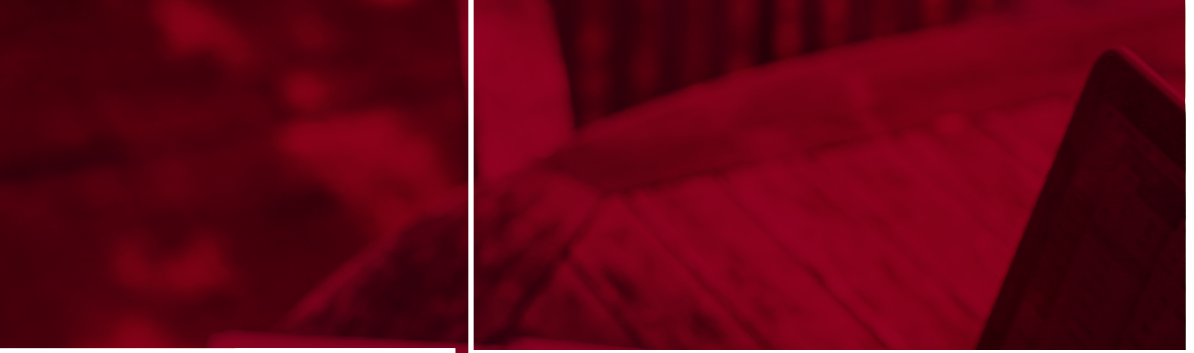


BYOD

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

INTRODUCCIÓN

Esta guía pretende ofrecer lineamientos generales para todas las personas que quieran aproximarse al uso de BYOD, conocer en qué consiste y los beneficios y riesgos asociados.

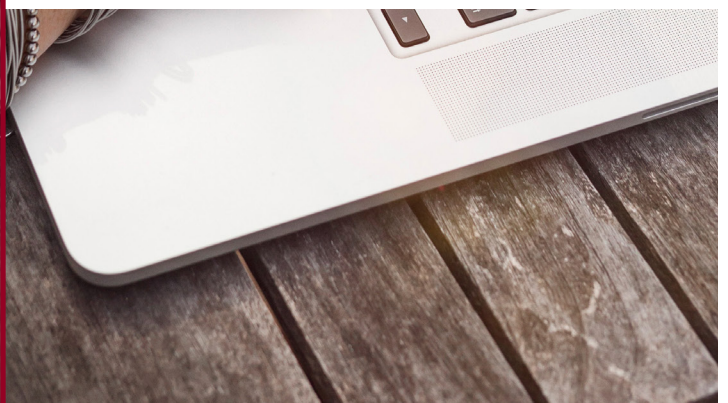
Además, incorpora recomendaciones para todos quienes quieran aplicar este tipo de estrategias en sus respectivas organizaciones, tanto públicas como privadas.

BYOD

¿Qué es BYOD?

Bring Your Own Device (BYOD, por sus siglas en inglés, traducido como "Trae Tu Propio Dispositivo") es una estrategia alternativa y cada vez más extendida en el ámbito laboral que refiere al uso de dispositivos personales (celulares, tabletas, notebooks, etc.) de los empleados para el cumplimiento de sus tareas en dicho ámbito, en forma presencial o a distancia. La estrategia puede ir desde la aceptación tácita por el empleador, hasta el reconocimiento expreso y pago de subsidios por su parte.

Las tendencias actuales marcan una extensión no solo de la utilización del dispositivo en sí mismo, sino también de las aplicaciones que este contiene, los espacios de almacenamiento empleados por el titular del dispositivo, las redes a las cuales se conecta y la tecnología empleada, entre otros.



La protección de datos personales para BYOD

La utilización de estos dispositivos impacta en diversos ámbitos, como por ejemplo, la protección de datos personales, la seguridad de la información y las relaciones laborales.

En particular, la preocupación respecto a la protección y utilización de los datos ha sido una constante en el caso de la implantación de estrategias BYOD. Se debe tener en cuenta que la información tratada a través de estos dispositivos no solo es información personal de los trabajadores, sino también de las empresas, organizaciones y terceros.

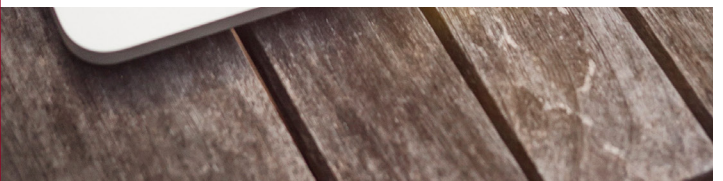
En este sentido, es importante tener presente que la Ley Nº 18.331, de 11 de agosto de 2008, expresa que el responsable del tratamiento de los datos es aquella persona que los utiliza en su calidad de propietario o decide sobre su finalidad o uso y es quien, además, debe adoptar medidas de seguridad que garanticen su seguridad y confidencialidad.

Por ello, resulta necesario valorar los riesgos y beneficios de esta estrategia, considerando, entre otras cuestiones, el tipo de información objeto de tratamiento (personal, laboral y de terceros), su propiedad, la limitación para su acceso, su almacenamiento (en el dispositivo, en la nube u otros) y las capacidades técnicas y económicas de la empresa, entre otras cuestiones.

Aspectos de protección de datos personales a considerar en la utilización de BYOD

Ante la posibilidad de utilizar BYOD, es necesario analizar algunos aspectos desde la perspectiva de la protección de los datos personales.

En primer lugar, debe tenerse presente que el responsable en esta materia va a ser el propietario de la base de datos o quien decida sobre su finalidad, contenido y uso. En este caso, por tanto, el empleador va a ser el responsable y quien debe adoptar medidas para cumplir con la normativa de protección de datos personales.



En segundo lugar, resulta importante tener en cuenta el principio de finalidad: los datos no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención. Por tanto, en el ámbito de BYOD se debe tener especial cuidado con los usos que se hacen de la información cuando esta se encuentra en poder de un tercero a la relación responsable-titular del dato.

En tercer lugar, corresponde considerar que los datos deben ser utilizados por el responsable dentro del marco para el cual fueron recabados.

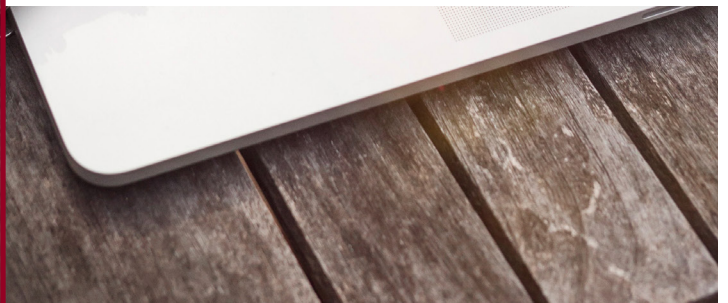
En cuarto lugar, resulta de interés el cumplimiento del principio de reserva, definido como la imposibilidad de divulgar a terceros información que los empleados conozcan en el ámbito laboral. En BYOD, la información se encuentra asociada a un dispositivo o aplicación personal del empleado, por lo cual el empleador no tiene forma de controlar los accesos. En este caso, se recomienda la adopción de un protocolo de actuación que prevea la adopción de medidas que aseguren el acceso o la no adulteración de la información.

Asimismo, la normativa de protección de datos exige la adopción de medidas de seguridad que resulten adecuadas para garantizar la seguridad y confidencialidad de los datos personales. Para asegurarse de que el responsable pueda dar cumplimiento a este principio en estos casos, se entiende necesario adoptar un protocolo con disposiciones claras.

En este marco, es importante la privacidad por diseño, lo que implica que antes de acordar la utilización del BYOD es necesario analizar qué datos se van a utilizar, de acuerdo con qué medidas y cómo dar cumplimiento a todas las normas de protección de datos personales.

Orientaciones para la utilización de BYOD

A la hora de optar por permitir la utilización de dispositivos o aplicaciones personales se deben tener presente las siguientes orientaciones:



Para las organizaciones

En el ámbito privado

- Establecer reglas claras, preferentemente, mediante la adopción de protocolos que contengan directrices acerca de cómo utilizar los dispositivos personales, que pueden incluir el uso de controles técnicos.
- Definir los mecanismos para separar la información personal del empleado de la información de la organización, a la vez que establecer los formatos para su almacenamiento, tratamiento y acceso.
- En caso de que la información contenida en los dispositivos o aplicaciones personales tenga la doble calidad de información personal y de la organización, se deben establecer todas las medidas necesarias para asegurar la integridad, completitud y veracidad de los datos.
- Evitar el uso de dispositivos personales de los empleados para el tratamiento de datos sensibles, salvo autorización expresa y por escrito de los titulares de los datos.
- Contar con una estrategia de seguridad de la información que contenga pautas ante el caso de que haya vulneraciones a los datos personales.

En el ámbito público

Sin perjuicio de la aplicación de las recomendaciones anteriores, en el ámbito público existen algunas características particulares que se deben tener presente:

- Existen normas en materia de adopción de políticas de seguridad de la información y guías.
- En la Administración Central, corresponde aplicar los lineamientos establecidos en el Decreto Nº 92/014, empleando páginas web y sistemas de correo seguros y con la extensión “.gub.uy” o “.mil.uy” y almacenar toda aquella información que pueda considerarse activo crítico en servidores ubicados geográficamente en Uruguay.

- Emplear en los accesos a la información mecanismos de autenticación de identidad seguros para aquellos sistemas o servicios a los que se acceda a través de los dispositivos personales de los empleados.
- Aplicar firma electrónica y firma electrónica avanzada para toda actuación realizada por funcionarios, cuando sea necesario.

Para los empleados

- En el dispositivo deberá mantenerse la información personal del empleado separada de la información vinculada al empleador.
- Los accesos a sistemas o servicios del empleador vía internet deberá hacerse por los canales previstos por este.
- Toda incorporación de software en general por la empresa en el dispositivo del empleado para la mejor realización de sus tareas deberá realizarse con su consentimiento previo, expreso e informado.
- El acceso a los dispositivos personales para la recolección, actualización y supresión de información del empleador es pertinente, pero debe realizarse con el consentimiento y en presencia del empleado.
- Las políticas de BYOD pueden prever compensaciones especiales por el uso de dispositivos personales

UNIDAD REGULADORA Y DE CONTROL DE
DATOS PERSONALES

www.datospersonales.gub.uy

agesic

PRESIDENCIA
República Oriental del Uruguay