DATOS PERSONALES PARA GODÍNEZ

MOVIMIENTO CIUDADANO

DATOS PERSONALES PARA GODÍNEZ

NOTA DEL AUTOR

Como se sabe, en una forma general, el término Godínez alude a los oficinistas que trabajan de 9 a 6 todos los días y los japoneses tienen algo parecido en el Salaryman. Es a esta idea a la que aludimos con el título Datos Personales para Godínez, no a un posible uso despectivo que pudiera darse. En el Chavo del ocho, Godínez era un estudiante desinteresado y distraído y en sí, el término se ha utilizado para referirse a un trabajador asalariado sin importancia, que lleva a cabo labores repetitivas y aburridas.

Lo que intento en este manual es referirme a los aspectos técnicos de la protección de datos personales que deben lleva a cabo quienes laboran como oficinistas dentro de una institución que resulta obligada. En ningún momento trato de hacer escarnio o burla de quienes tienen que lidiar con un horario de 9 a 6.

ATENTAMENTE,
ROBERTO MANCILLA
(Quien lleva lonchera a su trabajo)

INTRODUCCIÓN

Compañero(a), si estás leyendo esto es porque te encargaron hacerte cargo de una cuestión administrativa de suma importancia, la cual pocos entienden. Es una labor muy valiosa y noble la que tienes que realizar; nadie te lo va a agradecer y no existe mucha información respecto de lo que debes llevar a cabo.

Invariablemente de que esta responsabilidad haya recaído sobre ti porque, cuando fuiste por un trago de agua al bebedero, tu jefe estuviera decidiendo quién se haría cargo y providencialmente te vio, o tal vez porque tienes un perfil compatible con la posición o te hayas propuesto como voluntario(a), no estás solo(a).

Este cuadernillo está diseñado para proporcionar una explicación amena, rápida y fácil de asimilar de los aspectos prácticos que debes conocer para tu nueva posición. Para tal efecto, este estudio tiene tres partes: una es la descripción general del resguardo de los datos personales como práctica administrativa; la segunda es lo que debe saber una persona adscrita a una de las unidades administrativas responsables e involucradas; y la tercera, los conocimientos prácticos para alguien que trabaje en la Unidad de Transparencia. Posteriormente se presentan conclusiones.

Es importante notar que la diferencia de este cuadernillo con el de Datos personales para millennials es que ésta es una introducción técnica del tema y, por lo tanto, le delegamos la introducción elemental al otro documento.

Por último, debemos aclarar que en el presente cuadernillo vamos a hacer uso de la Ley General de Datos Personales en Posesión de los Sujetos Obligados, pues comprende a todos los sujetos gubernamentales y sujetos de derecho privado de relevancia pública, como lo son los sindicatos, partidos políticos, fideicomisos y todo aquel que ejerza actos de autoridad o reciba fondos públicos.

RESUMEN DE LA PRÁCTICA ADMINISTRATIVA DEL RESGUARDO DE DATOS PERSONALES

Los derechos fundamentales son como Santa Claus: recibimos los regalos, pero no entramos en razón de la friega que se puso un ejército de elfos. La protección de datos es un derecho constitucional consagrado en el artículo 16 constitucional, tanto particulares como gobierno deben obedecerlo, pero nadie toma en cuenta a la gente que se encarga de que algo tan lindo se vuelva realidad. Es decir, todo derecho se implementa por medio de recursos humanos y materiales dirigidos a una serie de acciones concretas.

En el caso presente, detrás del resguardo de datos personales, hay un grupo de Godínez dándole duro. Compañero(a), Ustedes son los elegidos, como lo fueron Neo, Harry Potter o Buffy, la Cazavampiros.

Con las reformas constitucionales de 2013 y de 2016 vinieron nuevas leyes: la Ley General de Transparencia y Acceso a la Información Pública y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados. Éstas trajeron consigo nuevas obligaciones y nuevos sujetos. Esto significa, en primer lugar, que a sujetos como partidos, sindicatos, fideicomisos y otros, se les aplica la misma ley que al gobierno, en vez de aquella que era para particulares; también implica mayores obligaciones en la materia. Traducción: si antes no tenías la obligación, ahora la tienes, y recio.

La responsabilidad de datos personales se traduce en dos tipos de acciones: la atención de solicitudes de derechos ARCO (acceso, rectificación, cancelación y oposición) y la recopilación, tratamiento y resguardo de los datos personales. Lo primero no es difícil de entender, existen personas que se dirigen a ti para que les permitas acceder a los datos personales que tienes de ellos y, con ello, puedan corregir, oponerse al uso que se les da o hacer que los quiten de tus bases de datos.

Pos me mato.

Lo segundo implica que cuando recopiles los datos de una persona le digas cómo se va a usar la información, en general, por medio de un aviso de privacidad; cuando tomas esa información, y la usas tienes que cuidar que exista un registro especifico de quiénes tocaron esa información, además debes tomar medidas específicas para cuidar que personas sin autorización no puedan ver esa información. La legislación pide ahora evaluaciones de impacto donde se identifiquen las áreas y el personal que tienen contacto con datos personales—el tipo de interacción que tienen con ellos—y se realice un inventario de datos personales y de los sistemas de tratamiento existentes.

La Ley entiende las medidas de seguridad como “acciones, actividades, controles o mecanismos…que permitan proteger los datos personales” (Artículo 3º LGPDPPSO), y distingue entre tres tipos: administrativas, físicas y técnicas. Las primeras las entendemos como “Políticas y procedimientos para la gestión, soporte y revisión de la seguridad de

la información a nivel organizacional, la identificación, clasificación y borrado seguro de la información, así como la sensibilización y capacitación del personal, en materia de protección de datos personales" (Artículo LGPDPPSO). Estas medidas se encuentran contenidas en los artículos 32 a 42 de la Ley y consisten en lo siguiente:

· Políticas internas para la gestión y tratamiento de los datos personales: se habla de la forma en cómo la organización para la que trabajas va a gestionar y tratar los datos que se le proporcionen; es un documento que, aunque es especializado, debe entenderse lo más posible. Debe tomar en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales; es decir, se obtienen para cumplir un propósito, se usan y, una vez cumplida la meta, se suprimen (Artículo 31, f. I, LGPDPPSO).

· Funciones y obligaciones del personal involucrado: debe tenerse un documento donde se establezca cuáles unidades administrativas poseen responsabilidades respecto de datos personales, la persona que dirige la unidad y el encargado de cumplir con las obligaciones (Artículo 31, f. II, LGPDPPSO).

· Inventario de datos personales: se refiere a qué datos personales se tienen, cuál tipo son (sensibles o no), cuántos sistemas de datos se tienen y en qué soportes se tiene la información, si es un documento físico o se encuentra en formato electrónico (Artículo 31, f. III, LGPDPPSO).

· Análisis de riesgo de los datos personales: es un estudio en el que se plantean las posibles amenazas al resguardo de datos y las debilidades existentes. Se deben listar también los recursos humanos y materiales involucrados en el tratamiento de datos personales (Artículo 31, f. IV, LGPDPPSO).

· Análisis de brecha: es el análisis donde se comparan las medidas de seguridad existentes contra las que establece la Ley. Se le conoce como "brecha" a las medidas faltantes en la organización (Artículo 31, f. V, LGPDPPSO).

· Plan de trabajo: una vez vistas las medidas faltantes, debe realizarse un plan para implementarlas, además de crear una parte sobre el cumplimiento cotidiano de las políticas de gestión y tratamiento de los datos personales (Artículo 31, f. VI, LGPDPPSO).

· Capacitación del personal: se debe de tener un plan para capacitar al personal; lo que se les enseña depende de las actividades y las responsabilidades en el tratamiento de datos personales (Artículo 31, f. VII, LGPDPPSO).

· Monitoreo y revisión periódica de las medidas de seguridad implementadas: se refiere a la inspección periódica de las medidas de seguridad existentes, así como de posibles amenazas y vulneraciones (Artículo 31, f. VII, LGPDPPSO).

· Documento de seguridad: es el documento que se crea con las evaluaciones de impacto de datos personales, debe contener todas las medidas expuestas hasta este punto, excepto la política de gestión.

· Bitácora de vulneraciones a la seguridad: se debe llevar un registro de toda vulneración de seguridad, entendidas como la pérdida o destrucción no autorizada, el robo, extravío, copia no autorizada, el daño, la alteración o modificación no autorizada y el uso, acceso o tratamiento no autorizado. Cada entrada deberá contener una descripción de la vulneración, la fecha en que ésta tuvo lugar, sus causas y las acciones tomadas (Artículo 39 LGPDPPSO).

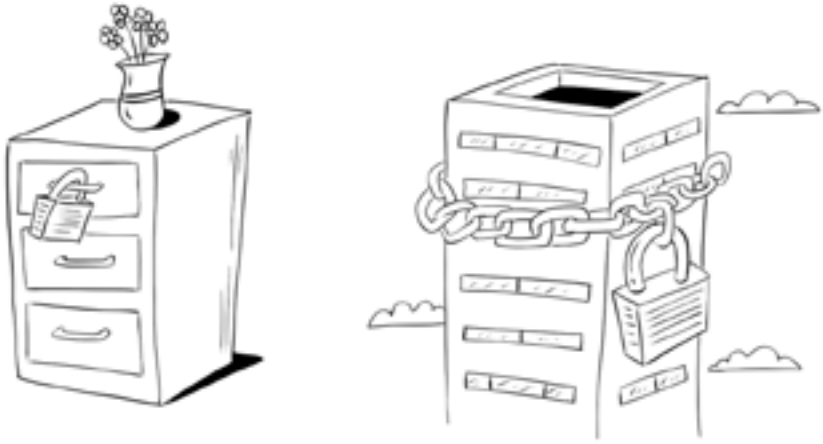
· Informe de vulneración al titular de los datos: en cada vulneración, además de registrarla, debe darse notificación a quien sea titular de los datos personales afectados. Se debe especificar la naturaleza del incidente, los datos personales comprometidos, las recomendaciones al titular, acciones correctivas y los medios con los que se pueda obtener mayor información (Artículos 40 y 41 LGPDPPSO).

· Aviso de privacidad: es un documento que debe dársele a todo titular de datos a partir del momento en el cual se recaben sus datos personales, con el objeto de informarle los propósitos del tratamiento de los mismos (Artículo 3, f. II, LGPDPPSO).

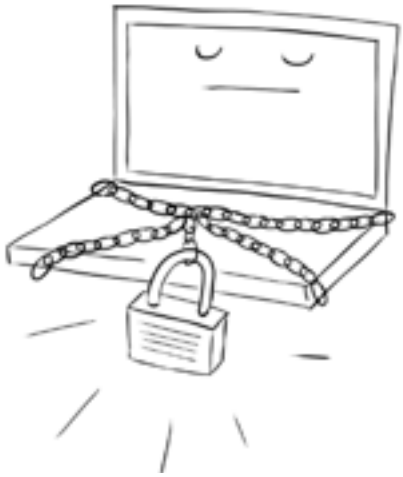
· Control de confidencialidad: son mecanismos para asegurar que todas las personas e instancias involucradas en el tratamiento de los datos personales guarden confidencialidad respecto de éstos. El contrato es la forma más común de cumplir con este mecanismo y la obligación que emana del mismo subsistirá aún después de finalizar sus relaciones con la organización obligada (Artículo 42 LGPDPPSO).

· Las medidas de seguridad físicas se toman para proteger

el entorno de los datos personales y los recursos utilizados para el tratamiento de los mismos; es decir, qué instrumentos usas para guardar los datos de una forma inasequible para personas sin autorización. Puesto en términos reales, serían el edificio y el cuarto donde se da resguardo físico a los datos personales, son la caja fuerte o los archiveros con candado donde se tienen los formatos físicos de los datos personales. También son la bitácora que registra cada persona que entra a este cuarto y de los momentos en que accede y sale, son el cerrojo de la puerta y la llave del personal autorizado.



Por último, las medidas de seguridad técnicas se refieren a las acciones y mecanismos implementados por medio de hardware y software para proteger los datos personales que están en soporte digital. Es decir, son los programas y el equipo de cómputo (y sus mejoras) que permiten el resguardo seguro de datos personales en sistemas electrónicos; esto también implica transferencias seguras, prevención de hackeo, resguardo seguro en la nube, entre otras cuestiones.



EL RESGUARDO DE DATOS PERSONALES EN LAS UNIDADES ADMINISTRATIVAS RESPONSABLES

Si estás leyendo esto, formas parte de las unidades administrativas responsables de resguardar datos personales, y a ti te toca ser el encargado de esa chamba. En tal caso, lo primero que debes de tener en cuenta es pedir el documento de seguridad, a grandes rasgos te permitirá saber qué parte del inventario de datos está bajo tu cuidado.

Resulta bueno ver tanto el análisis de riesgo—y así entender el contexto en el que se realiza tu actividad—como el de brecha para que entiendas lo que falta. Una vez entendido esto, verás en tu actividad que la mayoría de tus actividades se circunscribe a medidas físicas y técnicas de seguridad y, por excepción, te toca realizar un par de medidas administrativas.

Tus labores dependerán del soporte en que estén los datos personales a tu resguardo. Si tienes una serie de archiveros, te debes asegurar de que estén en un cuarto inaccesible sin tu aprobación. Los archiveros o contenedores donde se resguarda la información deben tener un candado al que tú tengas acceso y, en tal caso, deberás identificar bien las llaves disponibles porque vas a andar más cargado que un cerrajero.

También debes traer contigo (y esto es muy importante) una bitácora de quiénes son lo que entran al resguardo de datos: registro de quién entra (y que firme su entrada), a qué hora entra y sale, y qué archiveros o contenedores usó. Las transferencias que hagas de datos en físico deben de ir selladas y con mensajero de confianza (debe firmar un acuse), además de que te deben firmar de recibido, verificando que no los sellos no se hayan roto.

Por otra parte, si los datos personales bajo tu responsabilidad se encuentran en un sistema computarizado, debes asegurarte que los mismos sólo puedan accederse con usuario y contraseña; hay que llevar un registro de los usuarios y los mismos deben firmar un contrato de confidencialidad. Es necesario ver con el técnico (si es que tú no lo eres) si los niveles de seguridad para el resguardo y las transferencias electrónicas son adecuados para las buenas prácticas en el tipo de actividad que lleva a cabo tu organización. Por último, si tienes algunos datos (o todos) en un USB, CD, disco duro externo u otros, debes darles el mismo nivel de resguardo como en los soportes físicos.

Respecto a las medidas administrativas, sólo hay dos para tu trabajo: Por un lado, el control de confidencialidad, generalmente hecho como contrato, lo debes firmar y leer con cuidado; tu jefe debe de firmar uno también, así como los usuarios de los sistemas de datos personales.

Este contrato debe señalarte la obligación de guardar silencio sobre los datos que manejas—aun después de la relación de trabajo—además de indicar las sanciones que señala la Ley en caso de que la violentes. Ojo: no te puede obligar a sanciones adicionales, ni a cualquier otra cosa.

Por otro lado, tienes la bitácora de vulneraciones. Como se dijo, éste es el registro de todas las dobleces en la seguridad del sistema que está a tu cuidado; su manejo varía de una organización a otra. Algunos manejan una bitácora por unidad administrativa y una bitácora general que lleva el oficial de datos personales de la Unidad de Transparencia. Otros hacen que las unidades avisen a la UT y ésta registra todo. El informe debe hacerlo la Comisión de Transparencia y puede firmarse adicionalmente por la Unidad de Transparencia y por quien dirija la unidad administrativa donde se dio la vulneración.

EL RESGUARDO DE DATOS PERSONALES EN LA UNIDAD DE TRANSPARENCIA

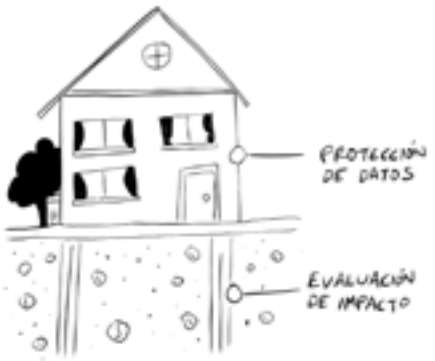
Si estás leyendo esta parte es porque trabajas en la Unidad de Transparencia de tu organización. Este es el departamento o división encargada de cumplir con las obligaciones de transparencia y de hacer una vigilancia sobre el resguardo de datos personales que se realizan; la Ley les permite tener un oficial de datos personales, encargado de eso, pero si estás leyendo esto, quiero pensar que eres un operador de piso entrenándose en esta responsabilidad.

Respecto al resguardo cotidiano de datos personales, la Unidad de Transparencia tiene tres responsabilidades: 1) responde las solicitudes de derechos ARCO, 2) se encarga de vigilar que las unidades administrativas instituyan las medidas de seguridad físicas y técnicas correspondientes 3) y se encarga de implementar las medidas administrativas de seguridad.

La primera consiste en recibir, por medio del Sistema Nacional de Transparencia, las peticiones de ejercicio de derechos ARCO, donde se pide el acceso, rectificación, cancelación y oposición; en ellos se puede responder si procede o no el ejercicio de ese derecho, pero se deben dar las razones de por qué y se tiene que citar la legislación que lo permite. A esto se le conoce como motivación y fundamentación, y es la base del principio de legalidad, contenido en los artículos 14 y 16 constitucionales.

Tanto la vigilancia como la implementación de medidas de seguridad implican la existencia de una o varias Evaluaciones de Impacto de Datos Personales. Ésta debe entenderse como un análisis de cómo se determinan los sistemas de protección de datos que constituyen el inventario, se realiza un estudio de los riesgos y de la brecha entre lo que exige la Ley y lo realizado; ésta debe arrojar también la información necesaria para generar el plan de trabajo y el esquema de capacitación.

Las evaluaciones deben arrojar la información necesaria para realizar un documento de seguridad; se necesita un equipo evaluador, podría ser el mismo que redacte el documento. Además de lo establecido por ley, un buen documento de seguridad debe contener información sobre el perfil de la gente que lo llevó a cabo, además de una debida fundamentación y motivación (por qué se está haciendo y en base a qué parte de la Ley). Saber quiénes realizan el estudio te ayuda a entender la forma como se redactó y la perspectiva que está expresando. Tener la justificación de por qué se hizo una revisión, te permite hacer un cotejo más completo entre revisiones nuevas y viejas. Todo esto sirve para hacer un mejor trabajo.



Ahora bien, se puede dar el caso de que nunca se haya realizado una inspección de datos personales en la organización. En tal caso, es necesario tener cuidado de que la evaluación inicial atienda este aspecto, las evaluaciones posteriores serán diferentes a medida que se progrese en la implementación de las medidas de seguridad exigidas por la legislación en la materia.

CONCLUSIONES

Detrás de todo derecho, vivimos y observamos un ejercicio de recursos humanos y materiales, y detrás de los mismos están tú y otros dándole duro a esta labor. Fuera de bromas, con todo esto de los Godínez, este tipo de esfuerzos administrativos pueden tener un sabor tedioso y molesto, pero lo cierto es que estás protegiendo los derechos de alguien más. Ésta es una labor noble y cumplirla a cabalidad incluso debe considerarse un deber cívico.

Intentamos dar una introducción técnica y fácil de entender para poder navegar todos los detalles importantes en el resguardo de datos personales que deben tomarse en cuenta, realizadas por distintas unidades administrativas, incluida la de transparencia. Hay muchísimo por abarcar, espero que lo anterior ayude a proveerte de lo necesario para realizar tu labor a cabalidad.

Roberto Mancilla es Presidente de la Comisión Nacional de Transparencia de Movimiento Ciudadano. Es Licenciado en Derecho por Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey y Doctor en Derecho por la Universidad de California, Berkeley. Le gusta escribir cuentos cortos y hacer artículos académicos.

Oliver Gonzalez es diseñador gráfico e ilustrador. Egresado de la carrera de Ciencias de la Comunicación del Instituto Tecnológico y de Estudios Superiores de Monterrey, Campus Monterrey. En sus tiempos libres disfruta de hacer garabatos y crear personajes; es saxofonista de la banda Corazón Attack.