

## Solo uno de cada cinco bancos y aseguradoras confía en su capacidad para detectar ciberataques

*La aplicación del Reglamento General de Protección de Datos a partir de mayo de 2018, obligará a tomar medidas y a ofrecer mayor transparencia a los clientes*

(NOTA: como anexo a este documento se distribuye un resumen específico de los datos del estudio para España).

Madrid, 14 de febrero de 2017 – Los clientes de bancos y aseguradoras son los que demuestran el nivel más alto de confianza en la ciberseguridad de los sistemas de las entidades: su índice de confianza (83%) es significativamente mayor que el de cualquier otro sector (siendo el 28% para las empresas de comercio electrónico y un 13% para las de telecomunicaciones y *retail*). Sin embargo, las entidades financieras no comparten este sentimiento, pues solo uno de cada cinco directivos (21%) tiene alta confianza en su capacidad para detectar un ciberataque, por no hablar de su capacidad para defenderse de él. Esta es la conclusión de un informe elaborado por [Capgemini](#), a través de su Instituto de Transformación Digital, bajo el título [The Currency of Trust: Why Banks and Insurers Must Make Customer Data Safer and More Secure](#).

En el caso de España los datos son similares: un 76% de los clientes del sector financiero confían en la protección de sus datos mientras que sólo uno de cada cinco directivos (22%) confía en la capacidad de su entidad para detectar brechas de seguridad.

Tal y como explica Mike Turner, COO mundial de Ciberseguridad de Capgemini: “Los clientes confían de manera implícita en las entidades donde tienen depositado su dinero, seguros y datos, pero esta confianza se nutre de la errónea convicción de que pueden ser 100% seguros. Frente a los esfuerzos cada vez mayores que dedican los bancos y aseguradoras a combatir las difíciles amenazas que representa la ciberdelincuencia, el desconocimiento del público de estas amenazas y retos sigue siendo alto”.

“Cuando empiece a aplicarse el Reglamento General de Protección de Datos de la UE y las violaciones de seguridad salgan a la luz poco después de haberse producido, a muchos les va a pillar por sorpresa”, comenta Zhiwei Jiang, responsable mundial de Servicios Financieros en el área Insights & Data de Capgemini. “La aplicación del Reglamento el próximo año es una oportunidad de primer orden para la transformación de bancos y aseguradoras hacia las fortalezas digitales con que los consumidores les asocian”.

El estudio de Capgemini ha sido realizado entre 7.600 consumidores y más de 180 altos ejecutivos del ámbito de la seguridad y la protección de datos de bancos y aseguradoras en ocho países (Francia, Alemania, India, Países Bajos, España, Suecia, Reino Unido y Estados Unidos). Las conclusiones ponen de relieve la brecha existente entre el nivel de confianza que los consumidores tienen en los bancos y aseguradores y la realidad.

### **Confianza en bancos y aseguradoras, factor determinante**

La mayoría de los clientes considera que confiar en la protección de sus datos personales y la seguridad son factores extremadamente importantes a la hora de elegir una entidad (65%). No obstante, parece que los consumidores confían instintivamente en bancos y aseguradoras, sin una razón fundamentada para ello. La divergencia entre la percepción de los consumidores y la realidad se constata principalmente en el hecho de que, si bien una de cada cuatro entidades ha denunciado haber sido víctima de un ciberataque, solo un 3% de los consumidores cree que su entidad ha podido ser víctima de cibercriminales. Es decir, una diferencia de 23 puntos. En el caso de España, esta divergencia es de 32 puntos.

### **La seguridad de los datos como reto**

A pesar de las enormes inversiones que las entidades financieras, especialmente los bancos, están realizando para garantizar la seguridad de sus sistemas, el número y la frecuencia de las violaciones de datos van en aumento. La rapidez con la que cambian las amenazas y la falta de claridad entre los órganos de gobierno podrían explicar el hecho de que, aunque con elevados niveles de inversión, el 71% de las entidades no cuenta con una estrategia efectiva de seguridad ni con políticas sólidas de protección de datos.

### **Con el RGPD, se tomará más conciencia sobre las ciberamenazas**

El Reglamento General de Protección de Datos (RGPD) de la UE, que será aplicable a partir de mayo de 2018, obligará a las organizaciones a informar de las violaciones de datos sufridas en un plazo de 72 horas si no quieren ser objeto de una sanción elevada. Aunque es normativa de la UE, el Reglamento se aplicará a compañías que, residentes o no en Europa, traten datos personales de ciudadanos europeos, por lo que se prevé que también afecte a bancos y aseguradoras de Estados Unidos, Reino Unido y Asia. A pesar de su obligatoriedad y de que solo falta un año para su aplicación, solo un tercio de los directivos consultados (32%) considera que su empresa ha avanzado considerablemente en la adopción de las medidas que marca el Reglamento.

### **Si se rompe la confianza, los clientes se irán**

A pesar de la confianza instintiva de muchos usuarios en sus bancos y aseguradoras en materia de protección de datos, es más que probable que tomasen medidas si dicha confianza se viera comprometida. Tres cuartas partes (74%) de los consumidores cambiarían de entidad en caso de una brecha de ciberseguridad. Entre los clientes que seguirían con su entidad a pesar del riesgo, más de una cuarta parte afirmó que tendría reservas a la hora de realizar nuevas inversiones. Los clientes españoles son más tajantes y un 90% cambiaría de entidad si supiera que ha sufrido un ciberataque.

### **Metodología**

El Instituto de Transformación Digital de Capgemini realizó una encuesta entre 7.600 consumidores de Francia, Alemania, India, Países Bajos, España, Suecia, Reino Unido y Estados Unidos, sobre sus opiniones acerca de la protección de datos y la seguridad en la banca y los seguros. Además, Capgemini mantuvo entrevistas en profundidad con 183 cargos directivos en materia de protección de datos y seguridad de Francia, Alemania, India, España, Reino Unido y Estados Unidos, para conocer cómo están enfocando sus organizaciones las cuestiones de ciberseguridad y tratamiento de datos; todos ellos directivos en bancos y aseguradoras que representan un volumen conjunto de ingresos superior a 500 millones de dólares a nivel mundial. El informe puede descargarse [aquí](#).

### **Notas a redactores**

#### **Acerca del Instituto de Transformación Digital**

El Instituto de Transformación Digital es el "think tank" interno de Capgemini para el estudio del ámbito digital. El instituto publica investigaciones sobre el impacto de las tecnologías digitales en grandes negocios tradicionales. El equipo se apoya en la red mundial de expertos de Capgemini y

trabaja codo con codo con socios académicos y tecnológicos. El instituto cuenta con centros de investigación especializados en Reino Unido y la India.

### **Acerca de Capgemini**

Con más de 180.000 empleados repartidos en más de 40 países, Capgemini es un líder mundial en consultoría, tecnología y outsourcing. El grupo alcanzó unos ingresos globales de 11.900 millones de euros en 2015. Capgemini, en colaboración con sus clientes, crea y proporciona las soluciones tecnológicas, digitales y de negocio que mejor se ajustan a sus necesidades y que les permiten alcanzar innovación y competitividad. Siendo una organización profundamente multicultural, Capgemini ha desarrollado su propia forma de trabajar, la [Collaborative Business Experience™](#), basada en su modelo de producción [Rightshore®](#).

Para más información: [www.es.capgemini.com](http://www.es.capgemini.com)

*Rightshore® es una marca registrada de Capgemini*