

¿Cómo potenciar la confianza del usuario digital?

La creciente preocupación de los usuarios por la seguridad está abriendo oportunidades a nuevos modelos de negocio en los que el usuario es capaz de monitorizar quién le “vigila” y bloquearlo si no le merece la suficiente confianza.

La tendencia de nuevos servicios que ofrecen la posibilidad de eliminar información propia de la Red destapa una oportunidad que debe ser capitalizada por las empresas que conforman el sector.



01 Soy 'screenager'

02 Lo quiero fácil

03 ¿Eres de confianza?

04 Gánate mi lealtad

05 Un mundo de nuevas oportunidades



Personalización de la seguridad

Las compañías que ofrezcan al usuario transparencia, autonomía y seguridad podrán desarrollar servicios de alto valor añadido y generar un valor adicional a través de: Personalización, Adaptación y Automatización.



Servicios de seguridad

Los usuarios digitales muestran preocupación por sus datos a la hora de introducir información confidencial en la red. Por el lado del desarrollo de productos, esto ofrece un nicho de mercado para productos que ofrezcan seguridad, desde antivirus y *antispyware*, hasta certificados digitales de seguridad y todo aquello que garantice al usuario que su información confidencial no será distribuida. Por el lado de organización, en las empresas se identifica la necesidad de adecuar sus roles y procesos para garantizar la seguridad del usuario digital. Esto hace surgir dentro de las organizaciones una nueva figura: el *chief security officer*.



Propiedad de los datos

Ahora la propiedad de los datos es del usuario y no los va a ceder fácilmente a no ser que se le aporte un valor diferencial, como los descuentos a cambio de información de los usuarios que ya ponen en práctica algunas empresas. Esto puede suponer una oportunidad tanto por los nuevos servicios que se pueden desarrollar como por el impacto de la percepción de los servicios sobre la imagen de marca. En el mundo digital, violentar la confianza del usuario puede tener un efecto devastador. Al mismo tiempo, la gestión y evaluación de riesgos no debe ser considerada como un punto aislado en la cadena, sino que debe ser abordada en conjunto con terceros y socios.



Protección en un mundo hiperconectado

En un mundo en el que incluso las casas y los coches están conectados, todas las empresas del sector deberían introducir medidas de protección para el enorme volumen de información privada que circula por la red y muchos usuarios no se sienten seguros, hasta el punto de que el 23 % no compran tecnologías *smart* para sus hogares porque no confían en la seguridad de la información. Además, se debería realizar un esfuerzo especial dentro de las empresas para reforzar el empleo de metodologías de testeo de productos de manera proactiva.