G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
2014, Año de las letras argentinas

Resolución

Número: RESOL-2014-239-ASINF

Buenos Aires, Martes 30 de Diciembre de 2014

Referencia: Expediente Electrónico N° 04591478-MGEYA-ASINF-2.013 - "Marco Normativo de Tecnología de Información"

VISTO: La Leyes Nros 2.689, 3304, 4.013, los Decretos Nº 660/GCABA/11, el Expediente Electrónico N° 04591478-MGEYA-ASINF-2.013, y

CONSIDERANDO:

Que mediante Ley N° 2.689, se creó la Agencia de Sistemas de Información del Gobierno de la Ciudad Autónoma de Buenos Aires (ASI), como órgano rector en materia de tecnologías de la información y las comunicaciones en el ámbito del Poder Ejecutivo, y como entidad autárquica en el orden administrativo, funcional y financiero;

Que la Ley de Ministerios N° 4.013 establece que la Agencia de Sistemas de Información (ASI) se encuentra bajo la órbita del Ministerio de Modernización del Gobierno de la Ciudad Autónoma de Buenos Aires, Unidad Ministerial que, se encarga de supervisar su funcionamiento, en un todo conforme con dicha Ley, su Decreto Reglamentario N°660/11 y sus modificatorios;

Que dada su naturaleza jurídica, la ASI es una entidad autárquica en el orden administrativo, funcional y financiero, en el ámbito del Ministerio de Modernización del GCABA;

Que los entes descentralizados tienen por definición la facultad de administrarse por sí mismos, poseen patrimonio y presupuesto propios y se rigen por las normas generales de Derecho Público, vinculándose con la Administración Central, mediante una relación jurídica de control administrativo o tutela;

Que asimismo, la ASI es el órgano rector en materia de tecnologías de la información y telecomunicaciones

y tiene como objetivo organizar y coordinar con todas las dependencias del Poder Ejecutivo, la infraestructura informática, de telecomunicaciones y de los sistemas de información, dotando a la Ciudad de un plan autosuficiente, razonable y coordinado de gobierno electrónico;

Que en este sentido en el artículo 3° de la Ley 2.689, se enuncia los Principios rectores bajo los cuales la Agencia deberá organizarse y funcionar, estableciendo entre otros, el de "*Promover la estandarización de los bienes informáticos, equipos, recursos, sistemas y programas a ser utilizados por el Poder Ejecutivo*", así como "*…el desarrollo, modernización y economía administrativa integral, en las dependencias y entidades de la administración pública, a fin de que los recursos y los procedimientos técnicos sean aprovechados y aplicados con criterios de transparencia, eficacia, eficiencia y austeridad"*;

Que en concordancia, se definen entre las funciones del ente, la de *" (…) a) Definir y establecer la política gubernamental en materia de Sistemas de Información y el uso de medios electrónicos para la gestión, dictando normas técnicas, metodologías de gestión de proyectos y desarrollo de software y estándares en materia de Tecnologías de Información y Telecomunicaciones a ser aplicadas en consonancia con estándares internacionales, que garanticen la interoperabilidad y accesibilidad de los servicios electrónicos del Poder Ejecutivo (…)"*(Articulo N° 4 de la Ley 2689);

Que mediante Resolución Nº 177/ASINF/13 (Orden Nº 27) se aprobó el "Marco Normativo de Tecnología de Información" obrante en el Anexo I, registrado en SADE bajo el número de informe, IF-2013-06227164-ASINF;

Que continuando con esta línea, ésta Agencia ha elaborado una serie de nuevas Políticas que complementan el "Marco Normativo de Tecnología de Información" que deberán ser aplicadas sobre todas las actividades relacionadas directa o indirectamente con la utilización de recursos de Tecnología de Información y comunicación dentro del ámbito del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires.

Que por otro lado, cada dependencia del Poder Ejecutivo de la Ciudad Autónoma de Buenos Aires, será responsable de dar cumplimiento y hacer cumplir con lo establecido en las presentes Políticas;

Que es dable destacar, que en las sucesivas versiones que pudieran generarse sobre las presentes Políticas serán actualizadas en el sitio de la ASI: http://www.buenosaires.gob.ar/asi;

Que la Sindicatura General del Gobierno de la Ciudad Autónoma de Buenos Aires y las Unidades de Auditoría Interna de cada jurisdicción, actuando como órganos del sistema de Control Interno del GCABA, serán responsables por la fiscalización del cumplimiento de las políticas establecidas por la ASI en virtud de las competencias que le son propias, según la normativa vigente;

Que la Dirección General de Infraestructura, la Dirección General de Integración de Sistemas, la Dirección General de Gobierno Electrónico, la Gerencia Operativa de Seguridad Informática, la Gerencia Operativa de Legales han tomando intervención en la elaboración de las presentes Políticas;

Que la Procuración General de la Ciudad Autónoma de Buenos Aires (Orden Nº 75) y la Sindicatura General del Gobierno de la Ciudad Autónoma de Buenos Aires (Ordenes Nros. 57 y 60) han tomando la debida intervención en el marco de las atribuciones que le son propias;

Que por lo expuesto, resulta necesario dictar el acto administrativo correspondiente a fin de complementar el "Marco Normativo de Tecnología de Información", que deberán observar todas las dependencias del Poder Ejecutivo del Gobierno de la Ciudad Autónoma de Buenos Aires.

Por ello, y en uso de facultades que le son propias,

EL DIRECTOR EJECUTIVO

DE LA AGENCIA DE SISTEMAS DE INFORMACIÓN

RESUELVE

Artículo 1º.- Compleméntase el "Marco Normativo de Tecnología de Información" aprobado por Resolución Nº 177/ASINF/13.

Articulo 2º.- Apruébase el Anexo I registrado en SADE bajo el número de informe (IF-2014-18613717-ASINF), el que a todos sus efectos forma parte integrante de la presente Resolución.

Articulo 3º.- Regístrese, publíquese en el Boletín Oficial de la Ciudad Autónoma de Buenos Aires, y para su conocimiento y demás efectos comuníquese a todos los Ministerios, Secretarías, Subsecretarias, las Direcciones Generales Técnicas, Administrativas y Legales u organismos equivalentes de cada dependencia y a la Sindicatura General de la Ciudad Autónoma de Buenos Aires. Cumplido, archívese.

RAUL MARTINEZ
DIRECTOR EJECUTIVO DE LA ASINF
AGENCIA DE SISTEMAS DE INFORMACIÓN (MMGC)

Marco Normativo de IT

PO0001 - Política Catálogo General

Gobierno de la Ciudad Autónoma de Buenos Aires

Política Catálogo General

1. Introducción

El presente documento tiene por objetivo actualizar el catalogo de documentos que conforman el Marco Normativo de TI, enumerando cada uno de ellos y exponiendo de manera concisa el contenido y codificación de los mismos.

2. Objetivo

Establecer la estructura, contenido y codificación de los documentos (política, procesos, procedimientos y estándares) que conforman el Marco Normativo de TI vigente en el GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

La *Política catálogo general* describe de forma sucinta cada una de las políticas que conforman el Marco Normativo de TI del GCABA y a partir del cual se irán actualizando e incorporando nuevos documentos a dicho marco.

El proceso de codificación y elaboración de nuevos documentos que pertenezcan al Marco Normativo de TI queda excluido de la presente política y deberá ajustarse a lo establecido en la *Política reguladora del marco normativo.*

Marco Normativo de TI

A continuación se resumen los documentos que conforman el Marco Normativo de TI, ordenados por dominio, exponiendo una breve descripción de su contenido y codificación:

0. Índice referencial

PO0001-Política catálogo general (Res. ASINF 177/13 - pág. 1)
Descripción y codificación de cada uno de los documentos que forman parte del Marco Normativo de TI.

1. Política de seguridad de la información

Administrar la seguridad de la información dentro de la organización, estableciendo una estrategia y un marco gerencial para controlar su implementación.

PO0101-Política externa reguladora (Res. ASINF 177/13 - pág. 9)
Exposición de criterios y lineamientos básicos a cumplir para la elaboración, codificación y contenido de los documentos que conformarán el Marco Normativo de TI.

PO0102-Política general de seguridad informática (Res. ASINF 177/13 - pág. 14)
Documento de máxima relevancia que establece un marco general para instituir y mantener las políticas, procesos, procedimientos y estándares que definen las medidas de seguridad de la información a aplicar, de acuerdo con la normativa vigente.

PO0103 – Política nomencladora (pág. 9, del presente Anexo)
Establecer la codificación y los criterios que se utilizarán las diferentes organismos y reparticiones para elaborar las Políticas, Procesos, Procedimientos, Estándares, Guías y Modelos que conforman el Marco Normativo de TI vigente en el GCABA.

GU0101-Guía del usuario de SSII de GCABA (pág. 14, del presente Anexo)
Establecer aspectos mínimos que deben conocer y aplicar los funcionarios de gobierno en el trabajo diario, con el fin de reducir la probabilidad de fallos y daños causados por problemas de seguridad.

2. Evaluación y tratamiento de riesgos

Identificar, cuantificar, y priorizar los riesgos de seguridad a los que se encuentra sometido el GCABA, definiendo cuáles deben ser las vías para determinar si serán aceptados, transferidos o mitigados.

PO0201-Política análisis de riesgos tecnológicos (Res. ASINF 177/13 - pág. 20)
Definir y establecer los requisitos para la realización de evaluaciones de riesgos tecnológicos y la administración de los mismos dentro del ámbito del GCABA.

3. Organización de la seguridad

Administrar la seguridad de la información dentro de la organización, estableciendo una estrategia y un marco gerencial para controlar su implementación.

PO0301-Política de contratación de proveedores de TI (Res. ASINF 177/13 - pág. 24)
Establecer las pautas que deben ser consideradas para toda adquisición de equipamiento, software, servicios, comunicaciones, telecomunicaciones y sistemas de información, debiendo garantizar su estandarización, interoperabilidad y seguridad.

4. Gestión de activos de Información

Alcanzar y mantener una adecuada protección de los activos, estableciendo roles y responsabilidades para la clasificación y tratamiento de los mismos. Cada Organismo clasificará la información de acuerdo a los criterios que establece el GCABA en sus políticas, contando para ello con la asistencia del Área de Seguridad Informática.

PO0401-Política de responsabilidades sobre la información (Res. ASINF 177/13 - pág. 28)
Establecer los roles y responsabilidades de actuación, los actores que custodian, administran y salvaguardan de la información, así como los que autorizan el acceso; a través de una correcta asignación y una adecuada segregación de funciones.

PO0402-Política de clasificación de la información (Res. ASINF 177/13 - pág. 34)
Establecer los criterios que se deben considerar para clasificar la información a fin de poder definir el nivel de criticidad de la misma y adoptar las medidas de protección y tratamiento adecuadas.

5. Seguridad de los recursos humanos

Asegurar que el personal de planta, personal con contrato de locación de servicio y proveedores, entiendan sus responsabilidades, sean adecuados a sus roles asignados y estén preparados para respaldar la Política General de Seguridad Informática.

A la fecha, el presente dominio no posee documentos asociados.

6. Seguridad física y del entorno

Impedir accesos físicos no autorizados, daños e interferencia a las instalaciones e información del GCABA.

PO0601-Política de seguridad física (Res. ASINF 177/13 - pág. 40)
Definir las pautas generales de seguridad física que permitan asegurar la integridad de los recursos informáticos utilizados para el procesamiento, transmisión y resguardo de la información.

7. Gestión de las comunicaciones y operaciones

Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información, implementando y manteniendo un nivel de seguridad adecuado en la provisión de servicios y detectando las actividades de procesamiento de información no autorizadas.

PO0701-Política de copias de resguardo y recuperación (Res. ASINF 177/13 - pág. 47)
Establecer los lineamientos para la generación, prueba y administración de copias de resguardo periódicas de la información, como así también los criterios básicos para su recuperación.

PO0702-Política de seguridad de las comunicaciones (Res. ASINF 177/13 - pág. 54)
Asegurar una adecuada protección en los procesos de intercambio de información y de las comunicaciones del GCABA.

PO0703-Política de seguridad en redes (Res. ASINF 177/13 - pág. 64)
Asegurar una adecuada protección de la información procesada en la red de datos del GCABA.

PO0704-Política de prevención de software malicioso (Res. ASINF 177/13 - pág. 74)
Establecer los requerimientos que deben cumplir todos los equipos de procesamiento centralizado y estaciones de trabajo conectados a la red de comunicaciones del GCABA, de forma de garantizar la detección y eliminación de software malicioso (virus informáticos, troyanos, gusanos, malware en general; incluyendo código móvil), minimizando el riesgo de infección y propagación de los mismos.

PO0705-Política de instalación de estaciones de trabajo (Res. ASINF 177/13 - pág. 79)
Establecer los lineamientos necesarios para regular el uso de las estaciones de trabajo, la instalación de software, hardware y responsabilidades de los agentes, cualquiera sea su función asignada.

PO0706-Política de uso de correo electrónico (Res. ASINF 177/13 - pág. 84)
Establecer las pautas de comportamiento referidas a la utilización del servicio de Cuenta de Correo Electrónico Gubernamental (CCEG) por parte de los usuarios, de forma de garantizar una adecuada protección de la información y los recursos informáticos y prevenir el tráfico de spam en la red de comunicaciones del GCABA.

PO0707-Política de uso de Internet (Res. ASINF 177/13 - pág. 88)
Establecer las pautas de comportamiento referidas a la utilización de Internet para un uso debido por parte de los usuarios conectados a la red de comunicaciones del GCABA, de forma de garantizar una adecuada protección de la información.

ES0701-Estándar de arquitectura del Data Center ASI
(http://www.buenosaires.gob.ar/asi/estandares)
Formalizar y especificar el modelo de arquitectura aplicable a los Data Centers operados por la ASI, asegurando mediante una adecuada gestión tecnológica, su escalabilidad, agilidad y alta disponibilidad.

8. Control de accesos

Controlar los accesos a la información sobre la base de los requerimientos de seguridad y de los objetivos definidos por el GCABA. Los accesos serán otorgados sobre los principios de "mínimo privilegio" y "necesidad de conocer", aplicables a cada usuario.

PO0801-Política de uso de equipos portátiles (Res. ASINF 177/13 - pág. 93)
Establecer los lineamientos de seguridad a implementar para el tratamiento de los equipos portátiles que procesan, almacenan información o requieran conexión a la red de comunicaciones del GCABA.

PO0802-Política de seguridad en dispositivos móviles (Res. ASINF 177/13 - pág. 99)
Asegurar una adecuada protección de la información en los dispositivos móviles que se conectan a la red de comunicaciones, procesen o almacenen información del GCABA.

PO0803-Política de registro de eventos en servicios de TI (Res. ASINF 177/13 - pág. 103)
Definir las pautas generales para asegurar una adecuada registración de eventos relacionados con los servicios de TI del GCABA, maximizando la trazabilidad de los mismos.

PO0804-Política de control de eventos en servicios de TI (Res. ASINF 177/13 - pág. 108)
Definir las pautas generales para asegurar una adecuada identificación y seguimiento de los eventos en los servicios de TI registrados en los sistemas del GCABA. Asegurar que se registren y se evalúen todos los eventos significativos para la seguridad de accesos

PO0805-Política de administración de usuarios GCABA (Res. ASINF 177/13 - pág. 113)
Establecer los lineamientos que permitan asegurar una adecuada administración de los usuarios del GCABA.

PO0806-Política de administración de usuarios en custodia (Res. ASINF 177/13 - pág. 120)
Establecer las medidas de control para la utilización de usuarios en custodia, de manera que los mismos sean utilizados solo en situaciones de emergencia que lo ameriten.

PO0807-Política de administración de contraseñas (Res. ASINF 177/13 - pág. 125)
Asegurar una adecuada administración (generación, modificación, utilización y almacenamiento) de las contraseñas de los usuarios del GCABA.

PO0808-Política de administración de accesos a software de aplicación (Res. ASINF 177/13 - pág. 131)
Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de usuarios al software de aplicación del GCABA.

PO0809-Política de administración de accesos a recursos de infraestructura de TI (Res. ASINF 177/13 - pág. 136)
Establecer los lineamientos que permitan asegurar una adecuada administración de los accesos de usuarios a los recursos de infraestructura de TI del GCABA.

PO0810-Política de accesos remotos (Res. ASINF 177/13 - pág. 141)
Establecer los aspectos de seguridad y reglas a cumplir al acceder a la red de comunicaciones del GCABA de forma, a fin de garantizar una adecuada protección de la información y los recursos informáticos de la misma.

9. Adquisición, desarrollo y mantenimiento de sistemas de información

Garantizar que la seguridad sea una parte integral del ciclo de vida de los sistemas de información, previniendo errores, pérdidas, modificaciones no autorizadas o mal uso de la información en las aplicaciones.

PO0901-Política de separación de ambientes de TI (Res. ASINF 177/13 - pág. 145)
Establecer los lineamientos y las pautas generales para garantizar una adecuada separación de ambientes de procesamiento de la información del GCABA, definiendo las características de los ambientes y asegurando una apropiada segregación de funciones y limitaciones de acceso.

PO0902-Política de control de cambios (Res. ASINF 177/13 - pág. 152)
Establecer los controles que deberán realizarse en el proceso de cambios de software de aplicación, software de base, información e infraestructura tecnológica de los ambientes, de manera de asegurar su integridad y minimizar el riesgo de pérdida de información, accesos no autorizados o falta de disponibilidad del servicio.

PC0901-Proceso de control de cambios para Organismos
(http://www.buenosaires.gob.ar/asi/estandares)
Establecer control y trazabilidad de cada cambio a implementar en las nuevas aplicaciones o versiones evolutivas y correctivas de aplicaciones existentes.

ES0901-Estándar de desarrollo ASI
(http://www.buenosaires.gob.ar/asi/estandares)
Definir los requerimientos que un desarrollo debe cumplir en relación con las tecnologías adoptadas por la ASI, como así también la interacción con los proveedores de software en cuanto a entregables, seguimiento de errores, control de cambios, etc.

10. Gestión de incidentes de seguridad de la información

Asegurar que se aplique un proceso de mejora continua para la gestión de los incidentes de seguridad de la información, garantizando que los eventos sean registrados y comunicados de forma correcta y oportuna.

PO1001-Política de respuesta ante incidentes de TI (Resolución ASINF 177/13 - pág. 158)
Establecer lineamientos que permitan corregir con la máxima celeridad posible, las consecuencias y efectos negativos de los incidentes de los servicios de TI, a fin de minimizar su impacto.

11. Gestión de la continuidad de las actividades

Desarrollar e implementar planes de continuidad que aseguren la reanudación oportuna de las operaciones esenciales. Contrarrestar las interrupciones de las operaciones y proteger los procesos críticos del GCABA.

A la fecha, el presente dominio no posee documentos asociados.

12. Cumplimiento

Impedir infracciones y violaciones a cualquier obligación legal, reglamentaria, reguladora o contractual, así como a cualquier requerimiento de seguridad. Garantizar el cumplimiento de las políticas, procesos, procedimientos y estándares de seguridad del GCABA.

PO1201-Política de licencias y legalidad de software (Res. ASINF 177/13 - pág. 162)
Establecer los lineamientos necesarios para asegurar que todo software que sea utilizado por el personal del GCABA en el desarrollo de sus tareas (tanto adquirido como desarrollado internamente) tenga la licencia de uso legal correspondiente.

GU1201-Guía de Protección de Datos Personales (pág. 26, del presente Anexo)
Orientar a los funcionarios del GCABA en el proceso de adecuación e inscripción de las bases de datos públicas según lo dispuesto por la Ley CABA 1845/2006; sometiendo las mismas a la supervisión y control de la Defensoría del Pueblo de la CABA, actuando como Órgano de Control en el Cumplimiento de la Ley. Instaurar entre los funcionarios públicos la cultura de la protección de datos personales como un elemento de singular importancia en el ejercicio de sus funciones.

13. Glosario

PO1301-Política glosario de términos y definiciones (Res. ASINF 177/13 - pág. 166)
Términos empleados en la redacción dentro del contexto del marco normativo de TI.

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la *información digital* sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

PO0103 - Política Nomencladora

Gobierno de la Ciudad Autónoma de Buenos Aires

1. Introducción

Al momento de elaborar documentos, tener en cuenta los aspectos básicos de las normas ortográficas y gramaticales posibilita una comunicación escrita con sentido y una transmisión clara del mensaje al lector. Cuando se emplea el lenguaje escrito, no hay modo de escapar a ciertas exigencias que no tiene el lenguaje oral.

Los criterios de elaboración de los documentos que conforman el Marco Normativo de TI se basan en el establecimiento de unas reglas claras de codificación y recomendaciones generales de redacción. Asimismo se define la tipología y el ciclo de vida de dichos documentos.

2. Objetivo

La presente política tiene por objeto establecer la codificación y los criterios que se utilizarán para elaborar las Políticas, Procesos, Procedimientos, Estándares, Guías y Modelos que conforman el Marco Normativo de TI vigente en el GCABA.

3. Alcance

Esta política alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

4. Contenido

A continuación se resumen los criterios a adoptar para la redacción del los documentos que conformarán el Marco Normativo de TI vigente en el GCABA:

a. Estructura de los documentos

La estructura de datos de identificación del documento deberá ajustarse a los siguientes parámetros:

Fecha: fecha de elaboración / modificación del documento.

Responsable: Propietario o Responsable de elaborar el documento.

Descripción: resumen de la información o modificación efectuada.

Versión: versionado secuencial según modificaciones efectuadas (0.x p/ borradores y 1.x p/ finales)

Estado: de acuerdo con la fase del ciclo de vida del documento (Elaboración/ Revisión/ Aprobación / Actualización).

Índice: Epígrafes de las principales materias incluidas

Título: Nombre asignado al documento

Introducción: Breve descripción introductoria a la temática del documento.

Objetivo: Objetivo (s) que se pretenden lograr.

Alcance: A quiénes o a qué áreas alcanza su aplicación.

Contenido: Breve descripción del documento.

b. Codificación del los documentos

Se asignará a cada documento un código alfanumérico de seis caracteres:

DDNNCC-Nombre

DD: Tipo de Documento	PO	Política
	PC	Proceso
	PR	Procedimiento
	ES	Estándar
	GU	Guía
	MO	Modelo

NN: Identificación ordinal del dominio al que pertenece (2 dígitos) de acuerdo con lo especificado en la "*PO0001 - Política Catálogo General*".

CC: Identificación ordinal del documento (2 dígitos).

Nombre: Denominación del documento dentro del marco normativo.

Cualquier otra extensión que sea necesaria deberá ser explicitada en el presente apartado.

c. Criterios de redacción

Los criterios que se deben seguir en la redacción de los documentos del marco normativo son los siguientes:

Tiempos verbales

Dentro de lo posible se deberá utilizar el mismo tiempo verbal para todo el documento.

Se recomienda utilizar el infinitivo o el futuro en tercera persona.

Es importante que el sujeto de la acción esté siempre claramente identificado: "abrir el archivo, registrar la incidencia, rellenar los datos del apartado 1,...", "el operador abrirá el archivo, registrará la incidencia y la comunicará a su responsable".

Las instrucciones y controles deben redactarse en imperativo, ya que la voz pasiva puede resultar ambigua "...la tiene que activar el lector".

Estructura del documento

En los procedimientos, se recomienda estructurar los mismos, en una secuencia cronológica de pasos, en el orden en que se deben de suceder.

Verbo 'deber'

No abusar del verbo 'deber': "se configurará la política de contraseñas" por "se deberá configurar la política de contraseñas".

Uso de 'deber' y 'deber de': 'deber' implica obligación y 'deber de' significa probabilidad: "el sistema debe cumplir", "el sistema debe de estar en mal funcionamiento".

Evitar la perífrasis

Usar siempre el menor número de palabras y expresar una sola idea:

"Tomar en consideración" por "Considerar"

"Resultado final" por "Resultado"

"Todos y cada uno" por "Todos"

"Eliminar completamente" por "eliminar"

"Botón de color rojo" por "Botón rojo"

Ser concreto

Evitar la ambigüedad seleccionando palabras precisas y los detalles necesarios: "Configurar el certificado" por "Abrir el archivo cert.cer y guardar el contenido del certificado".

Claridad

El sentido debe resultar unívoco y fácilmente comprensible para el lector.

Brevedad

Cuanto más largo es un documento más difícil es de leer y utilizar. El documento debe ser lo suficientemente largo como para resultar claro. Deben eliminarse las frases innecesarias, las redundancias, repeticiones y los principios de frase que no aporten nada.

Sencillez

Las frases deben ser breves (25 palabras como máximo). Transformar las frases largas en listas o en otras más breves.

Deben dividirse los párrafos largos en otros más breves.

Las palabras deben ser sencillas, precisas y descriptivas, en lugar de retóricas y complicadas. También la estructura de las frases debe ser sencilla.

Debe eliminarse la terminología técnica innecesaria.

Corrección formal

El lector se forma su primera impresión del documento a partir de sus aspectos formales. Si encuentra indicios de descuido, dudará de la calidad de la información.

Deben respetarse las reglas gramaticales (acentuación, puntuación, etc.).

Deben respetarse otras convenciones tales como: unidades físicas de medida, abreviaturas, acrónimos, etc.

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la *información digital* sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.
La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

Marco Normativo de IT

GU0101 - Guía del Usuario de los Sistemas de Información del GCABA

Gobierno de la Ciudad Autónoma de Buenos Aires

Introducción

Uno de los mayores cambios producidos en este período ha sido la aprobación y publicación -mediante la Resolución Nro. 177 ASINF/13- de un Marco Normativo que contiene Políticas y Directrices de Seguridad de la Información, destinadas a proteger nuestro principal activo: la información de los ciudadanos, de nuestros empleados y nuestras actividades de gestión.

Las Políticas se encuentran en el anexo siguiente, a partir de la página 473:
http://www.boletinoficial.buenosaires.gob.ar/areas/leg_tecnica/boletinOficial/documentos/boletines/2013/11/20131108ax.pdf

La seguridad es responsabilidad de todos. Por este motivo, pedimos tu participación en la protección de los sistemas y de la información soportada por ellos.

Esta guía informativa no reemplaza de ninguna manera a las políticas publicadas; recoge los aspectos mínimos que debés conocer y aplicar en tu trabajo, con el fin de reducir la probabilidad de fallos y daños causados por problemas de seguridad.

Contacto Mesa de Ayuda

4323-9393

asi.mat@buenosaires.gob.ar

Principios de Seguridad de la Información

PROTECCIÓN DE ACCESO A LOS SISTEMAS

Cuentas de Usuario y Contraseñas

Los servicios y aplicaciones ofrecidos por los diferentes sistemas de red de **GCABA** requieren que utilices una cuenta de usuario y una clave o contraseña que te identifique de manera única.

¿Quién debe conocer mi cuenta de usuario y contraseña?

Sólo vos. Es importante que **no las compartas ni comuniques a nadie**. No anotes la contraseña en lugares visibles o fácilmente accesibles como la pantalla, teclado, etc.

¿Cómo debe ser mi contraseña?

La contraseña que utilices debe tener una longitud de al menos 8 caracteres. La contraseña debe estar compuesta por mayúsculas, minúsculas y números.

No utilices contraseñas que sean **fáciles de adivinar** como por ejemplo parte de tu nombre, apellidos, fechas de nacimiento, matrícula, o palabras que se puedan encontrar en un diccionario.

¿Cuándo debo cambiar la contraseña?

Cuando la hayas hecho pública o sospeches que la contraseña es conocida por otra persona, deberás cambiarla. Además, se te pedirá que cambies tu contraseña de forma periódica.

Recordá que las cuentas de usuario y las contraseñas, no son transferibles, y no se deberán prestar a otros usuarios. El usuario es propietario del uso de la cuenta y será responsable de todas las acciones que se realicen con ella.

Uso de sistemas de bloqueo de equipos

¿Cómo puedo evitar que accedan a mi equipo personal?

Si tu equipo dispone de sistema de bloqueo (salvapantalla protegido por contraseña, bloqueo de terminal, etc.) deberás activarlos cuando abandones el puesto de trabajo.

Recordá que sos responsable de las acciones que se realicen con tu cuenta de usuario en los sistemas.

USO DE EQUIPOS INFORMÁTICOS

Uso de los equipos informáticos

¿Qué debo considerar cuando me ausento del puesto de trabajo?

No dejes tu equipo encendido y desatendido en **ausencias prolongadas** del puesto de trabajo. Si debes ausentarte del puesto, desconectate de la sesión o la aplicación en la que estés trabajando o protegé el equipo mediante el uso de una contraseña. De esta forma evitarás que alguien lo utilice sin tu autorización.

Instalación de software

¿Puedo instalar programas en mi equipo?

No ejecutes ni instales software en tu equipo. Si lo necesitas, debes solicitárselo a tu responsable para que lo gestione a través de la Mesa de Ayuda. Todo el software debe ser de uso legal y debe estar licenciado y homologado por el **GCABA** para su utilización.

Recordá que no se permite el uso de software sin licencia de uso, ni tampoco realizar copias del software propiedad de GCABA instalados en los equipos.

Componentes de los equipos informáticos

¿Puedo intercambiar componentes informáticos?

No intercambies componentes o elementos como teclados, pantallas, mouse, etc. entre PC's o terminales.

¿Puedo desplazar equipos fuera de las instalaciones?

No podés desplazar los equipos o cualquier elemento de los mismos **fuera de las instalaciones de GCABA,** salvo los equipos portátiles destinados para tal fin.

PROTECCIÓN DE LA INFORMACIÓN

Cuidado con la Información

¿A que tipo de información puedo acceder?

Recordá que debes acceder, exclusivamente, a la información necesaria para el desarrollo de tus funciones.

¿Que medidas debo adoptar para proteger la información?

Evitá dejar información confidencial desatendida en tu puesto de trabajo, como pendrives, listados o información visible en la misma pantalla del equipo personal. Almacena en lugares seguros toda la información confidencial o relativa a datos personales de ciudadanos, empleados u otras personas.

Distribuí la información exclusivamente a quién debe disponer de ella y evitá que las personas que no deban tener acceso a esa información puedan conocerla.

Si tenés sospechas de que tu estación de trabajo podría ser víctima de accesos no autorizados, comunicate con la Mesa de Ayuda.

¿Puedo usar servicios de almacenamiento en la nube?

La ASI ofrece un servicio propio de almacenamiento en la nube denominado **BACloud**. A diferencia de otros servicios externos, la información se encuentra físicamente almacenada y protegida en el Datacenter de la ASI. Este servicio tiene mecanismos de detección de malware / código dañino y otras amenazas. No intentes utilizar otros medios externos de almacenamiento en la nube, porque ponés en peligro la integridad de la información de todo el **GCABA**.

Recordá que sos responsable de toda la información que manejás para cumplir tu trabajo y de las acciones que adoptás para protegerla de forma adecuada.

Copias de Seguridad

¿Está protegida contra pérdida la información de mi trabajo diario?

Todas las aplicaciones y sistemas albergados en el Datacenter de la ASI están protegidos. Estos recursos se salvaguardan de forma continua a fin de evitar pérdidas.

¿Está protegida contra pérdida la información de mi equipo?

Vos sos el responsable de la información que generás y almacenás diariamente en tu equipo. Por ello es importante que realices frecuentemente copias de seguridad de tus archivos (Ej.: archivos Word, Excel etc.) y las mantengas bajo llave, a fin de protegerla la información de forma adecuada.

Protección de Datos Personales

¿Qué se entiende por Datos de Carácter Personal?

Se entiende por datos de carácter personal cualquier información concerniente a **personas físicas identificadas o identificables**. Por ejemplo, son datos de carácter personal los nombres y apellidos, los DNI, pasaportes, información de salud, etc.

¿Puedo almacenar información de carácter personal en mi equipo?

No se pueden almacenar datos de carácter personal en el equipo asignado sin permiso específico de tu Director General o Equivalente.

¿Existe alguna Ley al respecto?

En Argentina existe la Ley Nacional 25326 y la Ley Municipal 1845, que regulan la Protección de los Datos Personales. Estas leyes tienen por objeto garantizar y proteger los datos de carácter personal de todas las personas, incluidos los tuyos, y que penalizaría nuestra actuación en caso de que nos sustrajeran información.

¿Qué uso puedo hacer de los datos de carácter personal?

Sólo podés hacer uso de los datos de carácter personal para los fines de gestión gubernamental para los que han sido recabados.

Recordá que existe una Ley sobre Datos de Carácter Personal. Por este motivo, si trabajás con datos que se pueden asociar a personas, poné especial cuidado en su protección.

PROTECCIÓN CONTRA MALWARE Y OTRAS AMENAZAS

Malware y código malicioso

¿Qué es el malware?

Es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario. Existen distintos **tipos de malware o código dañino** de acuerdo a cómo actúan. Los virus informáticos son un tipo de malware que afecta principalmente a archivos ejecutables.

¿Qué es un antivirus o antimalware?

Es un programa informático específicamente diseñado para detectar la presencia de virus o código dañino y eliminarlo.

¿Cómo me puedo infectar?

La infección por virus se produce por la **ejecución de un programa contaminado**, por ejemplo si ejecutas un programa o abrís un archivo infectado independientemente de dónde esté (disco rígido, pendrive, correo electrónico, etc.), o si navegas por páginas de Internet que tienen código dañino.

¿Qué debo vigilar para no infectarme?

Es conveniente verificar periódicamente que el software de protección esté activo, y que el mismo sea el ofrecido y adquirido por la ASI.

Debes evitar el uso de productos sin licencia o adquiridos de fuentes sin garantía.

No abras o ejecutes archivos o programas de origen desconocido o sospechoso.

Resumiendo; todos los archivos descargados de Internet o recibidos por otros medios (pendrives, correo electrónico, etc.) deben ser convenientemente revisados en busca de presencia de virus o malware.

¿Qué hago si detecto un comportamiento inusual?

Si tenés sospechas fundamentadas sobre la existencia de código malicioso/virus en tu estación de trabajo, debés comunicarte con la Mesa de Ayuda, para el aislamiento de los sistemas afectados y la eliminación del virus.

Es tu responsabilidad adoptar las precauciones apropiadas para prevenir la distribución de estos y otros tipos de virus.

USO DE LAS COMUNICACIONES

Uso del correo electrónico

¿Qué cuidados debo tener con el correo electrónico?

Es recomendable que al recibir un **nuevo mensaje** de correo electrónico -antes de abrirlo- analices las cabeceras, intentando detectar si es un mensaje de dudosa procedencia.

¿Qué hago con el correo desconocido?

Si recibís **correos no solicitados** o de origen desconocido, debes **rechazarlos** por muy interesantes que parezcan, ya que pueden contener virus u otro tipo de amenazas.

Analizá antes de abrir, todos los correos electrónicos recibidos y sospechá de los mensajes no esperados, incluso si están en otro idioma. En caso de duda consulta siempre con la Mesa de Ayuda.

Y en especial, no abras o ejecutes **archivos adjuntos** (ejecutables, documentos, etc.) de **correos electrónicos no solicitados**.

¿Qué es el 'spam'?

'Spam' es la palabra que se utiliza para calificar el **correo masivo no solicitado** enviado por Internet.

¿Cómo puedo evitar el 'spam'?

Como regla general, sólo hay que dar nuestra dirección de correo electrónico a personas conocidas. No publiques tu dirección de correo electrónico en foros o en páginas web.

Cuando recibas correos electrónicos, debes comprobar la veracidad de los mensajes recibidos y eliminar aquellos provenientes de fuentes sospechosas. De esta forma podés ayudar a los demás en la detención de su distribución.

Nunca debes contestar a los mensajes de 'spam' ya que al hacerlo se reconfirma la dirección.

¿Puedo enviar información confidencial por correo electrónico?

No debes enviar información sensible o confidencial en los correos electrónicos.

¿Puedo usar otras cuentas de correo electrónico?

El correo corporativo suministrado por la ASI tiene mecanismos de detección de malware / código dañino y otras amenazas. No intentes utilizar otros servicios externos de correo para enviar información gubernamental, porque ponés en peligro la integridad de la información de todo el **GCABA**.

Recordá que el correo electrónico debe ser para uso laboral.

Phishing

¿Qué es el pishing?

El "phishing" es una modalidad de estafa con el objetivo de intentar obtener de un usuario sus datos, claves, cuentas bancarias, números de tarjeta de crédito, identidades, etc. Resumiendo "todos los datos posibles" para luego ser usados de forma fraudulenta.

¿En qué consiste?

Los atacantes suplantan la imagen de una empresa, un banco o una entidad pública, de esta manera te hacen "creer" que los datos solicitados proceden de un sitio "Oficial" cuando en realidad no lo es.

¿Cómo puedo evitarlo?

Jamás respondas solicitudes de información personal a través de correos electrónicos, llamadas telefónicas o mensajes de texto (SMS). Las entidades u organismos con los que tenés relación ya tienen tus datos y nunca te solicitarían contraseñas, números de tarjeta de crédito o cualquier información personal por correo electrónico, por teléfono o SMS.

Uso de Internet

¿Es segura la descarga de información de Internet?

Debes evitar la descarga de programas desde **lugares no seguros** de Internet. Si tenés que descargar programas, procura confirmar que sea un sitio reconocido y que esté avalado por un organismo público o una empresa de antivirus.

Es necesario que todo el software instalado en el equipo provenga de una **fuente conocida y segura**. Tampoco hay que confiar en los archivos gratuitos que se descargan de sitios web desconocidos, ya que son una potencial vía de propagación de virus.

¿Puedo acceder a Internet por medios alternativos?

La ASI ofrece un servicio de Internet corporativo. El mismo tiene mecanismos de detección de malware / código dañino, sitios no seguros y otras amenazas. No intentes evadir o acceder a Internet por otros medios, porque ponés en peligro la integridad de la información de todo el **GCABA**.

Recordá que Internet debe ser utilizado únicamente con fines laborales.

COMUNICACIÓN DE INCIDENCIAS DE SEGURIDAD

Incidencias de seguridad

¿Cómo identifico una incidencia de seguridad?

Debes poner la máxima precaución si observás que en el equipo se llevan a cabo **acciones sospechosas** (aumento de tamaño de los archivos, aparición de avisos no habituales, recepción de correos de personas desconocidas o en idiomas no utilizados habitualmente, pérdidas de datos o programas, etc.).

¿A quién debo acudir?

Deberás reportar a Mesa de Ayuda, aquellos eventos que observes que no son usuales.

Recordá, que si tenés conocimiento o incluso sospechas de una incidencia, sos responsable de la comunicación de la misma a Mesa de Ayuda.

Y recordá que…

Sos responsable de la protección de la información que manejas o custodias y del cumplimiento de las políticas de seguridad vigentes en el **GCABA**.

¿Y si tengo alguna duda?

En Mesa de Ayuda**, 4323-9393** o a través de correo electrónico: asi.mat@buenosaires.gob.ar, estamos a tu disposición para cualquier aclaración sobre cómo hacer un uso seguro de la información del GCABA.

Muchas Gracias

Marco Normativo de IT

GU0101 – Guía de Protección de Datos Personales

Agencia de Sistemas de Información

Gobierno de la Ciudad Autónoma de Buenos Aires

Guía de Protección de Datos Personales

5. Introducción

Todo tratamiento de datos personales genera un potencial riesgo para el derecho a la privacidad. Para enfrentar estas amenazas se ha establecido el derecho humano a la autodeterminación informativa, es decir, el derecho que tiene toda persona de controlar los alcances de su información personal. La presente guía está basada en la información publicada en el sitio web de la Defensoría del Pueblo.

6. Objetivo

Orientar a los funcionarios del GCABA en el proceso de adecuación e inscripción de las bases de datos públicas según lo dispuesto por la Ley CABA 1845/2006; sometiendo las mismas a la supervisión y control de la Defensoría del Pueblo de la CABA, actuando como Órgano de Control en el Cumplimiento de la Ley.

Instaurar entre los funcionarios públicos la cultura de la protección de datos personales como un elemento de singular importancia en el ejercicio de sus funciones.

7. Alcance

Esta guía alcanza todas las actividades relacionadas directa o indirectamente con la utilización de los recursos de tecnología de información y de las comunicaciones del GCABA.

8. Contenido

Objeto de aplicación de la Ley

La Ley de Protección de Datos Personales 1.845 tiene por objeto regular dentro del ámbito de la Ciudad de Buenos Aires, el tratamiento de datos personales referidos a personas físicas o de existencia ideal, asentados o destinados a ser asentados en archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires, a los fines de garantizar el derecho al honor, a la intimidad y a la autodeterminación informativa, de conformidad a lo establecido por el artículo 16 de la Constitución de la Ciudad de Buenos Aires.

ANEXO I

Ámbito de aplicación de la Ley

Su aplicación está limitada al ámbito público de la Ciudad de Buenos Aires, es decir que situaciones referidas a bancos de datos nacionales o empresas privadas no se encontrarían bajo la competencia de esta Ley. Sin embargo, en esos supuestos podrá darse intervención a la Dirección Nacional de Protección de Datos Personales http://www.jus.gov.ar/dnpdpnew/ dependiente del Ministerio de Justicia y Derechos Humanos.

Forman parte del sector público de la Ciudad:

- Órganos pertenecientes a la administración central y descentralizada cualquiera fuere su nivel, como por ejemplo ministerios, direcciones generales y subsecretarías.
- Entes autárquicos y autónomos, como por ejemplo el Ministerio Público Fiscal.
- Empresas y sociedades del Gobierno de la Ciudad o sociedades anónimas con participación estatal mayoritaria, sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde tenga participación en el capital o en la formación de las decisiones societarias, por ejemplo AUSA o CEAMSE.
- Los Poderes Legislativo y Judicial, en cuanto a su actividad administrativa.

Definiciones

A los fines de un mejor entendimiento de la norma se aclaran los siguientes conceptos:

- **Datos personales**: Información de cualquier tipo referida a personas físicas o jurídicas, determinadas o determinables.
- **Datos sensibles**: Aquellos datos personales que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir, por su naturaleza o su contexto, algún trato discriminatorio al titular de los datos.
- **Archivos, registros, bases o bancos de datos**: Indistintamente, designan al conjunto organizado de datos personales objeto de tratamiento, cualquiera sea la modalidad o forma de su recolección, almacenamiento, organización o acceso, incluyendo tanto los automatizados como los manuales.
- **Tratamiento de datos**: Cualquier operación o conjunto de operaciones, efectuadas o no mediante procedimientos automatizados, que permitan la recolección, conservación, orden,

almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción, registro, organización, elaboración, extracción, utilización, cotejo, supresión y, en general, el procesamiento de datos personales, así como también su cesión a terceros a través de todo tipo de comunicación, consulta, interconexión, transferencia, difusión o cualquier otro medio que permita el acceso a los mismos.

- **Titular de datos**: Persona física o jurídica cuyos datos sean objeto de tratamiento.
- **Responsable del archivo, registro, base o banco de datos**: Persona física o jurídica del sector público de la Ciudad de Buenos Aires que sea titular de un archivo, registro, base o banco de datos.
- **Encargado del tratamiento**: Persona física o jurídica, autoridad pública, dependencia u organismo que, solo o juntamente con otros, realice tratamientos de datos personales por cuenta del responsable del archivo, registro, base o banco de datos.
- **Usuario de datos**: Persona física que, en ocasión del trabajo y cumpliendo sus tareas específicas, tenga acceso a los datos personales incluidos en cualquier archivo, registro, base o banco de datos del sector público de la Ciudad de Buenos Aires.
- **Fuentes de acceso público irrestricto**: Exclusivamente, se entienden por tales a los boletines, diarios o repertorios oficiales, los medios de comunicación escritos, las guías telefónicas en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección o cualquier otro dato que indique de su pertenencia al grupo. Se entiende que la expresión "medios de comunicación escritos" incluye las publicaciones efectuadas a través de Internet en páginas Web públicas y oficiales, así como las reproducciones de publicaciones realizadas en soporte papel.

Órgano de control de la ley

La Defensoría del Pueblo de la Ciudad de Buenos Aires, de conformidad con lo establecido en la propia Ley de Protección de Datos, ha sido instaurada como el órgano de control del cumplimiento de los objetivos establecidos.

A tales fines, mediante la disposición 119/07 se creó el Centro de Protección de Datos Personales en el ámbito de la Defensoría http://www.cpdp.gov.ar/

Entre las misiones del órgano de control se encuentran:

- Diseñar y administrar el Registro de Bancos de Datos Personales del Sector Público de la Ciudad de Buenos Aires.
- Administrar y controlar el funcionamiento de la página Web del Centro.
- Realizar la inscripción de los organismos públicos de la Ciudad de Buenos Aires y de los prestadores de servicio.
- Elaborar y mantener actualizado el Manual de Protección de Datos Personales para los bancos de datos públicos.
- Elaborar -para su publicación y difusión- material explicativo para el público en general, como así también para la administración pública.
- Realizar eventos de capacitación y difusión.
- Desarrollar el plan de seguridad informática.
- Asistir y asesorar al usuario.
- Realizar toda otra acción que conduzca al mayor cumplimiento de la ley 1.845 y su reglamentación.

Principios rectores

Licitud del tratamiento de datos personales

Para que el tratamiento de datos personales sea legal debe cumplir con los siguientes requisitos (artículos 4, 6 y 24 de la ley 1.845):

- La creación y mantenimiento de bancos de datos debe responder a un propósito general y usos específicos lícitos y socialmente aceptados. Los archivos de datos no pueden tener finalidades contrarias a las leyes o a la moral pública (artículo 4).
- Todos los bancos de datos deben estar inscriptos en el Registro de Bancos de Datos a cargo de la Defensoría del Pueblo de la Ciudad de Buenos Aires (artículos 4, 18 y 23) y observar en su operación los principios que establece la normativa.
- Los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación con el ámbito y finalidad para los que se hubieren obtenido (artículo 6).
- La recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la presente ley (artículo 6).

ANEXO I

- Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas de aquellas que motivaron su obtención (artículo 6).
- Los datos deben ser exactos y actualizarse en el caso de que ello fuere necesario para responder con veracidad a la situación de su titular (artículo 6).
- Los datos total o parcialmente inexactos o que sean incompletos deben ser suprimidos y sustituidos, o en su caso completados, por el responsable o usuario del archivo, registro, base o banco de datos cuando se tenga conocimiento de la inexactitud o carácter incompleto de la información de que se trate, sin perjuicio de los derechos del titular establecidos en el artículo 13 de la presente ley (artículo 6).
- Los datos deben ser almacenados de modo que permitan el ejercicio del derecho de acceso de su titular (artículo 6).
- Los datos personales deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados, sin necesidad de que lo requiera el titular de los mismos (artículo 6).

No automaticidad

Son nulos e inválidos los actos y decisiones administrativos que impliquen una valoración del comportamiento o de la personalidad de las personas fundada en el tratamiento "automatizado" de sus datos personales. El titular de los datos tiene derecho a impugnar tales actos y decisiones, sin perjuicio de las demás acciones que le pudieran corresponder. Asimismo, siempre tendrá derecho a conocer la lógica del proceso de decisión automatizada explicado en términos simples y adecuados a su nivel social y cultural (artículo 21).

Tratamiento de datos sensibles

Los datos sensibles no pueden tratarse sin que medien razones de interés general autorizadas por ley o el consentimiento libre, previo, expreso, informado y por escrito del titular de los datos (artículo 8). Expresamente, el artículo 8 de la ley 1.845 dispone: "1. Ninguna persona puede ser obligada a proporcionar datos sensibles. En particular no se podrá solicitar a ningún individuo datos sensibles como condición para su ingreso o promoción dentro del sector público de la Ciudad de Buenos Aires. 2. Los datos sensibles sólo pueden ser tratados cuando medien razones de interés general autorizadas por ley. También podrán ser tratados con finalidades estadísticas o científicas, siempre y cuando no puedan ser identificados sus titulares. 3. Queda prohibida la formación de archivos, registros, bases o bancos de datos que almacenen información que directa o indirectamente revele datos sensibles, salvo que la presente ley o cualquier otra expresamente disponga lo contrario o medie el consentimiento libre, previo, expreso, informado y por escrito del titular de los datos. 4. Los datos relativos a antecedentes penales o contravencionales o infracciones administrativas sólo

pueden ser objeto de tratamiento por parte de las autoridades públicas competentes, en el marco de las leyes y reglamentaciones respectivas".

Sin embargo, vale destacar que cuando se trate de datos relativos a la salud por parte de los establecimientos sanitarios dependientes de la Ciudad de Buenos Aires, "... los profesionales vinculados a las ciencias de la salud que presten servicios en los mismos pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que acudan a los mismos o que estén o hubieren estado bajo tratamiento de aquéllos, respetando los principios del secreto profesional" (artículo 9).

Recolección de datos por parte de autoridades públicas

Por principio general, el tratamiento de datos personales por parte de las entidades públicas no requerirá el consentimiento del titular de los datos en la medida que se recaben para el ejercicio de funciones propias de los poderes de la Ciudad de Buenos Aires o en virtud de una obligación legal (artículo 7, inciso 3º).

El consentimiento deberá ser libre, expreso e informado y deberá constar por escrito o por otro medio que permita se le equipare de acuerdo a las circunstancias. El referido consentimiento prestado con otras declaraciones, deberá figurar en forma expresa y destacada, previa notificación al titular de datos, en forma adecuada a su nivel social y cultural, de la información que debe proporcionarse al titular del dato (artículo 7, inciso 1º). El consentimiento puede ser revocado por cualquier medio y en cualquier momento. Dicha revocación no tendrá efectos retroactivos (artículo 7, inciso 2º).

Cesión y divulgación de datos

Cesión entre organismos públicos: La cesión de datos personales puede efectuarse sin necesidad del consentimiento del titular del dato cuando se realice entre órganos del sector público de la Ciudad de Buenos Aires en forma directa, en la medida del cumplimiento de sus respectivas competencias (artículo 10, punto 3, inciso "c"); y cuando sea requerida por un magistrado del Poder Judicial, el Defensor del Pueblo o el Ministerio Público en el marco de una causa judicial en particular (artículo 10, punto 3, inciso "f").

Cesión a particulares: Los responsables de bancos de datos públicos podrán ceder datos a particulares en la medida que dicho acto se realice en ejercicio de la competencia y funciones del organismo (artículo 7, inciso 3 y artículo 10, inciso 3. b.); se acredite el interés legítimo del cesionario (artículo 10, inciso 1) identificándolo; se cumplan los principios de protección de datos (artículos 6 a 12); y no sean datos de tratamiento exclusivo (prohibición legal) o sensibles, ni se afecte la intimidad u otros derechos del titular del dato. En caso de que un organismo oficial en virtud de sus funciones específicas tenga destinados sus datos a la difusión al público en general, el requisito relativo al interés legítimo del cesionario se considera implícito en las razones de interés general que motivaron el acceso público irrestricto y la difusión de sus datos (artículo 10, decreto 725/2007).

ANEXO I

Cesión masiva: La cesión de datos que comprendan a un grupo colectivo de personas sólo puede ser autorizada por decisión del funcionario responsable, salvo que el banco de datos sea accesible en forma irrestricta por ley (2º párrafo del artículo 10, decreto 725/2007).

Responsabilidad solidaria: En todos los casos de cesión de datos personales, el cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias del cedente y éste responderá solidaria y conjuntamente por la observancia de las mismas ante el organismo de control y el titular de los datos de que se trate (artículo 10, inciso 4).

Transferencia internacional

- Únicamente se realizará una transferencia internacional de datos personales cuando se garanticen niveles de protección adecuados, salvo en los siguientes casos (artículo 12):
- Colaboración judicial internacional.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del afectado o una investigación epidemiológica, en tanto se hayan disociado los datos y el titular resulte inidentificable.
- Transferencias bancarias, en lo relativo a las transacciones respectivas y conforme la legislación que les resulte aplicable.
- Cuando la transferencia se hubiera acordado en el marco de tratados internacionales en los cuales la República Argentina sea parte y se realice a requerimiento de la autoridad judicial y en el marco de una causa.
- Cuando la transferencia tenga por objeto la cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo y el narcotráfico, y se realice a requerimiento de la autoridad judicial y en el marco de una causa.
- Cuando se obtenga el consentimiento del titular de los datos para dicha transferencia.

Se presume un nivel adecuado de protección cuando dicha tutela se deriva directamente del ordenamiento jurídico vigente o de sistemas de autorregulación o del amparo que establezcan las cláusulas contractuales que prevean la protección de datos personales (artículo 12, decreto 725/2007). No es necesario el consentimiento en caso de transferencia de datos desde un banco de datos del sector público que esté constituido para facilitar información al público y abierto a la consulta por el público en general o por cualquier persona que pueda demostrar un interés legítimo (artículo 12, decreto 725/2007).

Creación de bancos de datos del sector público

- La creación y mantenimiento de bancos de datos debe responder a un propósito general y usos específicos lícitos y socialmente aceptados y no pueden tener finalidades contrarias a las leyes o a la moral pública (artículo 4).

- Las normas sobre creación, modificación o supresión de archivos, registros, bases o bancos de datos pertenecientes a organismos públicos deberán publicarse en el Boletín Oficial de la Ciudad de Buenos Aires e indicar: a) Características y finalidad del archivo; b) personas respecto de las cuales se pretenda obtener datos y el carácter facultativo u obligatorio de su suministro por parte de aquéllas; c) procedimiento de obtención y actualización de los datos; d) estructura básica del archivo, informatizado o no, y la descripción de la naturaleza de los datos personales que contendrá; e) las cesiones, transferencias o interconexiones previstas; f) órgano responsable del archivo, precisando dependencia jerárquica en su caso; g) dependencia ante la cual los ciudadanos pueden ejercer los derechos reconocidos por la presente ley (artículo 4).
- En las disposiciones que se dicten para la supresión de los archivos, registros, bases o bancos de datos se establecerá el destino de los mismos o las medidas que se adopten para su destrucción (artículo 4).

Obligaciones de los funcionarios que manejan bancos de datos

Obligaciones de los responsables de las bases de datos

La ley impone a quien posea una base de datos pública que contenga datos personales los siguientes deberes (artículos 16, 17, 18 y 13):

- Inscribir el banco de datos en el Registro de Bancos de Datos del Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires (artículo 18).
- Requerir y obtener el consentimiento del titular de los datos personales, previo a su obtención y tratamiento, en los términos del artículo 7° de la presente ley.
- Respeto de los derechos del titular del dato: acceso, rectificación, actualización y/o supresión, procediendo en forma inmediata a la rectificación, actualización o supresión de los datos personales cuando fueran total o parcialmente inexactos, incompletos o desactualizados (artículos 13 y 18).
- Informar al titular de los datos en forma expresa y clara -y bajo pena de nulidad- previamente a recabar información referida a su persona, acerca de: la existencia del archivo, registro, base o banco de datos, electrónico o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable; la finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o categorías de destinatarios; el carácter obligatorio o facultativo de la respuesta a las preguntas que le sean formuladas; las consecuencias que se deriven de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos; la facultad y modo de ejercer los derechos de acceso, rectificación, actualización y

supresión de los datos que le confiere la presente ley; detalle sobre los órganos de aplicación de la presente ley (artículo 18).

- Respetar los principios de la protección de datos personales.
- Seguridad (artículo 17).
- Confidencialidad (artículo 16).

Obligaciones del encargado del tratamiento de las bases de datos

- El encargado del tratamiento -a quien el artículo 3 define como quien/es realice/n tratamientos de datos personales por cuenta del responsable del banco de datos- tiene los mismos deberes y obligaciones exigidas al responsable del banco de datos sobre la confidencialidad como del tratamiento de los datos personales conforme a los principios de protección de la ley (artículo 19).
- El encargado del tratamiento sólo actúa siguiendo instrucciones del responsable y no podrá, bajo ningún concepto, ceder los datos personales sometidos a tratamiento, ni aun para su conservación (artículo 19).
- A través de la Disposición Nº 05/CPDP-DP/11, el Director del Centro de Protección de Datos Personales crea la categoría registral de custodio de registros o bases de datos personales del GCABA y asigna este rol a la Agencia de Sistemas de Información, que aloja y administra bajo la figura de custodia, las bases de datos del GCABA, en cumplimiento de la Ley 1845 (artículo 4, 18 y 23).

Obligaciones del usuario de datos

- Todas las personas que actúen, trabajen o presten servicios de cualquier tipo en o para algún órgano del sector público de la Ciudad de Buenos Aires sólo podrán realizar tratamiento de datos personales cuando así lo disponga el responsable del banco de datos u obligación legal (artículo 20).
- El usuario tiene los mismos deberes y obligaciones exigidas al responsable del banco de datos sobre la confidencialidad como del tratamiento de los datos personales conforme a los principios de protección de la ley (artículo 20).
- El usuario de datos sólo podrá ceder los datos personales sometidos a tratamiento siguiendo expresas instrucciones del responsable del tratamiento (artículo 20).

ANEXO I

Inscripción en el registro

- Todo banco de datos alcanzado por la ley 1.845 debe inscribirse a través de su responsable en el Registro de Banco de Datos habilitado en el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires (artículo 4, 18 y 23).
- Los bancos de datos que deben inscribirse son aquellos de titularidad de los órganos pertenecientes a la administración central, descentralizada, de entes autárquicos, empresas y sociedades del estado, sociedades anónimas con participación estatal mayoritaria, sociedades de economía mixta y todas aquellas otras organizaciones empresariales donde el Estado de la Ciudad de Buenos Aires tenga participación en el capital o en la formación de las decisiones societarias, del Poder Legislativo y del Judicial en cuanto a su actividad administrativa, y de los demás órganos establecidos en el Libro II de la Constitución de la Ciudad de Buenos Aires (artículo 2, ley 1.845).
- Los prestadores de servicios de tratamiento de datos deben también proceder a inscribirse en el Registro creado al efecto: Registro de Prestadores de Servicios de Tratamiento de Datos (artículo 23, decreto 725/2007).

Seguridad

El tratamiento de datos personales se sujetará a las medidas de seguridad establecidas en la normativa nacional (ley 25.326, decreto 1.558/2001 y disposiciones DNPDP). Sin perjuicio de ello, la ley 1.845 expresamente dispone que el responsable del banco de datos, el encargado del tratamiento y los usuarios de datos deben adoptar todas las medidas técnicas y de organización necesarias y adecuadas que impidan la adulteración, pérdida, destrucción y el tratamiento o acceso no autorizado a los datos incluidos en sus archivos, registros, bases o bancos de datos. Dichas medidas deberán garantizar un nivel de seguridad apropiado en relación con la tecnología aplicada y sus avances, con la naturaleza de los datos tratados y con los riesgos propios del tratamiento (artículo 17, ley 1.845).

Confidencialidad

El responsable del archivo, registro, base o banco de datos, el encargado del tratamiento y los usuarios de datos están obligados al secreto profesional respecto de los datos personales sujetos a tratamiento y a mantenerlo una vez finalizadas las funciones o actividades en virtud de las cuales dichos datos fueron sometidos a tratamiento. En el caso del encargado del tratamiento y de los usuarios de datos, tal deber subsistirá aun después de finalizada su relación con el responsable del archivo, registro, base o banco de datos. El deber de secreto podrá ser relevado por resolución

judicial cuando medien razones fundadas relativas a la seguridad pública, la defensa nacional o la salud pública (artículo 16).

Infracciones a lo estipulado legalmente

Infracciones a la ley

El artículo 25 de la ley 1.845 considera como infracciones las siguientes conductas:

- Realizar el tratamiento de datos desconociendo los principios generales en materia de protección de datos, como por ejemplo: recolectar datos por medios desleales (Título III).
- Incumplir las obligaciones descriptas en el Título V (Obligaciones Relacionadas con los Datos Personales Asentados en Archivos, Registros, Bases o Bancos de Datos).
- No proceder a solicitud -del titular de los datos o del organismo de control- a la supresión, rectificación y actualización de los datos personales en los supuestos, tiempo y forma establecidos en esta ley.
- Obstaculizar o impedir el derecho de acceso reconocido en esta ley al titular o al organismo de control en los supuestos, tiempo y forma que la misma estipula.
- Ceder datos personales en infracción a los requisitos que se establecen en la presente ley.
- Crear archivos, registros, bases o bancos de datos, ponerlos en funcionamiento y/o iniciar el tratamiento de datos personales sin el cumplimiento de los requisitos establecidos en esta ley.
- No cumplimentar los demás extremos o requisitos que esta ley establece, así como aquellos que el organismo de control establezca en ejercicio de su competencia.
- Obstruir las funciones que por esta ley se le reconocen al organismo de control.
- Tratar los datos de carácter personal de un modo que lesione, violente o desconozca los derechos a la privacidad, autodeterminación informativa, imagen, identidad y honor, así como cualquier otro derecho de que sean titulares las personas físicas o de existencia ideal.

  La reglamentación determinará las condiciones y procedimientos para la aplicación de las sanciones previstas, las que deberán graduarse en relación a la gravedad y extensión de la violación y de los perjuicios derivados de la infracción, garantizando el principio del debido proceso.

ANEXO I

Los responsables, usuarios, encargados o cesionarios de archivos, registros, bases o bancos de datos del sector público de la Ciudad de Buenos Aires que en forma arbitraria obstruyan el ejercicio de los derechos que la presente ley le reconoce a los ciudadanos serán considerados incursos en falta grave (artículo 26).

Sanciones

- **Responsable del banco de datos**: En caso de comisión de alguna de las infracciones previstas en el artículo 25 de la ley 1.845 (sin perjuicio de las responsabilidades administrativas, por daños y perjuicios y/o de las sanciones penales que pudieran corresponder), el organismo de control dictará resolución recomendando al órgano del cual dependa jerárquicamente el banco de datos: a) la adopción de las medidas que proceda adoptar para que cesen o se corrijan los efectos de la infracción. Dicha resolución se comunicará al responsable del archivo, registro, base o banco de datos, al órgano del cual dependa jerárquicamente, al titular del dato y -cuando corresponda- a los encargados del tratamiento y cesionarios de los datos personales; b) la aplicación de las pertinentes sanciones administrativas a los responsables de la infracción individualizando al responsable, los hechos y los perjudicados. Cumplida la recomendación del organismo de control, el Poder Ejecutivo deberá abrir un sumario administrativo para determinar si existió o no una infracción a la presente ley y dicha conclusión deberá ser informada a la Defensoría del Pueblo.

  En los supuestos de infracción contemplados en los párrafos 5to (cesión de datos) y 6to (creación del banco de datos) del artículo 25 de la ley 1.845, el organismo de control podrá requerir al órgano del cual dependa jerárquicamente el banco de datos, la cesación en la utilización o cesión ilícita de los datos personales y -en caso de corresponder- la inmovilización del archivo, registro, base o banco de datos hasta tanto se restablezcan los derechos de los titulares de datos afectados.

- **Prestador de servicios de tratamiento de datos**: En caso de comisión de alguna de las infracciones previstas en el artículo 25 de la ley por parte de un tercero prestador se servicios de tratamiento de datos personales en virtud de un contrato celebrado de acuerdo a lo previsto por el artículo 5° de la ley, de acuerdo al tipo de infracción de que se trate, serán de aplicación con respecto al contratista infractor las sanciones establecidas por la ley nacional 25.326, su reglamentación y/o sus modificaciones.

ANEXO I

Derechos del ciudadano

Las opciones se dividen en "administrativas" y "judiciales":

Información a proporcionar por el responsable al titular de los datos

El ciudadano tiene derecho a que el responsable de un banco de datos lo informe por completo y en todo momento acerca de los usos concretos que se realizan de sus datos personales, en particular al momento de su recolección; por ello, el responsable o usuario de la base de datos informará en forma expresa y clara:

- La existencia del archivo, registro, base o banco de datos, electrónico o de cualquier otro tipo de que se trate y la identidad y domicilio de su responsable (artículo 18, ley 1.845).
- La finalidad para la que serán tratados y quiénes pueden ser sus destinatarios o categorías de destinatarios (artículo 18).
- El carácter obligatorio o facultativo de la respuesta a las preguntas que le sean formuladas (artículo 18).
- Las consecuencias que se deriven de proporcionar los datos, de la negativa a hacerlo o de la inexactitud de los mismos (artículo 18).
- La facultad y modo de ejercer los derechos de acceso, rectificación, actualización y supresión de los datos que le confiere la presente ley (artículo 18).
- Detalle sobre el órgano de aplicación de la presente ley: Defensoría del Pueblo de la Ciudad de Buenos Aires (artículo 18).

Cuando se traten datos personales recolectados a través de Internet, los sitios interactivos de la Ciudad de Buenos Aires deberán informar al titular de los datos personales los derechos que esta ley y la ley nacional les otorgan mediante una política de privacidad ubicada en un lugar visible de la página Web (artículo 4).

Los bancos de datos deben cumplir con el derecho que tiene cualquier persona a conocer su existencia, finalidad, la identidad y domicilio del responsable, destinatarios y categorías de destinatarios, condiciones de organización, funcionamiento, procedimientos aplicables, normas de seguridad, garantías para el ejercicio de los derechos del titular de los datos, así como toda otra información registrada (artículo 24).

Información de existencia de archivos

Más allá de lo expuesto, toda persona tiene derecho a ser informada sobre la existencia de archivos, registros, bases o bancos de datos de titularidad del sector público de la Ciudad de Buenos Aires y, en tal contexto, conocer su finalidad, identidad y domicilio de sus responsables. Ello podrá requerirse

al Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires (artículo 13).

La consulta es pública y gratuita. Vale destacar que el Centro de Protección de Datos Personales de la Defensoría del Pueblo de la Ciudad de Buenos Aires recaba parte de dicha información a través del proceso de inscripción de los bancos de datos en el Registro, pero no posee el contenido de dichos bancos de datos personales, pues la inscripción no implica la cesión del contenido, sino una descripción del mismo.

Derecho de Acceso

Ante la existencia de un Banco de Datos que contenga información personal, el titular del dato, previa acreditación de su identidad, tiene derecho a conocer la información referida a su persona. Más concretamente -según el artículo 13, inciso "b"-, el derecho de acceso permitirá al titular del dato:

- Exigir que se le informe, en forma amplia y sobre la totalidad de la información aun cuando se solicite sólo un aspecto de sus datos personales, sin restricciones ni requisitos de ningún tipo, y en un plazo no mayor de diez (10) días hábiles, acerca de la identidad de las personas a las que se le hubieran cedido sus datos, del origen de los datos incluidos en el archivo, registro, base o banco de datos consultado, y de la lógica utilizada en los tratamientos automatizados de datos que se hubieran realizado. El plazo se podrá prorrogar en forma excepcional por otros diez (10) días hábiles de mediar circunstancias que hagan difícil reunir la información solicitada.
- Optar para que la información se suministre por escrito, por medios electrónicos, telefónicos, de imagen u otro medio idóneo a tal fin.
- Ejercerlo en forma gratuita a intervalos no inferiores a dos meses, salvo que se acredite un interés legítimo al efecto, en cuyo caso podrá ejercerlo en cualquier momento.
- Iniciar acción judicial de habeas data una vez vencido el plazo sin que se satisfaga el pedido, o si evacuado el mismo, éste se estimara insuficiente.

Derecho de rectificación, actualización o supresión

A solicitud del titular del dato o advertido el error o falsedad, el responsable o usuario del banco de datos procederá -en el plazo máximo de cinco (5) días hábiles y siempre de manera gratuita- a rectificar, actualizar o -cuando corresponda- suprimir o someter a confidencialidad sus datos personales (artículo 13, inciso "c").

La supresión no procede cuando pudiese causar perjuicios a derechos o intereses legítimos de terceros o cuando existiera una obligación legal de conservar los datos (artículo 13, inciso "c").

ANEXO I

Durante el proceso de verificación y rectificación del error o falsedad de la información que se trate, el responsable o usuario del banco de datos deberá, o bien bloquear el banco de datos, o bien consignar la circunstancia de que dicha información se encuentra sometida a revisión al proveer información relativa al titular de los datos que hubiera solicitado la rectificación, actualización o supresión (artículo 13, inciso "c").

En el supuesto de cesión de datos personales a terceros, el responsable del archivo, registro, base o banco de datos cedente debe notificar la rectificación, actualización o supresión al cesionario dentro del quinto día hábil de efectuado el tratamiento del dato, debiendo el cesionario tomar cuenta de ello dentro del plazo de dos días de recibida la notificación (artículo 13, inciso "c").

El incumplimiento de esta obligación dentro del plazo habilitará al interesado a promover sin más la acción judicial de habeas data (artículo 13, inciso "c").

El ejercicio del derecho de acceso no requiere de fórmulas específicas, siempre que garantice la identificación del titular del dato, sus representantes legales o sucesores, pudiendo realizarse personalmente, por medio escrito o intimación fehaciente con constancia de recepción (artículo 13, decreto 725/2007).

Los responsables de las bases de datos podrán disponer de otros servicios de acceso como los medios electrónicos, las líneas telefónicas, la recepción del reclamo en pantalla u otro medio idóneo a tal fin. En cada supuesto, el encargado del registro podrá ofrecer preferencia de medios para conocer la respuesta requerida, a opción del titular de los datos (artículo 13, decreto 725/2007).

A fin de permitir que el titular de los datos tome conocimiento de la rectificación, actualización, supresión o confidencialidad de sus datos personales efectuada por el banco de datos, el órgano requerido deberá comunicar al titular de los datos que ha procedido a rectificar, actualizar, suprimir o someter a confidencialidad los datos personales solicitados, en un plazo máximo de cinco (5) días hábiles contados a partir del vencimiento del plazo para tal acción (artículo 13, decreto 725/2007).

A los efectos de cumplir con el requisito legal de informar cuando los datos personales se encuentren sometidos a revisión con motivo de una rectificación, actualización, supresión o confidencialidad, el responsable del banco de datos deberá consignar el siguiente mensaje: "Esta información está sujeta a revisión por petición, del titular de los datos personales en virtud de lo establecido por el artículo 13 de la ley 1.845" (artículo 13, decreto 725/2007).

Denegación del derecho de acceso, rectificación o supresión

Vale destacar que existen excepciones a los derechos mencionados; en efecto, la ley establece las siguientes:

- Razones fundadas en el orden o la seguridad pública.

ANEXO I

- La protección de los derechos o intereses de terceros cuando así lo disponga una autoridad judicial a partir de una medida cautelar inscripta.
- Cuando existieran medidas cautelares judiciales o administrativas, inscriptas, vinculadas a la investigación sobre el cumplimiento de obligaciones tributarias o previsionales, el desarrollo de funciones del control de la salud o del medio ambiente, la investigación de delitos y la verificación de sanciones administrativas.
- La resolución que deniegue el ejercicio de los derechos reconocidos por la presente ley debe ser dispuesta por un funcionario de jerarquía equivalente o superior a "director general", en forma fundada explicitando la medida que ampara la negativa y notificada al titular del dato.

Sin perjuicio de lo arriba expuesto, se debe brindar acceso a los archivos, registros, bases o bancos de datos en la oportunidad en que el titular de los datos tenga que ejercer su derecho de defensa.

Acción de habeas data

Como se mencionó, otra de las opciones previstas en favor del titular del dato consiste en la promoción de una acción judicial de habeas data ante el incumplimiento por parte del banco de datos de los derechos de acceso, actualización, rectificación, confidencialidad y supresión de los datos (artículo 13, ley 1.845).

Asimismo, el artículo 28 habilita la acción para los siguientes supuestos: a) para tomar conocimiento de los datos personales almacenados en archivos, registros o bancos de datos del sector público de la Ciudad de Buenos Aires, su fuente, origen, finalidad o uso que del mismo se haga; b) en los casos en que se presuma la falsedad, inexactitud, desactualización de la información de que se trata, o el tratamiento de datos en infracción de la ley nacional 25.326 o la presente ley, para exigir su rectificación, supresión, confidencialidad o actualización; c) en los casos de incumplimiento de las disposiciones previstas en la presente ley.

Los responsables de bancos de datos deben tener especialmente presente los vencimientos de los plazos legales para responder al ejercicio de los derechos de acceso, actualización, rectificación, confidencialidad y supresión de los datos, pues su mero vencimiento habilita la acción de habeas data; lo que implica que el Organismo, aun cuando haga lugar a la solicitud, si lo hace tardíamente y la acción judicial ya fue iniciada, deba abonar las costas judiciales.

ANEXO I

Otras cuestiones adicionales

Vale tener presente algunas otras cuestiones de importancia en el ámbito de la protección de datos:

Privacidad laboral

El artículo 39 de la ley 1.845 regula la privacidad laboral en el ámbito del sector público de la Ciudad de Buenos Aires, y dispone: "Cuando el correo electrónico sea provisto por un organismo del sector público de la Ciudad de Buenos Aires a sus dependientes en función de una relación laboral, se entenderá que la titularidad del mismo corresponde al empleador, independientemente del nombre y clave de acceso que sean necesarias para su uso.

El empleador se encuentra facultado para acceder y controlar toda la información que circule por dicho correo electrónico laboral, como asimismo a prohibir su uso para fines personales.

El ejercicio de las facultades de control sobre el correo electrónico laboral por parte del empleador, así como sus condiciones de uso y acceso, deberá ser notificado por escrito al trabajador, como requisito previo a su ejercicio.

El empleador deberá notificar fehacientemente a sus dependientes, la política establecida respecto del acceso y uso de correo electrónico personal, así como del uso de Internet en el lugar de trabajo.

El incumplimiento de las órdenes emanadas del superior con respecto a la política de uso del correo electrónico y de Internet en lugar de trabajo según lo previsto en esta norma, será sancionado de conformidad con lo dispuesto en los arts. 10 y 47 de la Ley Nº 471 (Ley de Relaciones Laborales en la Administración Pública de la Ciudad Autónoma de Buenos Aires)".

Bases de datos policiales

Si bien nada dispone al respeto la ley 1.845, cabe tener presente que la ley 25.326 regula el tratamiento de datos personales por parte de las bases de datos policiales, de servicios de inteligencia del Estado y de las Fuerzas Armadas, tanto las de fines administrativos como las de defensa nacional o seguridad pública:

"1. Quedarán sujetos al régimen de la presente ley, los datos personales que por haberse almacenado para fines administrativos deban ser objeto de registro permanente en los bancos de datos de las fuerzas armadas, fuerzas de seguridad, organismos policiales o de inteligencia; y aquellos sobre antecedentes personales que proporcionen dichos bancos de datos a las autoridades administrativas o judiciales que los requieran en virtud de disposiciones legales. 2. El tratamiento de datos personales con fines de defensa nacional o seguridad pública por parte de las fuerzas

armadas, fuerzas de seguridad, organismos policiales o inteligencia, sin consentimiento de los afectados, queda limitado a aquellos supuestos y categoría de datos que resulten necesarios para el estricto cumplimiento de las misiones legalmente asignadas a aquéllos para la defensa nacional, la seguridad pública o para la represión de los delitos. Los archivos, en tales casos, deberán ser específicos y establecidos al efecto, debiendo clasificarse por categorías, en función de su grado de fiabilidad. 3. Los datos personales registrados con fines policiales se cancelarán cuando no sean necesarios para las averiguaciones que motivaron su almacenamiento." (artículo 23 de la ley 25.326).

Estadísticas y censos

La ley 1.845 permite que los datos sensibles -aquellos que revelan origen racial o étnico, opiniones políticas, convicciones religiosas o morales, afiliación sindical, información referente a la salud o a la vida sexual o cualquier otro dato que pueda producir discriminación- puedan ser tratados con finalidades estadísticas o científicas, siempre y cuando no puedan ser identificados sus titulares (inciso 2 del artículo 8).

En tal sentido, la ley 25.326 establece que las normas de protección de datos no se aplican a "... las encuestas de opinión, mediciones y estadísticas relevadas conforme a la ley 17.622, trabajos de prospección de mercados, investigaciones científicas o médicas y actividades análogas, en la medida que los datos recogidos no puedan atribuirse a una persona determinada o determinable. 2. Si en el proceso de recolección de datos no resultara posible mantener el anonimato, se deberá utilizar una técnica de disociación, de modo que no permita identificar a persona alguna" (artículo 28 de la ley 25.326). En caso de que mediante dichas actividades se viole la ley 25.326 serán pasibles de las multas previstas por el artículo 31 de la ley 25.326 (reglamentación del artículo 28, decreto 1.558/2001).

Servicios sobre Solvencia Patrimonial y de Crédito

En el caso que bancos de datos personales del sector público de la Ciudad de Buenos Aires (organismos, empresas o dependencias) se dediquen a la prestación de servicios de información sobre solvencia patrimonial y de crédito, quedan sujetos, en lo que a la prestación de dichos servicios se refiere, a las disposiciones específicas de la ley nacional 25.326 o de la ley 1.845, la que resulte más favorable al titular del dato (artículo 38, ley 1.845). Al respecto, el artículo 26 de la ley 25.326 expresamente dispone: "1. En la prestación de servicios de información crediticia sólo pueden tratarse datos personales de carácter patrimonial relativos a la solvencia económica y al crédito, obtenidos de fuentes accesibles al público o procedentes de informaciones facilitadas por el interesado o con su consentimiento. 2. Pueden tratarse igualmente datos personales relativos al cumplimiento o incumplimiento de obligaciones de contenido patrimonial, facilitados por el acreedor o por quien actúe por su cuenta o interés. 3. A solicitud del titular de los datos, el responsable o usuario del banco de datos público, le comunicará las informaciones, evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses..." (inciso 3ro.), no siendo exigible

a la administración pública indicar el nombre y domicilio del cesionario en el supuesto de tratarse de datos obtenidos por cesión para el caso de archivos o bases de datos públicos dependientes de un organismo oficial destinadas a la difusión al público en general (2do. párrafo de la reglamentación del artículo 26, decreto 1.558/2001). "4. Sólo se podrán archivar, registrar o ceder los datos personales que sean significativos para evaluar la solvencia económico-financiera de los afectados durante los últimos cinco años. Dicho plazo se reducirá a dos años cuando el deudor cancele o de otro modo extinga la obligación, debiéndose hacer constar dicho hecho. 5. La prestación de servicios de información crediticia no requerirá el previo consentimiento del titular de los datos a los efectos de su cesión, ni la ulterior comunicación de ésta, cuando estén relacionados con el giro de las actividades comerciales o crediticias de los cesionarios".

Generalidades

Cualquier violación a la presente política puede derivar en la restricción inmediata del acceso a la *información digital* sin perjuicio de otras acciones que se puedan emprender en el ámbito administrativo, civil o penal.

La presente política debe ser interpretada armónicamente con el plexo normativo vigente a nivel local y con las demás políticas y reglamentos dictados por la *ASI*. En caso de conflicto de interpretación se resolverá de buena fe, de conformidad a los fines perseguidos y de acuerdo a los principios generales del derecho.

G O B I E R N O DE LA C I U D A D DE B U E N O S A I R E S
2014, Año de las letras argentinas

Hoja Adicional de Firmas
Anexo

Número: IF-2014-18613717- -ASINF

Buenos Aires, Lunes 29 de Diciembre de 2014

Referencia: EE N° 04591478-MGEYA-ASINF-2.013 - Anexo I Marco Normativo de TI

El documento fue importado por el sistema GEDO con un total de 45 pagina/s.

RAUL MARTINEZ
DIRECTOR EJECUTIVO DE LA ASINF
AGENCIA DE SISTEMAS DE INFORMACIÓN (MMGC)