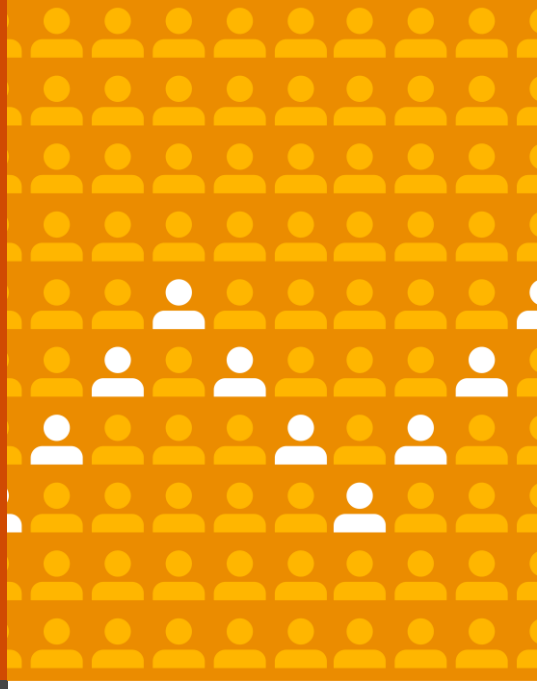
Alerta COVID-19: Regulación Digital

Diez recomendaciones para un teletrabajo más seguro



Incluimos una serie de recomendaciones para garantizar la seguridad y confidencialidad de la información de la compañía y los datos personales de los profesionales, con respecto al uso de las TIC

Marzo, 2020

Ponte en contacto con PwC Tax & Legal Services:

Assumpta Zorraquino
Socia responsable de Regulación Digital
assumpta.zorraquino@pwc.com

Alejandra Matas
Directora en el área de Regulación Digital
alejandra.matas.brancos@pwc.com

En este escenario complejo e inusual ante el que nos encontramos, y ante el desarrollo de la actividad de forma mayoritaria mediante teletrabajo, debemos tener presente la necesidad de recordar a vuestros empleados y colaboradores la vigencia de las normas de uso de los recursos TIC, al objeto de garantizar la seguridad y confidencialidad de la información de la compañía y sus datos personales.

En este sentido, incluimos a continuación una serie de pautas e indicaciones cuya implementación adicional resulta aconsejable:

1. Que en el desempeño de sus funciones laborales, los empleados o colaboradores hagan uso única y exclusivamente de los medios corporativos facilitados por la compañía, ya sean ordenadores, *tablets*, teléfonos móviles, etc.
2. Que en el desempeño de las actividades laborales debe seguir cumpliéndose con la normativa en materia de protección de datos y seguridad de la información.
3. Prohibir el uso personal de dichos dispositivos por parte de los empleados o colaboradores, así como cualquier tipo de uso por parte de terceros ajenos a la empresa, salvo los que hayan sido expresamente autorizados.
4. Incidir en la importancia de que, en el uso de los medios corporativos, no se acceda a redes wifi públicas o no seguras. En la misma línea, subrayar la importancia de que no comunicar ni compartir con otras personas el identificador de usuario y la clave de acceso al sistema.
5. Evitar imprimir o extraer documentación en papel, pen drive o similares fuera de las oficinas, que contengan información confidencial o datos personales. Si fuera estrictamente necesario hacerlo, se debería poner en conocimiento previo del director del departamento que corresponda, o del Delegado de Protección de Datos de la compañía para que estos valoren la situación y, en su caso, aprueben las medidas necesarias. En todo caso, se deberá respetar la normativa aplicable en esta materia, manteniendo la máxima confidencialidad sobre los datos y aplicando las medidas de seguridad pertinentes.
6. En el caso de que algún empleado tuviese alguna incidencia que afectase a los medios corporativos facilitados, se deberá comunicar tal circunstancia al responsable de seguridad de la compañía a la mayor brevedad posible.
7. Recordar a los empleados que la compañía podrá establecer sistemas de control del cumplimiento de las Normas de Uso, así como de la jornada laboral durante la vigencia del teletrabajo, y recordar la importancia de cumplir con las normas de confidencialidad de la compañía.
8. Recordar a los empleados la necesidad de disponer de la correspondiente licencia o autorización de la compañía para descargarse e instalar programas o aplicativos informáticos.
9. Informar a los empleados de que los dispositivos deberán devolverse a la compañía con todas las conexiones con servidores y páginas web debidamente cerradas.
10. Informar respecto del aumento de actividades delictivas mediante remisión de correos electrónicos (phishing, etc.)