ABDALA & CIA
ABOGADOS

APLICACIÓN DE LA PROTECCIÓN DE DATOS A LEY DE TELETRABAJO O TRABAJO A DISTANCIA

I. Introducción. La relevancia de proteger los datos hoy.

La protección de datos es un tema de creciente importancia para todas las empresas; cada día tiene mayor injerencia en cómo se relacionan las empresas con sus clientes y proveedores, cómo contratan y retiene a su personal, y cómo responden a los requerimientos de la autoridad.

Abdala & Cia., hace mucho tiempo está trabajando en la protección de datos personales de las personas y de las empresas con la firma española Samaniego.

La protección de datos ya es un tema de primera preocupación en Estados Unidos y en Europa, donde las multas por incumplimiento de la normativa de protección de datos pueden alcanzar millones de dólares. En Chile, el 16 de junio del 2018 se incorporó a nuestra Constitución la garantía a la protección de datos personales, y hoy se está tramitando un proyecto de ley que endurece fuertemente la regulación de los datos, lo que prontamente será un tema de relevancia jurídica.

Hoy por hoy, y en razón de la pandemia mundial producida por el COVID-19 el trabajo a distancia se ha convertido en la modalidad principal de trabajo y el teletrabajo ha cobrado mucha relevancia y protagonismo. En esta nueva forma de trabajo, los trabajadores se llevan el computador y información relevante de la empresa a su domicilio y se conectan a redes sin la protección habitual, en razón de lo anterior, ahora más que nunca, no debemos olvidar de proteger los datos personales propios, los de la empresa y aquella información que manejamos de terceros .

II. Recomendaciones que ayudarán a garantizar la seguridad de los datos durante el teletrabajo.

La ley Nº 21.220, que entró en vigor el 1 de abril de 2020, regula en forma expresa el trabajo a distancia. Se espera que con la contingencia sanitaria son muchas las empresas y profesionales independientes que optarón y optarán por esta modalidad de trabajo.

Está de más decir que pocos pudieron realizar preparativos para su correcta aplicación.

Uno de los temas de preocupación debe ser tener muy presente la seguridad de los datos, toda vez que al estar trabajando desde fuera de la oficina, se pierde el control físico sobre los documentos de trabajo, y además se expone la seguridad de las comunicaciones de la empresa.

Las siguientes **recomendaciones** ayudarán a garantizar la seguridad de los datos durante el teletrabajo.

1. <u>Si es posible, proveer a los trabajadores de equipos con las debidas medidas de seguridad</u>.

La ley Nº 21.220 establece que los equipos, las herramientas y los materiales para el trabajo a distancia o para el teletrabajo, incluidos los elementos de protección personal, deberán ser proporcionados por el empleador al trabajador. El trabajador no podrá ser obligado a utilizar elementos de su propiedad.

Igualmente, los costos de operación, funcionamiento, mantenimiento y reparación de equipos serán siempre de cargo del empleador.

Durante esta emergencia sanitaria, es probable que muchas empresas no hayan tenido forma de proveer equipos a todos sus trabajadores para el trabajo remoto.

Si los trabajadores están usando sus propios equipos <u>se recomienda</u>:

1.1 Aumentar las medidas de seguridad para entrar a las redes internas de la empresa.

Muchas empresas tienen redes internas que solo pueden utilizarse desde sus propias oficinas. Estas deben abrirse al acceso remoto, pero ello conlleva riesgos. Una forma de mitigar estos es mejorar la seguridad de las claves de ingreso, ya sea pidiendo una segunda clave creada solo para estos efectos, o usando un sistema de autenticación de dos factores (en que al trabajador le llega una clave numérica al celular cada vez que ingresa a la red).

1.2 Invertir en software de seguridad, incluyendo redes privadas virtuales (VPN), sistemas de encriptación de las comunicaciones y programas antivirus, que deben mantenerse actualizados en cada equipo.

2. <u>Capacitar a los trabajadores</u>.

Nuevamente, la premura de la emergencia hace poco factible que las empresas hayan podido darle una debida capacitación a los trabajadores conectados desde su domicilio. Sin embargo, será útil que la empresa pueda hoy –mediante videoconferencias, comunicaciones por correo electrónico o incluso la suscripción de anexos de contratos— enfatizar a sus colaboradores algunas medidas de seguridad básica para esta modalidad de trabajo:

2.1 No utilizar los equipos de trabajo para otros fines.

El uso de los computadores de la oficina para fines privados aumenta el riesgo de que estos sean infectados por virus, e incluso capturados por programas de ransomwear.

2.2 Tener precaución de los intentos de phishing.

La revista Forbes reveló que los intentos de phishing (el uso de correos electrónicos de origen falso para propagar virus) ha aumentado un 350% desde el inicio de la pandemia. El 22% de los norteamericanos reporta haber sido blanco de intentos de ciberfraude. Por ello, es fundamental que los trabajadores a distancia no bajen archivos de origen dudoso ni sigan links si no están seguros de su autenticidad.

En particular, los trabajadores remotos pueden estar expuestos al spear-phishing, en que los criminales se hacen pasar por gerentes o jefes de la propia empresa. Una buena práctica es que los trabajadores siempre verifiquen que el correo venga de quien dice antes de abrir archivos adjuntos.

2.3 No usar redes de wi-fi desconocidas.

Aunque es poco probable que los trabajadores puedan acceder a redes públicas durante la cuarentena, es indispensable enfatizar que éstas nunca deben usarse para tratar datos de la empresa, aun después de pasada la emergencia. Ello, por cuanto aumentan significativamente el riesgo de que terceros intercepten las comunicaciones.

2.4 No bajar aplicaciones no autorizadas.

La empresa debe señalar cuáles aplicaciones pueden ser utilizadas para el trabajo. Cualquier otra aplicación debe ser consultada con los expertos de ciberseguridad de la empresa, para evitar descargar programas que espíen o capturen la información contenida en los equipos.

2.5 Evitar usar equipos externos de almacenamiento.

Estando en casa, es más probable que un trabajador pueda recurrir a algún viejo pendrive o disco duro externo para almacenar datos. Ello aumenta considerablemente el riesgo de seguridad de los equipos. La empresa debe proporcionar estos dispositivos, si son necesarios.

3. Proteger los datos de los clientes.

Para asegurar la integridad de los datos de los clientes, y evitar su posible difusión, algunas medidas útiles para los trabajadores son:

3.1 Usar medidas para la seguridad física de los documentos: en lo posible, los trabajadores a distancia deben contar con cajas de seguridad bajo llave para almacenar los documentos de trabajo. Si no, en la medida de lo posible dejar los documentos en piezas o cajones que se puedan cerrar con llave. Igualmente, los computadores deben quedar resguardados cuando no se estén usando.

3.2 No transmitir documentos por vías poco seguras: si se han instalado medidas de seguridad como un VPN o sistemas de cifrados, estos deben usarse siempre, evitando la tentación de utilizar mecanismos menos engorrosos, como Whatsapp, para transmitir información entre colegas.

3.3 Avisar a los clientes y, en lo posible, conseguir su consentimiento: claramente, ni las empresas ni sus clientes pudieron prever esta repentina necesidad de trabajo a distancia. Por ello, es recomendable que las empresas comuniquen a los clientes de la extensión del teletrabajo, de las medidas de seguridad que se han empleado y, sin es factible, solicitarles que den su consentimiento expreso para ello. Esta precaución servirá para tranquilizar a los clientes y mitigar la posible responsabilidad futura por casos de brechas.

*****

En caso de requerir más información contactar a **Andrés Culagovski** aculagovski@abdala.cl de nuestra Área de Protección de Datos y Ciberseguridad.