Funciones y Obligaciones del Personal en relación con la Seguridad en los Sistemas de Información

OCTUBRE 2020

Agustín Manuel Chávez 1-1, Centro de Ciudad Santa Fe, 01210, México, DF, tel. +52(55) 5292 5232, fax +52(55) 5292 5233,
www.bgbg.com.mx

ÍNDICE

1. INTRODUCCIÓN

En el marco de la Política de Protección de Datos Personales adoptada por Vitro Canceles, S.A. de C.V. (en adelante "Responsable"), se ha desarrollado una Política de Protección de Datos Personales para proteger este tipo de información en posesión de nuestra organización, con una clara orientación hacia la Seguridad de la Información. El objetivo es claro: proteger como activo esencial las bases de datos de la organización.

La seguridad es cosa de todos, y por este motivo, pedimos tu participación en la protección de los sistemas informáticos y de la información contenida en ellos. Esta Norma implica los principales aspectos y medidas que debes conocer y aplicar en tu aportación a la seguridad, con el fin de reducir la probabilidad de fallos y daños causados por problemas de seguridad.

2. OBJETO

El presente documento forma parte de la política interna de Protección de Datos Personales y, tiene por objeto establecer los controles de seguridad necesarios para el buen uso de los sistemas de información, para que estos puedan ser conocidos y aplicados por todos los empleados del Responsable y por sus colaboradores externos, a fin de reducir la probabilidad de vulneraciones de seguridad relacionados con el tratamiento de información y datos personales.

3. ÁMBITO DE APLICACIÓN

Esta norma es aplicable con carácter obligatorio a toda la organización, así como a las entidades colaboradoras que hagan uso de la información y de los sistemas propiedad del Responsable para el desarrollo de sus actividades, en cualquier momento del ciclo de vida de la información.

Asimismo, esta Norma es aplicable, en todo aquello que resulte procedente conforme a la naturaleza de los soportes que la contengan, tanto a los sistemas de información automatizados que tratan datos personales como a los sistemas de información manuales o no automatizados (papel), y por extensión a los sistemas mixtos que traten dichos datos personales.

Cualquier actuación que afecte a la seguridad de la información deberá ajustarse a las disposiciones y recomendaciones del presente documento.

Esta norma está basada en criterios y buenas prácticas internacionales como marco de referencia, adoptando las precauciones necesarias para garantizar el nivel de seguridad exigido por la legislación Vigente: Ley Federal de Protección de Datos Personales en Posesión de los Particulares (en adelante, la LFPD) y su Reglamento.

El presente documento forma parte integral de la Política de Protección de Datos del Responsable, es una extensión a las funciones y obligaciones del personal.

4. DIRECTRICES DE SEGURIDAD

4.1 Directrices Generales

Todos los empleados y colaboradores del Responsable están obligados al secreto profesional y al deber de confidencialidad, obligación que subsistirá aún después de finalizar sus relaciones con el Responsable.

El personal deberá proteger y hacer buen uso de los activos de la organización, incluyendo: sistemas de información, equipos de cómputo, información confidencial, mobiliario que se le ha otorgado para llevar a cabo sus funciones y material de oficina.

Los activos del Responsable deberán utilizarse para propósitos relacionados con el trabajo diario. El uso personal de los recursos asignados a cada empleado será acorde con el uso racional admitido por la empresa. Cualquier uso de los recursos o instalaciones de la empresa que se haga con fines distintos a los autorizados está estrictamente prohibido.

Los usuarios están obligados a utilizar las redes, en su caso, intranet y sus datos, sin incurrir en actividades que puedan considerasen ilícitas o ilegales, que infrinjan los derechos de la empresa o de terceros, o que puedan atentar contra la moral o las normas de conducta y códigos de ética.

Cuando el colaborador abandone su puesto de trabajo, deberá verificar que el material y la documentación de trabajo se encuentra debidamente guardado y con las medidas de protección correspondientes, prestando especial atención a toda aquella información cuya divulgación pudiera perjudicar los intereses del Responsable.

El Responsable garantizará la protección de las instalaciones y los activos de la organización dentro de las mismas instalaciones.

4.2 Uso de los identificadores de Usuario

Todos los empleados y colaboradores del Responsable deberán mantener en secreto los datos relativos a su “usuario” y “contraseña” que utilicen para acceder a cualquier equipo de cómputo, programa de software para llevar a cabo sus actividades diarias, aplicaciones móviles o, en su caso, las que sean necesarias para el acceso a instalaciones.

Queda expresamente prohibido compartir o facilitar dicha información a otra persona, sea ésta personal del Responsable o colaborador, a fin de garantizar su privacidad y asumir las responsabilidades del uso que haga de la misma.

No se deberán anotar las contraseñas en lugares visibles o fácilmente accesibles como la pantalla o el teclado; a fin de evitar que usuarios no autorizados pudieran hacer uso de las mismas.

Si el usuario sospecha que otra persona conoce sus datos de identificación y acceso, procederá a su cambio y a su notificación al Registro de Incidencias.

4.3 Uso de los Sistemas de Información Automatizados

Todos los sistemas, redes y terminales utilizados por los empleados son propiedad del Responsable, siendo el personal designado y autorizado por el Área de Sistemas el encargado de su mantenimiento y supervisión.

Todos los usuarios deberán de utilizar el software cuyas licencias han sido adquiridas por el Responsable, y homologado para su utilización.

Los usuarios habilitarán las medidas de seguridad que sean establecidas o necesarias para garantizar la autoprotección de su equipo y la seguridad en su entorno de trabajo.

El usuario comprobará que su terminal o terminales tienen actualizados el programa antivirus para prevenir la entrada en el sistema de cualquier elemento destinado a destruir o corromper los datos informáticos.

Ningún empleado o colaborador podrá, bajo ninguna circunstancia, desactivar los sistemas de seguridad de su equipo, ni incorporar otros, sin consultarlo previamente con las unidades responsables y más concretamente con Área de Sistemas.

Todos las PCs, computadoras portátiles (*laptops*), *tablets* y *smartphones* utilizados por los empleados y colaboradores del Responsable en el desarrollo de sus funciones deberán utilizar la función de blockeo antes de abandonar su puesto de trabajo. Así como apagar adecuadamente y resguardar el equipo de cómputo a la conclusión de su jornada laboral.

Todos los empleados y colaboradores del Responsable deberán de comunicar cualquier anomalía derivada del mal funcionamiento del hardware, software o virus informáticos, al Registro de Incidencias habilitado a tal efecto.

Se deberá informar al personal de sistemas de cualquier vulneración en el momento que se lleve a cabo, que deberá quedar registrada en el documento indicado por el departamento de protección de datos.

Estará prohibido la utilización de los equipos informáticos y la información del Responsable para fines particulares, incluso fuera del horario habitual de trabajo. Por lo anterior, se deberán tomar las medidas adecuadas de seguridad, para evitar que la información física o automatizada salga de las oficinas.

4.4 Confidencialidad de la Información

Todos los empleados y colaboradores del Responsable, cuando abandonen su puesto de trabajo, guardarán toda la información que estén tratando, de forma que no queden desatendidos los CD’s, memorias portátiles, listados o la información visible en la propia pantalla del PC.

Cuando se trate de equipos compartidos de impresión, éstos deberán asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos que deban estar protegidos. Si la impresora es compartida con otros usuarios no autorizados para acceder a los datos, los responsables de cada puesto deberán retirar los documentos conforme vayan siendo impresos.

La información será distribuida exclusivamente a quien debe disponer de ella y evitar que las personas que no deban tener acceso a esa información puedan conocerla.

Todos los empleados y colaboradores del Responsable deberán conocer y emplear los medios necesarios para destruir los soportes que contengan información confidencial antes de su desechado o reutilización.

Los colaboradores no deberán tener acceso a información propiedad del Responsable, distinta a la que sea absolutamente necesaria para realizar sus funciones.

Queda estrictamente prohibido el uso de programas o aplicaciones que carezcan de la correspondiente licencia. Asimismo, queda prohibido el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención protegida por los derechos de propiedad intelectual o industrial del Responsable, sin permiso expreso y por escrito de la Dirección General de la empresa.

4.5 Software Malicioso y Antivirus

Todos los empleados y colaboradores del Responsable deben de conocer los peligros que pueden ocasionar el software malicioso o no autorizado. Un virus o software malicioso es un programa informático que produce acciones nocivas en el sistema informático en el que actúa. Existen distintos tipos de virus o códigos dañinos como:

- Virus Informáticos: Código que es capaz de generar copias de si mismo en programas distintos al que ocupa.
- Gusanos: Código que absorbe recursos del sistema, de forma creciente, hasta que lo bloquea por saturación.
- Caballos de Troya: Programa de uso autorizado que contiene un código dañino. Cuando este programa comienza a ejecutarse, el código dañino toma el control del sistema.
- Bombas Lógicas: Código que se ejecuta al producirse un hecho predeterminado, por ejemplo, una determinada fecha, un número de encendidos del sistema, determinada secuencia de teclas, etc.
- Phishing: modelo de software utilizado para adquirir información confidencial de forma fraudulenta.
- Spyware: Software utilizado para recolectar información de una persona o una organización sin que éstos se percaten que está sucediendo.

Para evitar el software malicioso, todos los empleados y colaboradores del Responsable deberán tener en cuenta las siguientes medidas:

- Tendrán instalado y actualizado un antivirus para detectar y reparar de forma rutinaria su equipo de trabajo.
- Comprobarán cualquier archivo recibido de fuentes desconocidas, archivos descargados de Internet o recibidos por otros medios (CD's, memorias externas, etc.). Éstos deben ser convenientemente revisados en busca de la presencia de virus.
- Cualquier infección detectada tiene que ser notificada al Registro de Incidencias, para el aislamiento de los sistemas afectados y la eliminación del virus.

4.6 Uso del Correo Electrónico

Como norma general, todos los empleados del Responsable y el personal externo tienen prohibido el uso de correo electrónico corporativo para fines particulares.

Los empleados podrán utilizar el correo electrónico, su e-mail corporativo, con libertad y en el sentido más amplio, para el desempeño de las actividades de su puesto de trabajo.

Se debe seleccionar cuidadosamente la información enviada por correo electrónico con el fin, en su caso, de implementar las medidas de seguridad que requiera el tipo de información que por este medio se transmita (cifrado, firma electrónica, etc.)

Queda expresamente prohibido enviar mensajes con anexos de gran tamaño o realizar envíos sin relación alguna con el desempeño profesional.

Todos los empleados deberán ser extremadamente precavidos con la recepción de archivos adjuntos de remitentes desconocidos.

Está terminantemente prohibido intentar leer, borrar, copiar o modificar los mensajes de correo electrónico o archivos de otros usuarios sin su consentimiento.

Está terminantemente prohibido abrir todos los archivos de procedencia dudosa sin adoptar las medidas de seguridad que eviten poner en peligro los Sistemas de Información.

Está prohibido el envío de mensajes o imágenes de material ilegal, ofensivo, difamatorio, inapropiado o con contenidos discriminatorios por razones de género, edad, sexo, discapacidad, etc.

Cuando existan indicios de uso ilícito o abusivo por parte de un empleado, la empresa está facultada para realizar las comprobaciones oportunas y, si fuera preciso, para efectuar una auditoría en la computadora del empleado o en los sistemas que ofrecen el servicio. Esta revisión se efectuará en horario laboral y, si el empleado lo desea, en presencia de algún representante de los trabajadores, respetando en todo caso la intimidad y demás derechos del empleado.

4.7 Uso de Internet

El empleo de los sistemas de Información del Responsable para acceder a redes públicas como Internet, se limitará a aquellos aspectos directamente relacionados con la actividad de la empresa y las responsabilidades propias del puesto de trabajo del usuario.

Se prohíbe la descarga de archivos sin haber adoptado las medidas que eviten peligros a los sistemas, quien incumpla esta norma será el responsable de sus posibles efectos.

El acceso a páginas web (www), grupos de noticias (Newsgroups) y otras fuentes de información como CHATS, RSS, etc., se limitará a aquellos que contengan información relacionada con la actividad del Responsable.

No estará permitido el acceso a redes sociales personales desde los equipos de cómputo de la compañía. En este sentido, tampoco se permitirá utilizar los perfiles personales para contactar a prospectos o clientes de la organización.

4.8 Comunicación de Incidencias

Todo el personal y colaboradores del Responsable estarán obligados a comunicar al Departamento de Datos Personales para el registro de incidencias de cualquier irregularidad que se produzca en los sistemas de información a los que tenga acceso.

Dicha comunicación deberá realizarse con la mayor brevedad desde el momento en que se produzca o se tenga conocimiento de la incidencia correspondiente.

Toda investigación de incidencias, así como la manipulación de la información que se origine, en cualquier tipo de soporte, será realizada por personal autorizado y con conocimientos técnicos relevantes.

El conocimiento y la no notificación de una incidencia por parte de un usuario serán considerados como una falta contra la seguridad de los sistemas de información por parte de ese usuario.

5. RESPONSABILIDADES

El Área de Sistemas tendrá la responsabilidad de promover y apoyar el establecimiento de medidas técnicas, organizativas y de control que garanticen la autenticidad, integridad, disponibilidad, confidencialidad y trazabilidad de la información.

La gestión de esta Norma corresponde al responsable del Departamento de Datos Personales del Responsable, que podrá solventar las dudas que puedan surgir en su aplicación, así como proceder a su revisión cuando sea necesario, para actualizar su contenido o porque se cumplan los plazos máximos establecidos para ello, verificando su efectividad en todo momento.

Lo anterior, como parte de sus funciones como Departamento de Datos Personales, dentro de las que se encuentra las siguientes:

- Coordinar, gestionar y ejecutar las medidas y acciones necesarias para tramitar y responder en tiempo y forma las solicitudes de ejercicio de los derechos ARCO y de revocación del consentimiento que formulen los titulares de datos personales, en coordinación con los Responsables Funcionales.
- Adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, reglas vigentes de aspecto organizativo, así como las consecuencias en que dicho personal pudiera incurrir en caso de incumplimiento. A tales efectos, deberá contar con el apoyo de los Responsables Funcionales.
- Determinar junto con el Área de Sistemas el nivel de seguridad recomendable para las bases de datos personales, en función de los tipos de datos contenidos en las mismas; controlar junto con el Área de Sistemas la adopción de las medidas definidas en la Relación de Medidas de Seguridad de cada base de datos.
- Asegurar junto con el Área de Sistemas el establecimiento de procedimientos de identificación y autenticación para el acceso a los datos personales tratados por el Responsable.
- Autorizar las personas y Unidades que, de acuerdo con las necesidades de gestión, puedan acceder a la información, según las solicitudes dirigidas por los Responsable Funcionales de las bases de datos.
- Actualizar junto con el Área de Sistemas la Relación de Medidas de Seguridad de las bases de datos, cuando sea procedente de conformidad al Reglamento de la LFPD.
- Realizar revisiones de control sobre el cumplimiento y seguimiento de las normas y procedimientos establecidos en la Relación de Medidas de Seguridad.
- Analizar, junto con los Responsables Funcionales y el Área de Sistemas, los Informes de Auditoría que se emitan sobre los sistemas de información que tratan datos personales y elevar las conclusiones a la Dirección General de la organización.
- Coordinar dentro de la organización acciones de formación y concientización periódicas en materia de protección de datos.

- Revisar periódicamente que los Avisos de Privacidad se encuentren debidamente actualizados.
- Custodiar debidamente las Relaciones de Medidas de Seguridad, documentación interna en materia de protección de datos; documentación relativa a las funciones y obligaciones del personal que trata datos personales, así como los Informes Jurídicos y de Auditoría elaborados sobre la materia para el Responsable.
- En el caso de las bases de datos del Responsable que contienen datos personales considerados sensibles (origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y/o preferencia sexual), controlar los mecanismos de registro de acceso a los datos protegidos, revisar periódicamente la información de control registrada, así como elaborar un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes, elevando las conclusiones de dicho informe al Responsable Funcional de la base de datos correspondiente y, en su caso, al Responsable Operativo de la misma.
- Guardar el secreto profesional respecto de los datos personales a que tenga acceso con motivo de sus funciones.
- Actuar como interlocutor, en representación de la empresa, en todas aquellas actuaciones que se lleven a cabo frente al INAI.
- Cualquier otra actividad prevista en la presente Política de Protección de Datos Personales que le identifique como responsable de su gestión y control.

6. INCUMPLIMIENTO DE LA POLÍTICA

El incumplimiento manifiesto de la presente Normativa de Seguridad podrá acarrear el inicio de las medidas disciplinarias oportunas y, en su caso, las responsabilidades legales correspondientes; en particular aquéllas de naturaleza laboral derivadas del incumplimiento de las instrucciones dadas por el empleador a sus empleados.

Finalmente, se pone en conocimiento de los destinatarios de esta Norma el contenido del Capítulo XI de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares:

CAPÍTULO XI

De los Delitos en Materia del Tratamiento Indebido de Datos Personales

Artículo 67.- Se impondrán de tres meses a tres años de prisión al que estando autorizado para tratar datos personales, con ánimo de lucro, provoque una vulneración de seguridad a las bases de datos bajo su custodia.

Artículo 68.- Se sancionará con prisión de seis meses a cinco años al que, con el fin de alcanzar un lucro indebido, trate datos personales mediante el engaño, aprovechándose del error en que se encuentre el titular o la persona autorizada para transmitirlos.

Artículo 69.- Tratándose de datos personales sensibles, las penas a que se refiere este Capítulo se duplicarán.