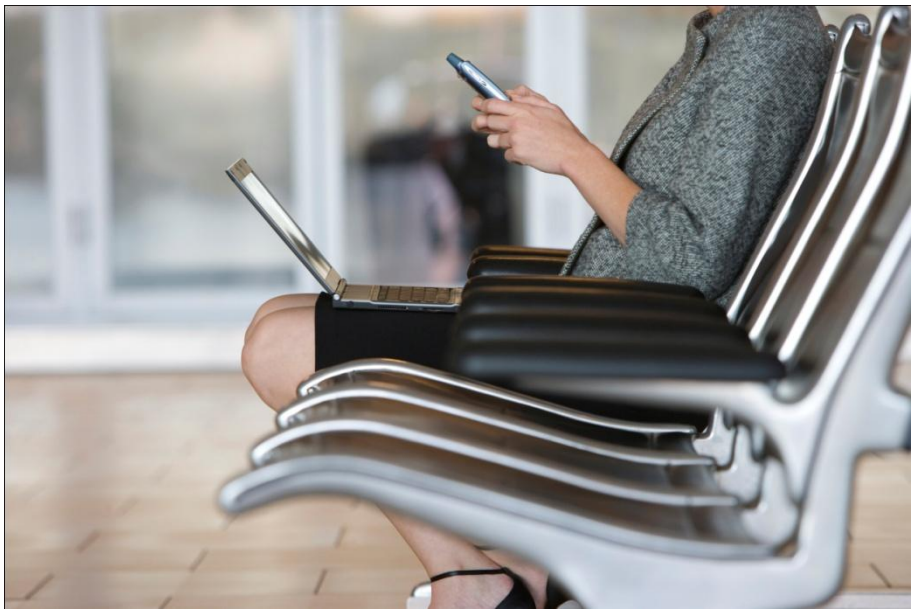
Estar siempre conectados: oportunidades y amenazas



Mientras que la nueva era de "estar siempre conectados" presenta una oportunidad de negocios, esto también ha creado nuevas amenazas.

En particular, el aumento de la penetración de móviles conjuntamente con un panorama cambiante de amenazas y un mercado de tecnología móvil fragmentado, ha dado lugar a profundas preocupaciones sobre la seguridad y riesgos de privacidad.

Los consumidores están cada vez más preocupados por la seguridad de sus datos y la privacidad de la información en sus dispositivos móviles. De hecho, según un reciente informe de KPMG International, los usuarios de muchos mercados están cada vez más dispuestos a pagar más por sus aplicaciones móviles con el fin de garantizar el mantenimiento de su privacidad.

Los consumidores tienen buenas razones para estar preocupados. Un estudio reciente de las aplicaciones móviles gratis realizado por **Appthority** (https://www.appthority.com) encontró que el 96 % de todas las aplicaciones gratuitas disponibles en App Store de Apple y Google Play comparten datos con terceros y el 76 % de las 50 aplicaciones gratuitas más populares están asociadas con comportamientos de riesgo o de invasión de la privacidad. Sin embargo, un estudio reciente de Universidad Carnegie Mellon encontró que mientras que los usuarios pueden estar preocupados, en general no son muy conscientes de lo que las aplicaciones móviles están haciendo con sus datos.

"El hecho que las aplicaciones gratis son capaces de triangular localización y anuncios basados en preferencias personales ha demostrado que el potencial de abuso es alto"
Greg Bell, Information Protection y Business Resiliency Service Leader, KPMG USA.

De acuerdo a una encuesta de **Forrester** de 2012 *Global Technographics Online*, los usuarios de dispositivos móviles expresan niveles significativos de preocupación por su privacidad y la seguridad cuando acceden a Internet desde sus teléfonos móviles (Figura 1).

En el mundo empresarial las preocupaciones sobre la seguridad de los

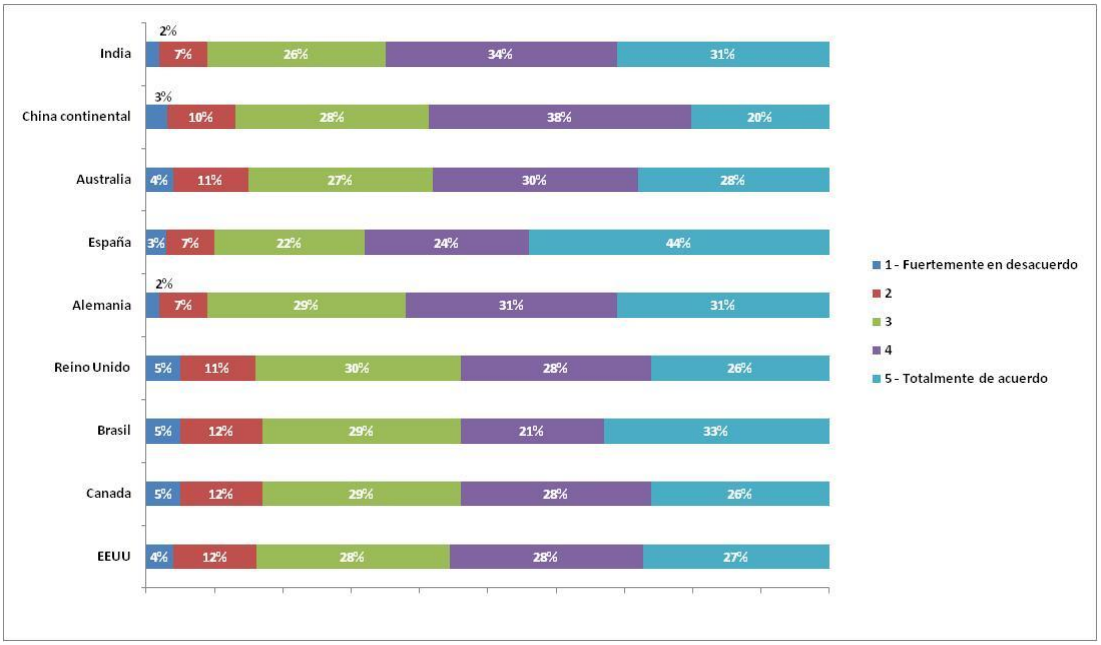


Figura 1. Consulta si los consumidores están preocupados por la seguridad y privacidad de datos. Fuente: Forrester Research Global Technographics Online Benchmark Survey, Q2, Q3 2012.

© 2013 KPMG Sociedad Civil, sociedad civil uruguaya y firma miembro de la red de firmas miembro independientes de KPMG afiliadas a KPMG International Cooperative ("KPMG International"), una entidad suiza. Derechos reservados.

móviles está en incremento. Particularmente la preocupación de la pérdida de datos por extravío o robo de los dispositivos se encuentra entre los puntos relevantes y por consiguiente debe ser prioritario implementar o mejorar la seguridad.

En relación al punto anterior podemos tomar como referencia los resultados de la Figura 2 en donde se muestra el grado de preocupación sobre ciertos problemas de la seguridad de los móviles en el mercado norteamericano y europeo.

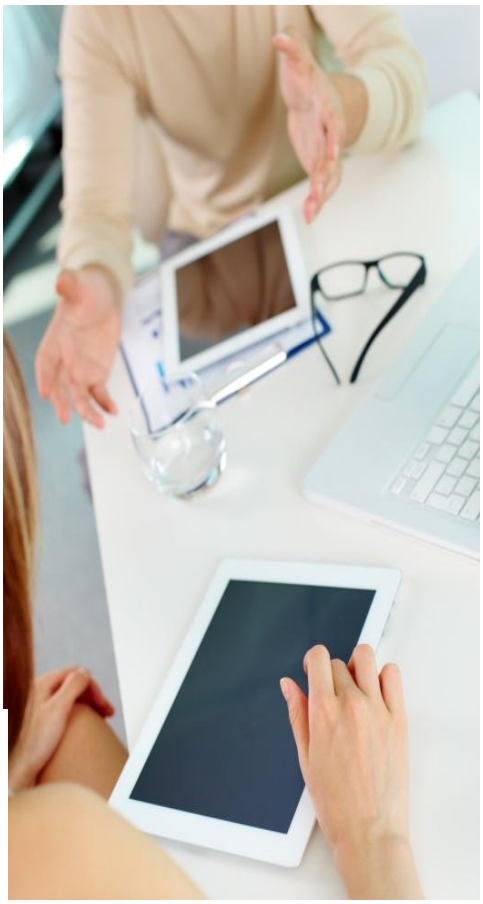
Si bien estas preocupaciones son temas a trabajar, la incorporación de los dispositivos móviles en nuestro día a día ha resultado ser un gran cambio. Estar conectados sin importar el lugar, acceder a documentos, aplicaciones, redes sociales, correo electrónico o navegar por Internet significa una gran oportunidad.

Es por esta razón que las ventas de dispositivos móviles van en aumento. Apple y dispositivos con Android dominan el mercado con un 80 % del mismo.

El conjunto de dispositivos con Android es claramente el ganador en términos de unidades vendidas, pero Apple sigue siendo el número uno cuando se trata de valor - ya sea de los ingresos generados por las aplicaciones, las comisiones de comercio electrónico y el tráfico en Internet.

Esta situación del mercado y la innovación tecnológica hace que las empresas deban plantearse el lugar que debe tener lo móvil en sus estrategias y modelos operativos.

Si en el modelo operativo de la empresa los dispositivos móviles pasan a jugar un papel relevante es necesario que se evalúen amenazadas y definir acciones en relación a las mismas.



"Los consumidores están empezando a tomar conciencia de las implicancias de sus decisiones cuando se trata de proteger su privacidad y la seguridad en sus móviles, incluso si no están seguros de qué hacer al respecto". Greg Bell, Information Protection and Business Resiliency Service Leader, KPMG USA

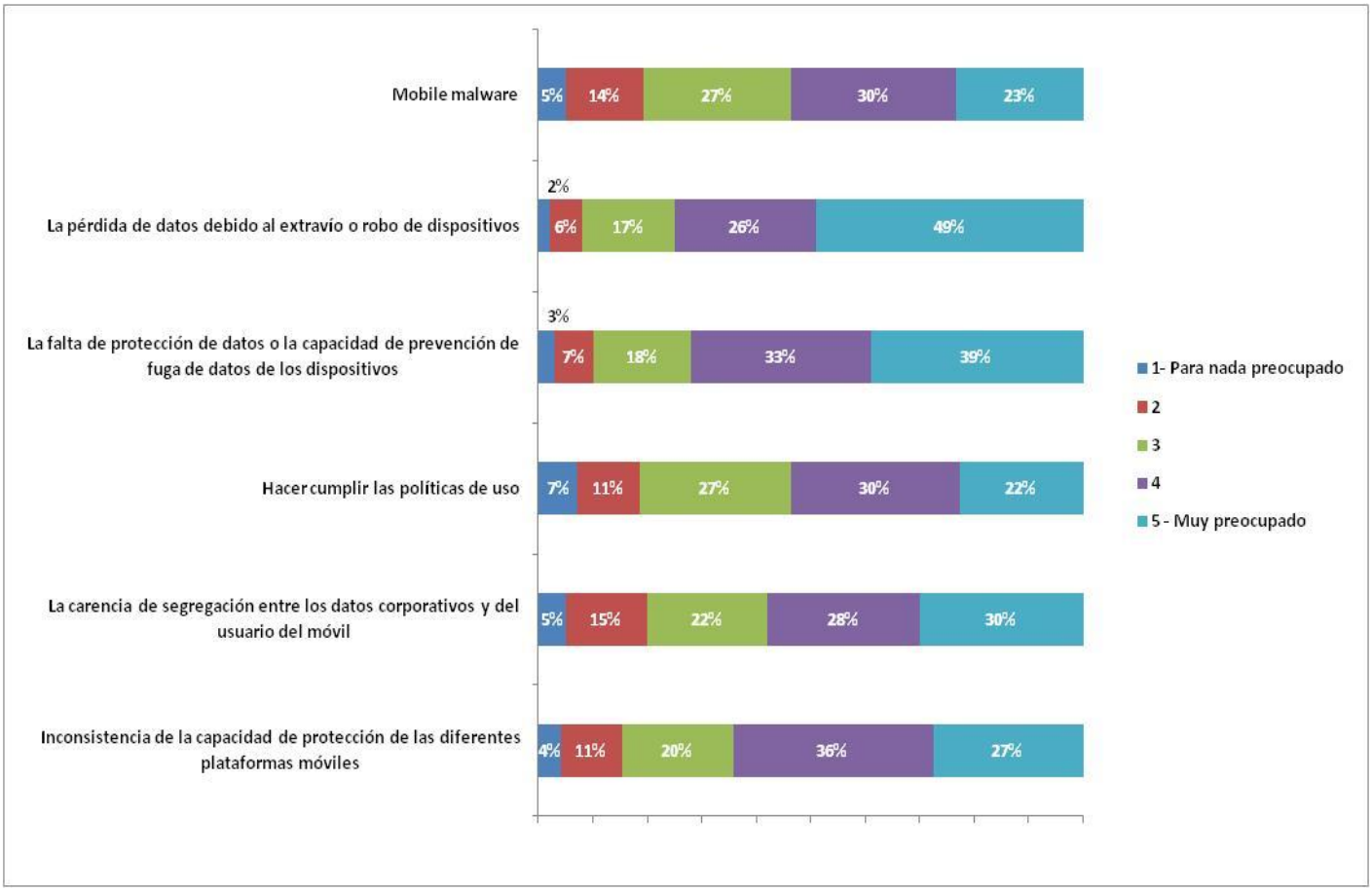


Figura 2. Fuente: Forrester Research Global Technographics Online Benchmark Survey, Q2, Q3 2012.

© 2013 KPMG Sociedad Civil, sociedad civil uruguaya y firma miembro de la red de firmas miembro independientes de KPMG afiliadas a KPMG International Cooperative ("KPMG International"), una entidad suiza. Derechos reservados.

Principales prioridades para los tomadores de decisiones de TI en Estados Unidos y Europa

Políticas y tecnologías que podrían disminuir las preocupaciones actuales.

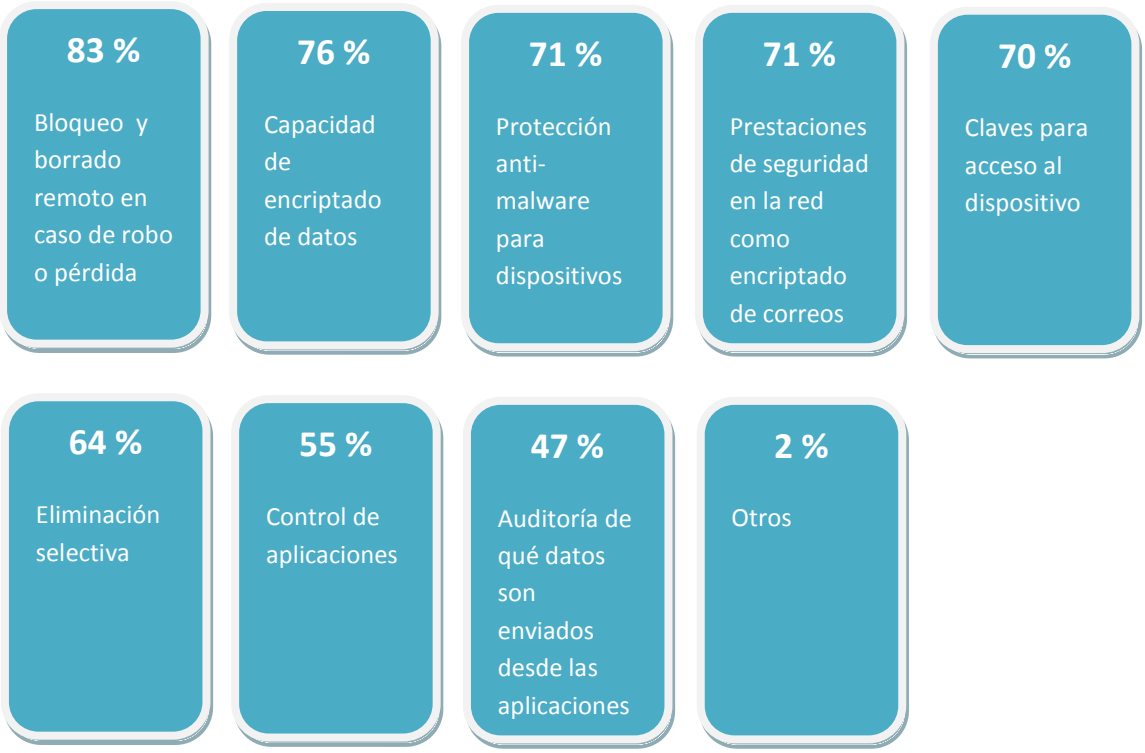


Figura 3. Fuente: Forrester Research Global Technographics Online Benchmark Survey, Q2, Q3 2012.

"Tratar de hacer cumplir una política de seguridad coherente y al mismo tiempo tratar de ofrecer una experiencia de usuario sin fisuras, es una tarea difícil. Pero es algo que claramente necesita ser abordado" **Sanjaya Krishna**, Principal and Digital Risk Consulting Leader, KPMG USA.

Consejos para proteger nuestros dispositivos móviles

- ✓ **Utilizar código de bloqueo**: algunos dispositivos ofrecen la posibilidad de utilizar un código numérico, mientras que otros ofrecen la posibilidad de utilizar un patrón. Esta protección no permitiría el uso del dispositivo por parte de un usuario malintencionado.
- ✓ **Establecer contraseña en las tarjetas de memoria:** en los dispositivos que dispongan de memoria extraíble, como pueden ser las tarjetas microSD, utilizar una contraseña en las mismas supone un nivel de seguridad adicional en caso que se extraiga la tarjeta y se intente leer en otro dispositivo.
- ✓ **Respaldos periódicos**: copiar la información del dispositivo en una ubicación segura supone una protección adicional, tanto en caso de robo, pérdida o falla del equipo. Copiar por ejemplo los contactos del teléfono celular puede ser útil. Existen servicios provistos por algunos fabricantes para tal fin, o puede utilizarse un PC convencional para ello.
- ✓ **Utilizar soluciones antirrobo**: en caso de robo o pérdida, existen soluciones antirrobo que permiten bloquear y/o borrar la información del dispositivo, mediante internet o bien por el envío de un mensaje de texto. En caso de ser encontrados, se podría deshabilitar el bloqueo y el dispositivo quedará activo nuevamente.
- ✓ **Uso de redes no protegidas**: el uso de redes WiFi abiertas en lugares como cafés o aeropuertos es una comodidad, aunque al ser redes de acceso público, generalmente no están protegidas con contraseña. No es recomendable utilizar las mismas para enviar información confidencial como información bancaria, dado que puede ser interceptada por un tercero.
- ✓ **Utilizar soluciones antivirus**: los virus no son una amenaza solamente para las computadoras tradicionales, sino que los dispositivos móviles también se ven afectados. Los mismos pueden ejecutar acciones como conectarse a internet para enviar información, enviar mensajes de texto, borrar información o bloquear el equipo exigiendo un pago para liberarlo. Es por ello que es recomendable contar con una solución antivirus que proteja el dispositivo.

© 2013 KPMG Sociedad Civil, sociedad civil uruguaya y firma miembro de la red de firmas miembro independientes de KPMG afiliadas a KPMG International Cooperative ("KPMG International"), una entidad suiza. Derechos reservados.

Contáctenos

Para más información sobre este tema, contácte a alguno de los siguientes profesionales de KPMG:

Cr. Rodrigo Ribeiro
Socio
rribeiro@kpmg.com

Ing. Pablo Romero
Gerente Senior
promero1@kpmg.com

Lic. Marcelo Cagnani
Gerente Senior
marcelocagnani@kpmg.com

kpmg.com.uy

Es un producto confeccionado por el Departamento de Management Consulting de KPMG. Queda prohibida la reproducción total y/o parcial de esta publicación, así como su tratamiento informático, y su transmisión o comunicación por cualquier forma o medio, ya sea electrónico, mecánico, por fotocopia, por registro u otros métodos, bajo apercibimiento de las sanciones dispuestas por la Ley Nº 9.739, con las modificaciones introducidas por la Ley N° 17.616, salvo que se cuente con el consentimiento previo y por escrito de los autores.

Nota al usuario: La visión y opiniones aquí reflejadas son del autor y no necesariamente representan la visión y opiniones de KPMG. Toda la información brindada por este medio, es de carácter general y no pretende reemplazar ni sustituir cualquier servicio legal, fiscal o cualquier otro ámbito profesional. Por lo tanto, no deberá utilizarse como definitivo en la toma de decisiones por parte de alguna persona física o jurídica sin consultar con su asesor profesional luego de haber realizado un estudio particular de la situación. Asimismo, nos remitimos a lo establecido en "AvisoLegal - Política de Privacidad" de nuestro sitio web.

© 2013 KPMG Sociedad Civil, sociedad civil uruguaya y firma miembro de la red de firmas miembro independientes de KPMG afiliadas a KPMG International Cooperative ("KPMG International"), una entidad suiza. Derechos reservados.