ECIJA
Torre Mural. Av. Insurgentes Sur 1605 piso 10
Col. San José Insurgentes, C.P. 03900,
Ciudad de México, México
Tel: (+52) 5556626840
www.ecija.com

nota informativa

Ciudad de México, 27 de enero de 2023

Trabajo remoto: retos en materia de ciberseguridad

La adaptación del trabajo al modelo remoto presenta grandes oportunidades y beneficios, tanto para las empresas como para sus trabajadores. No obstante, esta nueva modalidad de trabajo no está exenta de riesgos, **siendo particularmente relevante la seguridad de la información y datos utilizados por los trabajadores**.

La legislación laboral mexicana establece como obligación de los patrones, el implementar mecanismos que preserven la seguridad de la información y datos que son tratados por los trabajadores que se encuentren en la modalidad de trabajo remoto o teletrabajo.

Sin embargo, ¿cuáles pudieran ser estos mecanismos? o ¿Qué criterios debieran seguirse para su elección? **Todo dependerá del tipo de información y datos de que se traten, el riesgo al cual se encuentra expuesta la información y las consecuencias que pudiera derivar de su vulneración**. La consideración de estos factores resulta obligatoria en la determinación de las medidas de seguridad para proteger los datos personales.

Para ello, la normatividad de la materia prevé la elaboración de un inventario de los datos personales y de los activos involucrados en su tratamiento y almacenamiento (ej.: personal, procesos, hardware, software, redes, telecomunicaciones, etc.), así como un análisis de riesgo de los mismos, para con base en ello seleccionar e implementar las medidas de seguridad que permitan mitigar algún incidente, considerando las medidas ya existentes contra las que serían convenientes o necesarias de implementar.

Dentro de las acciones previstas para establecer y mantener la seguridad de los datos personales, se contemplan el establecimiento de políticas internas y la capacitación de los trabajadores, con la finalidad de que éstos conozcan los lineamientos y criterios aplicables dentro de la empresa respecto a la seguridad de la información.

Para poner lo anterior en un contexto más gráfico, abordaremos el uso de dispositivos del propio trabajador para el desempeño de sus laborales (ej.: smartphones, laptops, tablets, etc.), ya sea para leer y contestar correos institucionales, acceder a bases de datos de la empresa, interactuar con clientes y proveedores, etc. Esta práctica es cada vez más común y es conocida como Bring Your Own Device (BYOD).

Sin perjuicio de las ventajas que ofrece esta práctica, es importante considerar y gestionar los riesgos que conlleva en la seguridad de la información de la empresa,

como es la pérdida de la información por virus, daño o robo del dispositivo, o inclusive por la eventual terminación de la relación laboral.

En ese sentido, **se vuelve relevante el diseño e implementación de una política BYOD que regule el acceso a los recursos de la empresa, a través de los dispositivos personales de los trabajadores**. Estas políticas por lo regular contemplan la instalación de elementos mínimos, como contraseñas, antivirus o cifrado de bases de datos, acciones a seguir en caso de dispositivos perdidos o robados, entre otras.

También es recomendable contar con procedimientos para la encriptación y cifrado de información. El cifrado permite codificar la información de tal forma que la misma no sea inteligible ni manipulable por terceros. Esto se sugiere especialmente en el tratamiento de datos personales sensibles (crecencias religiosas, estado de salud, preferencias sexuales, etc.).

Otros procedimientos que se consideran indispensables son los relativos al uso de medios tecnológicos y notificación de incidencias. El primero tiene por objeto regular el uso adecuado de equipos, correos institucionales, internet, servicios de cómputo en la nube o cualquier otro recurso de la empresa; y el segundo busca establecer un protocolo de actuación en casos de vulneraciones a la seguridad.

La implementación de un sistema de gestión de seguridad integral no sólo permite a las empresas dar cumplimiento a sus obligaciones en materia laboral y de protección de datos personales, sino también mitigar riesgos inherentes a sus operaciones y así garantizar la continuidad de su negocio ante eventuales incidencias.

Noticias destacadas: Fraudes cibernéticos

El 26 de octubre de 2022, la Guardia Nacional publicó las modalidades fraude más comunes con la finalidad de alertar a la población; a saber: suscripciones gratuitas con códigos maliciosos; comunicados falsos con el objetivo de confundir a los usuarios; correos alarmantes para obtener información personal o financiera; servicios gratuitos (smishing) que ofrecen premios al entrar a un link fraudulento; correos spam con archivos maliciosos; ofertas atractivas que suelen ser irreales y pueden derivar en robo; y páginas apócrifas (phishing) que solicitan donativos o información.

Con el fin de evitar ser víctimas de fraudes en línea, la Guarda Nacional recomienda, tomar las siguientes medidas, entras otras: utilizar tarjetas para uso exclusivo de compras online; navegar a través de conexiones y sitios seguros; actualizar dispositivos utilizados para realizar operaciones bancarias y mantener instalados antivirus; validar la descripción de los productos o servicios a adquirir; utilizar dispositivos propios para realizar compras en línea; comprar en sitios web reconocidos o con buena reputación; proporcionar solamente datos estrictamente necesarios; y activar notificaciones de compra de tarjetas bancarias.

Área de TMT ECIJA México
socios.mexico@ecija.com
info.mexico@ecija.com