por sí solo no tiene valor. Necesita un contexto en el que esa información tenga valor y que la persona que la posea tenga criterio para interpretarla”. Félix Alarcón, director de RR.HH. de Wolters Kluwer, recordó que

### La seguridad de la información es un aspecto crítico para evitar la mala imagen que produce una empresa incapaz de contener fugas de datos estratégicos

“el paradigma ha cambiado. Antes quien tenía la información tenía el poder. Ahora tiene el poder quien maneja la información adecuadamente y quien diseña y ejecuta la estrategia de forma correcta”.

Ramón Bartolomé, socio de Boyden, partió de otro planteamiento: “Imaginemos que hemos definido bien cuál es la información sensible. Yo me quedaría con dos indicadores, uno es la prevención y el otro es el control. La cuestión será hasta qué punto somos capaces de crear mecanismos de prevención con las nuevas tecnologías disponibles para anticiparse a posibles escenarios de riesgo. El control molesta al ser humano, por tanto hay que plantear una estrategia para que en lugar de controlar la gente participe voluntariamente en un proyecto corporativo con honestidad”.

Rafael Cabarcos, con una gran experiencia de gestión en grandes compañías, expuso otro punto de vista: “Hay ata->



ques internos y externos. Yo creo que las compañías no se protegen igual de las posibles malas prácticas de sus empleados como de los ataques que vienen del exterior. Cuando se produce un ataque estamos ante un delito, pero antes de llegar a esta situación suelen haber disputas, personas que se han ido mal de las compañías y se han llevado los clientes”.

También aludió al hecho de que actualmente la transparencia se considera un valor: “El empleado ahora está en empresas muy transparentes que ganan su compromiso a través de compartir información, de hacerle participe de las grandes decisiones. Cuanta mayor información dispone mayor involucración tiene. Son elementos culturales. Es una cuestión de formación, de inculcar una cultura de la prevención, de enseñar a manejar la información de forma discreta”. A este respecto recordó que con el auge de los dispositivos móviles nos encontramos con que se celebran reuniones sobre temas delicados y hay gente que los va twitteando: “Sales de la reunión y ya hay gente que sabe lo que se ha dicho”, comentó.

## UNA CUESTIÓN DE CONFIDENCIALIDAD

Guzmán de Aguilar, socio director de Piniés & Aguilar, cambió de tercio al plantear los posibles conflictos que se plantean en el trabajo de los headhunters. “Cuando se busca una persona para cubrir una posición alta, ¿cómo se puede gestionar el posible conflicto de intereses? En el fondo el cliente demanda un perfil, unos conocimientos y una información. Es lo que necesita y es por lo que paga”, planteó. A esta cuestión Ramón Bartolomé respondió que “cuando entrevistamos a un profesional

y nos advierte de alguna información sensible, esa información no pasa al cliente, la utilizamos para sacar nuestras conclusiones y llevar a cabo nuestro trabajo pero no la utilizamos ante terceros”.

De Aguilar insistió en que “al margen de que una empresa tenga unos procedimientos y unas políticas de control, sería importante que el mercado en España valorara a los profesionales que sean éticos. Eso tiene que ver mucho con la formación del profesional, que no se busque al mercenario que te aporte un poquito más de negocio en el corto plazo sino que valore un determinado perfil de profesional que aporte valor en el largo plazo”. A lo que Rafael Cabarcos comentó que “eso dependerá de lo que busques, si es una persona con una cualificación determinada o alguien con contactos y capacidad de influir”. A lo que añadió: “Eso me recuerda que hay Fondos de Inversión que solo invierten en lo que llaman empresas éticas”.

## La clave está en conciliar la información confidencial con las políticas de Recursos Humanos que tienden de la transparencia y el compromiso

Félix Alarcón argumentó que “para desarrollar su trabajo diario todos nuestros empleados necesitan conocer cuál es nuestro negocio, la estrategia de la compañía y las compañías tendemos a maximizar el valor de la información. Si yo tuviera que

decir cuál es la máxima de las organizaciones en las que he estado diría que comunicar, comunicar y comunicar; y trabajar con honestidad y con responsabilidad. Cada vez que lanzamos un mensaje, el empleado tiene que saber que es información que no debe conocer ningún competidor”. Para Alarcón, la clave está en conciliar la información confidencial con las políticas de RR.HH. que tienden de la transparencia y el compromiso”.

En este sentido, Borja González señaló que “la cuestión es que los protocolos de actuación tienen que estar por escrito para que la empresa tenga la posibilidad de defender ante una mala actuación de un empleado. Si las normas son claras, escritas y conocidas se pueden llegar a dar casos de despidos procedente”. Ignacio Mazo recordó que en Arthur Andersen, compañía en la que trabajó durante unos años, se comunicaba a todos los nuevos empleados qué precauciones debían observar en su trabajo cotidiano: ser cuidadoso con comentarios

en aviones o lugares públicos, no llevar carpetas visibles con el logotipo de los clientes y otras medidas similares.

Miguel Ángel Zuil consideró que “las cláusulas de confidencialidad son muy importantes pero no son la solución cuando el daño está hecho. Yo creo que la prevención llega por la vía de la satisfacción del empleado. Yo diría que es importante saber qué grado de satisfacción tienen los empleados con acceso a información sensible”. Bruce Goslin apuntó que K2 Global realiza muchas investigaciones sobre fugas de información: “No es solo una cuestión de haber perdido información importante o de que haya pasado a un competidor, sino del efecto que puede provocar en el mercado. Una empresa que pierde información pierde la confianza de sus clientes. La protección de la información de la empresa es importante por el efecto económico que puede tener sobre la propia empresa”.

## CULTURA Y OPERACIONES

Ignacio Mazo dijo que “la cultura anglosajona es más sensible a esa protección y a establecer mecanismos que son aceptados por las dos partes. En la cultura hispana molesta el control y siempre hay cierta

reticencia. Una empresa que establece mecanismo de control tiene mala imagen y esa ‘penalización’ del mercado hace que la empresa no sepa protegerse. Para mí, al final es un tema cultural. La Dirección General tiene que definir las políticas de confidencialidad, desde RR.HH. hay que establecer las políticas de control y desde Tecnología implantarlas”.

Lorena Martínez, directora Asociada del Career Management Centre del IE Business School, explicó que en la escuela “lo que nosotros intentamos es fomentar un comportamiento profesional con el que sabes qué información puedes compartir y qué información no puedes compartir, siempre tratando de favorecer el networking. Creo que tanto la prevención como la reacción ante las fugas de información se podrían evitar si fomentamos una conciencia clara de lo que está bien y lo que está mal”. Abundando en ello, Lucía Andrés, también directora asociada en el mismo

centro, recordó que el Departamento de Admisiones cuenta con unas normas estrictas de confidencialidad de los datos que maneja de los alumnos. No podemos controlar a todos los alumnos en todo momento, ni lo que dicen o con quién hablan, pero nosotros sí tenemos que ser muy estrictos en la reserva de los muchos datos de que disponemos”.

Goslin aprovechó para comentar que en su empresa existen unas medidas muy fuertes de acceso a los diferentes proyectos. “Solo tienes acceso al proyecto si estas trabajando en él, pero es para afianzar una cultura de protección de la información. Ponemos mucho énfasis en los aspectos éticos. Nuestros empleados saben que si vulneramos la confidencialidad de un cliente la empresa va a perder su reputación y la reputación de la empresa es lo que nos ayuda a llegar a los clientes. La creación de esa cultura en

los nuevos empleados es bastante importante, inculcarles determinados valores para que los transmitan a través de su comportamiento. Los empleados son reflejo de sus empresas”.

Otro tema que se discutió en el coloquio fue el de las personas que dejan una firma para crear otra, llevándose el know

how y los contactos. En el mundo de los headhunters, como en otras ramas de la consultoría, ha sucedido en incontables ocasiones. Miguel Ángel Zuil consideró que “hay mucha gente que ha salido de empresas por razones profesionales o personales y han entrado en este negocio pensando que lo podía hacer mejor. A nosotros nos preocupa desde el punto de vista del mensaje que se puede transmitir al mercado”.

También desde el ámbito de la consultoría, Ignacio Mazo explicó que su firma suele actuar desde tres ámbitos: “Primero, hacer entender a esa persona que eso está mal; segundo, que perciba que ese comportamiento no es bueno; tercero, hacerle ver las consecuencias de no llevar a cabo una conducta adecuada, aunque a veces es complicado”. Cerró el coloquio Félix Alarcón asegurando: “A mí me gustaría pensar que no solamente vamos a ser capaces de controlar por el miedo al castigo, sino porque vamos a premiar el buen comportamiento”. ■