POLÍTICA DE SEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES

Objeto

Esta política tiene como objeto brindar fundamentos herramientas y procedimientos necesarios para proteger información de carácter personal, como también su tratamiento en los registros, archivos y bases de datos almacenados en la compañía.

La presente política provee un esquema de gestión destinado implementar y mantener cierto nivel de seguridad de la información de los riesgos que se presenten y cuyo propósito es:

Garantizar que la información esté segura.

Que se cumpla con las obligaciones regulatorias.

Poner de manifiesto la postura de UBICAR en lo que respecta a la prevención, atención y seguimiento de incidentes de seguridad de la información.

Informar que se habilitan y disponen los mecanismos necesarios para el tratamiento adecuado y coordinado de los conceptos de seguridad.

Alcance.

Esta política aplica todo personal de UBICAR que tenga acceso a información de carácter personal sobre clientes, prestadores, proveedores y empleados de la compañía. También aquella persona que realiza operaciones sobre la información estará alcanzada por esta política. Todo el personal deberá respetar sin excepción las normas estándares guías de mejores prácticas y procedimientos de la seguridad en información derivada de la presente política.

Definiciones.

La ley 25326 tiene como objeto proteger los datos de las personas sentados en archivos, registros, bancos de datos y/u otros mecanismos técnicos de control , sean estos públicos o privados, otorgando protección a los ciudadanos sobre su derecho a la intimidad, facilitando el control de la información personal, del acceso a datos personales contenidos en los distintos bancos de datos, de conformidad a lo establecido en artículo 43, párrafo tercero de la Constitución Nacional (artículo 1º de la ley 25 326)

La citada ley reglamentó la actividad de los bancos de datos públicos y privados que procesan información personal por medios informáticos o manuales y los sometió al control de la Dirección Nacional de Protección de Datos Personales (en adelante DNPDP) en el ámbito nacional, creándose el Registro Nacional de Bases de Datos, a fin de que los ciudadanos puedan conocer la existencia de los bancos de datos y la información que los mismos contienen sobre ellos.

Datos personales: información de cualquier tipo referida a personas físicas o de existencia ideal determinadas o determinable (artículo 2 de la ley número 25326).

Datos sensibles: datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o la vida sexual (artículo 2 de la ley 25326)

Archivo, registros, base o banco de datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico no (puede ser en papel), cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso (artículo 2 de la ley 25326).

Tratamiento de datos: operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, y en general el procesamiento de datos

personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

Titular de los datos: toda persona física o persona de existencia ideal con domicilio legal o delegaciones o sucursales en el país, cuyos datos sean objeto de tratamiento que se da dentro de la compañía, como resultado de una relación contractual.

Responsable de seguridad

Si bien toda la organización es responsable del mantenimiento de un adecuado nivel de seguridad de los archivos con datos personales, se define la función de responsable de seguridad de la privacidad responsable de seguridad informática. Ubicar delega en la función de seguridad informática el desarrollo, la implementación y mantenimiento de las medidas de seguridad que resulten necesarias para resguardar la información y los distintos dispositivos informáticos y de red que posee UBICAR. Para ello participa en los desarrollos, adquisiciones o modificaciones de los sistemas informáticos y de red, y coordina las acciones preventivas, correctivas, o de mejora sobre los sistemas en producción para mantener la integridad, confidencialidad y disponibilidad de la información que utiliza para su gestión comercial.

El personal con funciones de seguridad informática deberá contar con recursos propios, no pudiendo cumplir estas responsabilidades, personal de terceros.

Se designa como responsable de la gestión de la seguridad informática en la firma a UBICAR SRL

Confidencialidad de los datos personales.

Toda persona alcanzada por esta política que intervenga en cualquier fase de tratamiento de datos personales de asociados, proveedores, prestadores clientes y personal de la compañía deberá cumplir con las obligaciones y funciones documentadas en la siguiente normativa "Manual de Seguridad"

Los mismos también deberán aceptar los términos de los convenios de confidencialidad de la compañía en relación a la información que administra la misma, firmando y dejando una copia dentro de la empresa.

Recolección de datos.

UBICAR deberá recolectar información de clientes, prestadores, empleados, de manera lícita, dando a conocer los fines para los cuales los mismos serán utilizados, y recibiendo el consentimiento expreso de la persona que los otorga. También deberá informar que la persona que sus datos pueden ejercer su derecho de acceso, modificación y eliminación de datos, de manera gratuita hasta dos veces al año.

(Artículo 14 inciso tres de la ley 25326)

Seguridad de los datos

Todas las personas que trabajan para UBICAR así como los terceros que prestan servicios, deberán tener acceso sólo a la información necesaria para el desarrollo de sus actividades laborales, y con el único propósito del cumplimiento de las mismas.

Usuarios

Todas las personas que trabajan para UBICAR, así como los terceros que prestan servicios, deberán firmar los acuerdos de confidencialidad y no divulgación de la información, previo otorgar el acceso a la información de Ubicar

Todo usuario que requiera acceder a datos o información de ubicar, deberá poseer un código de usuario contraseña que lo acredite frente a los sistemas, los cuales serán exigidos previo a su ingreso y validados por un mecanismo de comprobación que certifique la validez de los mismos. Dicho código es personal e intransferible siendo su propietario responsable por su uso y toda actividad realizada con la misma.

Resguardo de información

Toda plataforma tecnológica propiedad de UBICAR o de terceros, donde se procese y manipulé datos e información, deberá cumplir con todas las medidas vigentes de resguardo que garanticen los principio de confidencialidad, integridad, disponibilidad y seguridad física de la información.

Todo sistema de información, conjunto de datos y plataforma tecnológica deberá poseer los planes de contingencias y recursos que asegure la continuidad de los procesos de negocios en tiempo razonable y recupero de los datos, contemplando como mínimo las aplicaciones críticas y los riesgos más probables de ocurrencia que puedan afectar su continuidad.

Segregación de ambientes de desarrollo producción: los distintos ambientes del ciclo de vida de los aplicativos informáticos, deberán estar debidamente segregados y protegidos, minimizando el riesgo de acceso no autorizado su información y programas allí contenidos. Los sistemas de información y plataformas tecnológicas utilizadas en los procesos productivos de ubicar, deberán emplear un procedimiento de control de cambio que verifique y asegure que sólo se realizaran los cambios autorizados, los cuales no podrán ser ejecutados, aprobados , implantados por la misma persona, de modo tal que disminuyan la seguridad existente.

Cualquier convenio con terceros que involucre elementos que procesan datos e información, deberán cumplir con las medidas de seguridad informática vigentes.

Antivirus

Toda estación de trabajo y servidor de la compañía, deberá tener instalado y en funcionamiento software antivirus provisto por UBICAR, caso contrario la misma no podrá conectarse a la red interna de UBICAR.

TRANSFERENCIA INTERNACIONAL DE DATOS

UBICAR no realiza ningún tipo de transferencia internacional de datos, y la misma se encuentra prohibida, con las siguientes excepciones:

Colaboración judicial internacional;

Cooperación internacional con organismos de inteligencia;

Tratados internacionales de los cuales la República Argentina participe.

Tratamiento en el exterior de un asociado, o investigación epidemiológica; para estos casos la información debe ser enviada de forma disociada y cifrada.

PUBLICIDAD DIRECTA

En toda comunicación con fines de publicidad directa, UBICAR incorporará un aviso informando al titular del dato sobre los derechos de retiro o bloqueo total o parcial, de su nombre de la base de datos, previendo como mecanismo para su ejercicio la recepción de un email en la casilla info@ubicar.net con más la transcripción del artículo 27, inciso 3, de la Ley Nº 25.326 y el párrafo tercero del artículo 27 del Anexo I del Decreto Nº 1558/01.

A su vez dichas comunicaciones deberán incluir los siguientes párrafos según lo dispuesto por la Disposición 10/08:

"El titular de los datos personales tiene la facultad de ejercer el derecho de acceso a los mismos en forma gratuita a intervalos no inferiores a seis meses, salvo que se acredite un interés legítimo al efecto conforme lo establecido en el artículo 14, inciso 3 de la Ley Nº 25.326".

"La DIRECCION NACIONAL DE PROTECCION DE DATOS PERSONALES, Órgano de Control de la Ley Nº 25.326, tiene la atribución de atender las denuncias y reclamos que se interpongan con relación al incumplimiento de las normas sobre protección de datos personales".

Estas dos últimas leyendas, deberán también incluirse en los formularios de recolección de datos de la página web de UBICAR.

SERVICIOS DE TERCEROS

Cuando UBICAR contratare servicios de terceros que involucren la necesidad de consulta o manipulación de datos personales a través de sistemas o aplicaciones de UBICAR o bien de los terceros involucrados, deberán incluirse en el contrato de servicios celebrado, cláusulas que indiquen cuál o cuáles serán los fines para los que serán tratados los datos personales. También deberá dejarse asentado que los datos no deberán cederse a otro tercero, ni tampoco conservar los datos personales una vez finalizado el contrato.

Por otro lado, se deberán firmar los convenios de confidencialidad y no divulgación de datos personales, con los terceros que manipulen dicha información.

DERECHOS DE LOS TITULARES DE DATOS

Conforme a lo expresado en los artículos 14, 15, y 16 de la ley 25326 Protección de Datos Personales, todo titular de datos o su representante legal tiene el derecho a solicitar y obtener información de sus datos personales, como también el derecho a modificación y supresión de los mismos.

UBICAR, previa recepción de solicitud firmada por el titular de datos o su representante legal, y luego de comprobar la identidad de solicitante, procederá a otorgar la información dentro de los plazos establecidos por la ley. En caso de que la solicitud no cumpla los requisitos mínimos solicitados, UBICAR podrá denegar la misma.

UBICAR dispone de la norma interna "Ejercicio de Derecho a Acceso" que permite facilitar las tareas relacionadas con el tema, como también pone a disposición un formulario estandarizado para entregar a asociados que quieran ejercer sus derechos.

CONCIENTIZACIÓN

Definición

La información es uno de los recursos más valiosos de UBICAR. La seguridad de la información es una responsabilidad diaria de cada integrante de la compañía, y la pérdida de la misma puede provocar la pérdida de horas-hombre invertidas en generarla, como también en caso de tratar de recuperarla. Por otro lado, si la misma se pierde fuera del ambiente de UBICAR., permite que los competidores se aprovechen de esta situación para beneficio propio. En este título se mencionan los lineamientos de implantación y ejecución para tomar conciencia de la importancia de la información.

Pautas para la concientización

Se les comunicará la política de seguridad de la información y los procedimientos relacionados establecidos por UBICAR a los empleados actuales, terceros que accedan y/o utilicen nuestros sistemas, y a todos aquellos que se incorporen en un futuro. Todos los empleados existentes y los que se incorporen, deberán firmar el Convenio de Confidencialidad de la compañía.

Todas las novedades relacionadas a la seguridad de la información se publicarán para asegurar que todos los empleados que están afectados o alcanzados por las políticas de seguridad, tengan acceso a ellas.

Responsabilidades

Del Responsable de Seguridad Informática y de Recursos Humanos: difundir una cultura de seguridad de la información entre todos los empleados de la compañía.

De los empleados y terceros con acceso a sistemas de información de UBICAR: acordar por escrito que desempeñan su trabajo respetando lo especificado en el Convenio de Confidencialidad acompañado de su firma. Leer y comprender toda la información relacionada con la seguridad de la información, comprometiéndose a cumplir con todas aquellas normas y políticas publicadas y alentadas por UBICAR.