ABDALA & CIA
ABOGADOS

Porqué Es Importante Hacer Ahora Una Evaluación De Impacto De La Protección De Datos

Ante la contingencia de la crisis sanitaria, muchas empresas han visto cambiada radicalmente la forma de relacionarse con empleados, proveedores y clientes. Una de las consecuencias de esta nueva realidad es un aumento explosivo de los ciberataques, que buscan vulnerar la seguridad informática de las empresas. Uno de sus objetivos es obtener información personal de sus clientes, lo toque podría generar grandes perjuicios y gatillar su responsabilidad legal. Las empresas deben prevenir estos ataques, y una de las herramientas más eficaces para ello es la **Evaluación de Impacto de la Protección de Datos**.

I. ¿Qué es el phishing y porqué aumentó con el coronavirus?

Según la empresa Microsoft, el 91% de los ciberataques se inicia a través del correo electrónico. Estos ataques, conocidos como phishing, buscan incitar a la víctima a revelar datos personales o a abrir archivos adjuntos, que típicamente instalan aplicaciones maliciosas en sus computadores.

Como explica un experto de la BBC, los ataques de phishing siempre comparten una hebra común: la incitación o dependencia en una emoción que nos hace actuar de manera intespectiva o pensar menos en nuestras acciones. Las condiciones de encierro y trabajo a distancia causados por la pandemia han gatillado un aumento de más de 600% en el envío de correos de phishing. Google reporta que elimina 100 millones de correos de phishing al día, y que muchos de ellos hacen referencia al coronavirus.

Estos ataques se han vuelto cada vez más sofisticados, afectando a empresas de mayor tamaño y complejidad. En 2017 se reveló que Facebook y Google mandaron más de US$ 100 millones cada una a un estafador en Lituania, que se hacía pasar por un proveedor de tecnología basado en Taiwán.

II. Responsabilidad por la protección de datos.

Si bien la ley chilena actual, número 19.628, contiene mecanismos institucionales y sancionatorios relativamente poco usados para estos casos, los tribunales de justicia han establecido claramente la responsabilidad de las empresas por brechas de datos con perjuicio para sus clientes.

Así, por ejemplo, la Corte de Apelaciones de Santiago, en 2017, condenó a un banco nacional a restituir a una cliente dineros sustraídos a una cliente mediante el phishing, en función de sus obligaciones de resguardo respecto de los fondos de la cuenta corriente y tarjeta de crédito contratadas por la clienta. La Corte Suprema confirmó dicha sentencia el año 2019.

En un fallo de la propia Corte Suprema en 2019, que nuevamente responsabilizó a la empresa de la pérdida de datos, un voto concurrente enfatizó que las obligaciones de monitoreo y control de fraudes recaen expresamente en las instituciones que manejan los datos, donde los patrones de conducta del cliente son elementos de juicio para la determinación de una operación engañosa.

III. ¿Para qué sirve una Evaluación de Impacto de la Protección de Datos?

Una Evaluación de Impacto de la Protección de Datos (EIPD) revisará confidencialmente todos los procesos de tratamiento de datos que hace la empresa, tanto respecto de sus clientes y proveedores; en sus actuaciones internas; y respecto a empresas que provean servicios informáticos, como archivos remotos. El EIPD levantará los riesgos a que están expuestos los datos y establecerá un plan de acción para su mitigación. Finalmente, el EIPD propondrá un calendario de auditoría continua, para detectar y controlar el surgimiento de nuevos riesgos.

IV. Preparación para la nueva ley.

Además de hacer frente al mayor riesgo que conlleva la cuarentena por coronavirus, realizar desde ya un EIPD ayudará a la empresa a hacer frente a los cambios legales previstos para el futuro cercano. Un proyecto de ley actualmente en trámite en el Senado, y de pronto despacho a la Cámara de Diputados, obligará a las empresas que hacen tratamiento masivo de datos a hacer un EIPD, y será un mitigante de responsabilidad para cualquier empresa afectada.

Este proyecto sigue el esquema de las leyes ya vigentes en Europa, que afectan a todas las empresas que buscan tratar datos personales de residentes en la Unión Europea. La pronta realización de un EIPD puede detectar los riesgos surgidos en esos contactos, evitando multas y posibles efectos nocivos sobre sus operaciones internacionales.