Providencia

Oficio N: 1401

Fecha: - 4 MAR 2024

Antecedente: Solicitud MU228T0009367 de fecha 22 de enero de 2024, de la Sra. Daniela Bustamante, Externo N°594 de fecha 22 de enero de 2024.-

Materia: Entrega de información por Ley de Transparencia, Ingreso Externo N°594/2024.-

DE: ALCALDESA MUNICIPALIDAD DE PROVIDENCIA

A: SRA. DANIELA BUSTAMANTE

En respuesta a su solicitud recibida por esta Municipalidad con fecha 22 de enero de 2024, donde requiere *"En relación con la Gestión Municipal de Educación, Cultura y Salud se solicita información correspondiente a periodo 2022 a 2024, sobre: 1.- Presupuesto Municipal asignado a: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales, año 2024 2.- Unidad, Departamento, sección u Oficina Municipal encargada de: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales. 3.- Plan anual de Capacitaciones año 2024. 4.- Lista o nómina o Registro de Incidencias en materia de Ciberseguridad o brecha de seguridad que haya afectado la confidencialidad, integridad o disponibilidad de datos personales, y reporte de la incidencia y medidas adoptadas para el restablecimiento de los sistemas, así como informe de daños. 5.- Inventario de Infraestructura Crítica municipal. 6.- Inventario de Activos de Información sobre Datos Personales que gestiona el Municipio, sobre Funcionarios, Ciudadanos, Proveedores, etc. 7.- Redes Sociales del Municipio. 8.- Medidas de seguridad técnicas y organizativas implementadas en el municipio para garantizar la confidencialidad, disponibilidad, integridad y resiliencia en el procesamiento de datos personales. 9.- Lista o nómina de procedimientos municipales que implican el procesamiento de Datos Personales. 10.- Lista o nómina de actividades de Tratamiento de Datos Personales. 11.- Lista o nómina de Contratos de Servicios contratados que implican el procesamiento de datos personales en manos de terceros distintos al municipio (por ejemplo, contratos de encargo de tratamiento con empresas proveedoras que ayudan en la organización de eventos, seguridad física para el control de ingreso y salida de visitantes, gestión de recaudación de pagos, patentes municipales, entrega de beneficios sociales, etc), y copia de éstos. 12.- Decretos, Instrucciones y/o Reglamentos que aprueben las siguientes Políticas: a) Política de Privacidad; b) Política de Cookies; c) Política de Tratamiento de Datos Personales; d) Política de Seguridad de la Información; y e) Política de Gestión de Incidentes de Ciberseguridad. 13.- Procedimientos sobre gestión de contraseñas y controles de acceso físico o lógico a los programas y sistemas municipales, uso de dispositivos institucionales, uso de dispositivos privados para fines institucionales. 14.- Procedimiento y responsable de la función de atención y respuesta al ejercicio los derechos de los titulares de datos personales, del derecho de acceso, rectificación, cancelación y oposición de los datos. 15.- Procedimientos municipales que impliquen recopilación de datos mediante sistemas biométricos (por ejemplo, captura de huellas digitales para registrar el ingreso de las personas que laboran en el municipio, sistemas de videovigilancia y, de ser el caso, si dicho sistema captura imagen y voz), y copia de los contratos de los respectivos proveedores de los servicios. 16.- Contratos para la instalación y gestión de cámaras de videovigilancia, y Unidad Técnica del Contrato. 17 .- Procedimiento de fiscalización efectuado al municipio relativo a la gestión que hace de datos personales ante la Contraloría*

Providencia

General de la República, Consejo para la Transparencia o Tribunales de Justicia." [sic], adjunto remito a Ud., Memorándum N°3965 de fecha 04 de marzo de 2024 de la Dirección Administración Municipal, con la información solicitada.

Los datos de carácter personal concernientes a personas naturales han sido protegidos según lo dispuesto en la Ley N°19.628 "SOBRE PROTECCION DE LA VIDA PRIVADA".

De no encontrarse conforme con la respuesta precedente, en contra de esta decisión Ud. podrá interponer amparo a su derecho de acceso a la Información ante el Consejo para la Transparencia, en el plazo de 15 días hábiles contados desde la notificación de este Oficio.-

Saluda Atentamente a Ud.,

I. MUNICIPALIDAD DE PROVIDENCIA
ALCALDESA
CHILE

EVELYN MATTHEI FORNET
Alcaldesa

NBR/CVR/MRMQ/MINU/MBR/JRJ/jvp.-

c.c ADMINISTRADORA MUNICIPAL
SECRETARÍA MUNICIPAL
DEPARTAMENTO DE TRANSPARENCIA

soyprovidencia

Memorándum : 3965.-

Fecha : 04 MAR 2024

Antecedente : 1.- Ingreso externo N°594 de 22 de enero de 2024 del Sra. Daniela Bustamante.
2.- Memorándum de Transparencia N°72 de 22 de enero de 2024 de Secretaría Municipal.

Materia : Envía respuesta al ingreso externo N°594 de 2024 de Transparencia.

DE : CAROL VARGAS ROJAS
ADMINISTRADORA MUNICIPAL

A : MARÍA RAQUEL DE LA MAZA QUIJADA
SECRETARIO ABOGADO MUNICIPAL

Junto con saludar cordialmente, en relación al ingreso externo N°594, que solicita información *"En relación con la Gestión Municipal (...) se solicita información correspondiente a periodo 2022 a 2024, sobre: 1.- Presupuesto Municipal asignado a: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales, año 2024..." [sic],* comunico a usted que la información se encuentra publicada en https://transparencia.providencia.cl/Carpeta/Listado/11.

"...2.- Unidad, Departamento, sección u Oficina Municipal encargada de: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales..." [sic], comunico a Ud. que, la información se encuentra publicada en nuestra página web:

www.providencia.cl
link: TRANSPARENCIA ACTIVA LEY TRANSPARENCIA
carpeta: POTESTADES Y MARCO NORMATIVO
sub-carpeta: MARCO NORMATIVO
sub-carpeta: REGLAMENTOS INTERNOS
sub-carpeta: REGLAMENTO INTERNO DE LA MUNICIPALIDAD DE PROVIDENCIA, ahí encontrará en el año 2023, el Decreto Exento N°688 de fecha 22 de mayo de 2023, que fija el texto refundido y sistematizado del Reglamento Interno de la Municipalidad de Providencia, en cuyos artículos 139 y siguientes encontrará la Dirección de Tecnología y Gestión Digital.

"...3.- Plan anual de Capacitaciones año 2024..." [sic], comunico a Ud. que de acuerdo a lo informado por la Dirección de Personas, en conformidad a la Ley Nº 20.285 "Sobre Acceso a la Información Pública", y las causales de reserva ahí establecidas, en el artículo 21, es decisión de esta Municipalidad denegar la entrega de la información, aplicándose en este caso el Nº1 letra b) que establece ***"Cuando su publicación, comunicación o conocimiento afecte el debido cumplimiento de la funciones del órgano requerido... b) Tratándose de antecedentes o deliberaciones previas a la adopción de una resolución medida o política, sin perjuicio que los fundamentos de aquellas sean públicos una vez que sean adoptadas."***, esto último en cuanto a que de acuerdo a lo informado por la Dirección de Personas el Plan Anual de Capacitación se encuentra en proceso de elaboración y por tanto, no se ha adoptado la decisión.

"...4.- Lista o nómina o Registro de Incidencias en materia de Ciberseguridad o brecha de seguridad que haya afectado la confidencialidad, integridad o disponibilidad de datos personales, y reporte de la incidencia y medidas adoptadas para el restablecimiento de los sistemas, así como informe de daños..." [sic], comunico a Ud. que de acuerdo a lo informado por nuestra Dirección de Tecnología y Gestión Digital tuvimos un incidente el cual fue debidamente reportado en conformidad con el Decreto N°273 de 2022, del Ministerio del Interior y Seguridad Pública, que establece obligación de reportar incidentes de ciberseguridad; y que la entrega de mayor información compromete la seguridad del sistema tecnológico, exponiéndonos a la explotación de vulnerabilidades del sistema.

"...5.- Inventario de Infraestructura Crítica municipal. 6.- Inventario de Activos de Información sobre Datos Personales que gestiona el Municipio, sobre Funcionarios, Ciudadanos, Proveedores, etc (...) 9.- Lista o nómina de procedimientos municipales que implican el procesamiento de Datos Personales. 10.- Lista o nómina de actividades de Tratamiento de Datos Personales. 11.- Lista o nómina de Contratos de Servicios contratados que implican el procesamiento de datos personales en manos de terceros distintos al municipio (por ejemplo, contratos de encargo de tratamiento con empresas proveedoras que ayudan en la organización de eventos, seguridad física para el control de ingreso y salida de visitantes, gestión de recaudación de pagos, patentes municipales, entrega de beneficios sociales, etc), y copia de éstos..." [sic], comunico a Ud. que en conformidad a la Ley Nº20.285, sobre acceso a la información pública, y las causales de reserva ahí establecidas, en el artículo 21, es decisión de esta Municipalidad denegar la entrega de la información, aplicándose en este caso el Nº2 **"cuando su publicidad, comunicación o conocimiento afecte los derechos de las personas, particularmente tratándose de su seguridad, salud, la esfera de su vida privada o derechos de carácter comercial o económico"**, de acuerdo a lo indicado por la Dirección de Tecnología y Gestión Digital la entrega a un tercero de esta información compromete la seguridad de los sistemas y servicios tecnológicos, exponiéndonos a la explotación de vulnerabilidades del sistema, incluso desconocidas por el fabricante. Lo anterior, implica que nos expone a accesos no autorizados de la información almacenada en nuestros sistemas tecnológicos y que debe ser resguarda por el municipio en virtud del artículo 19 N°4 de la Constitución Política de la República y de la Ley N°19.628, sobre protección de la vida privada, ya que pueden verse vulnerados los

derechos de las personas cuya información se encontrará almacenada en las bases de datos de nuestras soluciones tecnológicas.

"...7.- Redes Sociales del Municipio..." [sic], comunico a Ud. que, de acuerdo a lo informado por nuestras Direcciones de Comunicaciones, Barrios y Patrimonio y de Desarrollo Local, las redes sociales del Municipio son las siguientes:

Municipalidad:

- X: @muni_provi
- Instagram: @muniprovi
- Facebook: Municipalidad de Providencia
- Youtube: @muniprovi

Centro Cultural Montecarmelo:

- Instagram: @cmontecarmelo
- Facebook: Centro Montecarmelo

Departamento de Bibliotecas:

- Instagram: @biblotecasprovi
- Facebook: BibliotecasProvi
- Tik Tok: @biblotecasprovi

HUB Providencia:

- Instagram: @hubprovidencia
- Facebook: hubprovidenciacl

"...8.- Medidas de seguridad técnicas y organizativas implementadas en el municipio para garantizar la confidencialidad, disponibilidad, integridad y resiliencia en el procesamiento de datos personales (...) 12.- Decretos, Instrucciones y/o Reglamentos que aprueben las siguientes Políticas: a) Política de Privacidad; b) Política de Cookies; c) Política de Tratamiento de Datos Personales; d) Política de Seguridad de la Información; y e) Política de Gestión de Incidentes de Ciberseguridad. 13.- Procedimientos sobre gestión de contraseñas y controles de acceso físico o lógico a los programas y sistemas municipales, uso de dispositivos institucionales, uso de dispositivos privados para fines institucionales. 14.- Procedimiento (...) de la función de atención y respuesta al ejercicio los derechos de los titulares de datos personales, del derecho de acceso, rectificación, cancelación y oposición de los datos ..." [sic], adjunto remito a Ud., copia Decreto Ex. N°473 de fecha 13 de abril de 2022 que aprueba la Política de Seguridad y Confidencialidad de la Información y del Decreto Ex.D.T.G.D N°70 de fecha 31 de marzo de 2022 que aprueba el "Instructivo Control de Acceso, Identificación y Autenticación."

A mayor abundamiento, por bases de licitación nuestros prestadores de servicios tecnológicos, sus trabajadores y consultores asociados a éste están obligados a dar cumplimiento al "COMPROMISO DE CONFIDENCIALIDAD Y SEGURIDAD DE LA

INFORMACIÓN", a través de la firma de un formulario que debe ser entregado al momento de la celebración del contrato, con el objetivo de que el prestador del servicio guardará especial atención a la confidencialidad de los datos personales a que pueda tener acceso en virtud del presente contrato. En este sentido, el prestador del servicio no podrá recolectar, almacenar, transferir, transmitir, comunicar, tratar, ceder o usar, de cualquier forma, los datos indicados anteriormente, salvo que dichas acciones sean indispensables para el cumplimiento de las obligaciones consignadas en el presente contrato y/o que medie una autorización escrita por parte del representante legal de la Municipalidad de Providencia. en ningún caso se entenderá que él prestador del servicio tiene algún derecho sobre tales datos personales.

Concordante con lo anterior, nuestros convenios de colaboración incorporan una cláusula de confidencial y protección de datos personales de acuerdo normativa vigente, estableciendo la prohibición de almacenamiento, tratamiento o difusión de la información que han tomado conocimiento con ocasión del convenio, así como las responsabilidades de quienes infringieran esta normativa.

"...14.- (...) responsable de la función de atención y respuesta al ejercicio los derechos de los titulares de datos personales, del derecho de acceso, rectificación, cancelación y oposición de los datos..." [sic], comunico a Ud. que el cargo de "Delegado de Protección de Datos Personales" corresponde a don Juan Carlos Lillo Molina, profesional Encargado de la Seguridad de la Información dependiente de la Dirección de Tecnología y Gestión Digital.

Adjunto remito a Ud. copia Decreto Ex. N°422 de fecha 16 de febrero de 2021, que designa al funcionario, don JUAN CARLOS LILLO MOLINA, Encargado de Seguridad de la Información.

"...15.- Procedimientos municipales que impliquen recopilación de datos mediante sistemas biométricos (por ejemplo, captura de huellas digitales para registrar el ingreso de las personas que laboran en el municipio...y copia de los contratos de los respectivos proveedores de los servicios..." [sic], comunico a Ud. que de acuerdo a lo informado por nuestra Dirección de Tecnología y Gestión Digital no tenemos procedimientos municipales que impliquen recopilación de datos mediante sistemas biométricos.

"...16.- Contratos para la instalación y gestión de cámaras de videovigilancia, y Unidad Técnica del Contrato..." [sic], comunico a Ud. la información se encuentra publicada en Portal Mercado Público con el ID 2490-83-LR22 y 2490-45-LQ23.

Lo anterior, según lo establecido en la Ley 20.285, en el artículo 15 *"Cuando la información solicitada esté permanentemente a disposición del público, o lo esté en medios impresos tales como libros, compendios, folletos, archivos públicos de la Administración, así como también en formatos electrónicos disponibles en internet o en cualquier otro medio,*

se comunicará al solicitante la fuente, el lugar y la forma en que puede tener acceso a dicha información, con lo cual se entenderá que la Administración ha cumplido con su obligación de informar."

"...17 .- Procedimiento de fiscalización efectuado al municipio relativo a la gestión que hace de datos personales ante la Contraloría General de la República, Consejo para la Transparencia o Tribunales de Justicia." [sic], comunico a Ud. que, de acuerdo a lo informado por nuestra Dirección de Control, no se identifica la ejecución de fiscalizaciones sobre esta materia por parte de los Organismos mencionados.

"...En relación con la Gestión... de Educación, Cultura y Salud..." [sic], comunico a Ud. que, la Corporación de Desarrollo Social y la Fundación Cultural de Providencia son quienes poseen esta información. Por tanto, en virtud de lo establecido en el artículo 13 de la Ley Nº 20.285 "SOBRE ACCESO A LA INFORMACIÓN PÚBLICA", esta parte de su solicitud de información ha sido derivada a dichos organismos, a través de Oficios N°1391 y 1392 de fecha 04 de marzo de 2024 (se adjuntan copias).

Los datos de carácter personal concernientes a personas naturales han sido protegidos según lo dispuesto en la Ley Nº19.628, sobre protección de la vida privada.

Saluda atentamente a usted,

MUNICIPALIDAD DE PROVIDENCIA ADMINISTRADORA

CAROL VARGAS ROJAS
ADMINISTRADORA MUNICIPAL

MUNICIPALIDAD DE PROVIDENCIA DIRECCIÓN DE TECNOLOGÍA Y GESTIÓN DIGITAL DIRECTOR

DIRECTOR DE TECNOLOGÍA Y GESTIÓN DIGITAL (S)

ENCARGADO DE LA SEGURIDAD DE LA INFORMACIÓN

MFA

Distribución:
- Secretaría Municipal
- Depto. Transparencia
- Archivo Adm. Municipal

MUNICIPALIDAD DE PROVIDENCIA
SECRETARÍA MUNICIPAL
DEPARTAMENTO DE TRANSPARENCIA
RECEPCIÓN DOCUMENTOS
FECHA 04/03/2024
HORA 17:06

Providencia
Secretaría Municipal

PROVIDENCIA, 13 ABR. 2022

EX.N° 473 **/ VISTOS:** Lo dispuesto en los artículos 5 letra d), 12 y 63 letra i) de la Ley N°18.695, Orgánica Constitucional de Municipalidades; y

CONSIDERANDO: 1.- El Memorándum N°4.974 de 22 de Marzo de 2022, del Encargado de Seguridad de la Información.-

2.- El Memorándum N°5.503 de 29 de Marzo de 2022, de la Administradora Municipal.-

DECRETO:

Apruébase la versión 2.1 de la **POLITICA DE SEGURIDAD Y CONFIDENCIALIDAD DE LA INFORMACION,** cuyo texto se agrega al presente Decreto como Anexo I y se considera parte integrante de este Decreto.-

Anótese, comuníquese y archívese.-

Ilustre Municipalidad de Providencia
SECRETARIO ABOGADO MUNICIPAL

MARIA RAQUEL DE LA MAZA QUIJADA
Secretario Abogado Municipal

EVELYN MATTHEI FORNET
Alcaldesa

CVR/MRMQ/IMYJ/vpga.-
DISTRIBUCION:
Todas las Direcciones
Archivo
Decreto en Trámite N° 1073.-

soyprovidencia

DIRECCIÓN DE TECNOLOGÍA Y GESTIÓN DIGITAL

"Política de Seguridad y Confidencialidad de la Información"

Decreto EX N° 473 Fecha: 13 ABR. 2022

VERSIÓN	2.1
FECHA	24 DE FEBRERO DE 2022

1 Introducción

La masificación de tecnologías de información en todas las industrias y ámbitos del quehacer, junto con un crecimiento exponencial de los volúmenes de datos que se almacenan y transmiten, hacen imprescindible a todas las instituciones tomar los resguardos necesarios para asegurar la información y su adecuado uso. Así, la seguridad de la información y la protección de los datos personales constituyen uno de los mayores desafíos actuales. En tal grado es su importancia, que el año 2018 se consagró su cautela a nivel Constitucional, insertándolo en el artículo 19° numeral 4.

Esto adquiere especial relevancia cuando es un órgano público el que debe resguardar la información que recibe, almacena y produce, puesto que toda su actividad se despliega en beneficio de las personas y en aras del bien común.

Por consiguiente, reconociendo la trascendencia del tema y el imperativo constitucional, la Municipalidad de Providencia ha desarrollado la "Política de Seguridad y Confidencialidad de la Información" que aquí se presenta.

En esencia, se establecen lineamientos y principios; se definen roles y responsabilidades; se crea un Comité de Seguridad Permanente y se determina un Plan de Contingencia, entre otros.

Así, se instaura un instrumento fundamental con pautas claras, que permitirá a la Municipalidad tutelar de mejor forma los derechos de las personas, y continuar ciñéndose al marco normativo vigente.

2 Objetivo

Como ya se ha establecido previamente, el objetivo de esta política es propender a gestionar la seguridad de la información como un imperativo. Por ende, se deberá velar por su cumplimiento, como también por el cumplimiento de las políticas complementarias, normativas, reglamentos, procedimientos, manuales, instructivos, guías y otros documentos que emanen de ella, además de toda Ley relacionada a la materia de Seguridad y Confidencialidad de la Información, las buenas prácticas y normativas aplicables para este efecto.

En el entendido de que siempre existirán riesgos identificables, los cuales pueden ser eliminados o mitigados, la institución se compromete a gestionar la seguridad de la información, como un proceso continuo en el tiempo, tendiente a homogeneizar los criterios de seguridad y preservar sus activos de información, en cuanto a:

1. **Integridad**: La información estará correcta y sin grado de corrupción alguno.
2. **Confidencialidad**: La información reservada o secreta estará debidamente protegida, permitiendo el acceso solamente a las personas autorizadas.
3. **Disponibilidad**: La información estará disponible y accesible en forma oportuna cuando sea requerida por aquellas personas debidamente autorizadas.

Con el fin de establecer los niveles de seguridad y medidas adecuadas, se aplicarán continuamente las metodologías y técnicas estándares desarrolladas para estas materias, introduciendo un ciclo de mejora continua sostenible en el tiempo. En consecuencia, la PSI se actualizará permanente de acuerdo a los lineamientos de la Organización y su evolución, con al menos una actualización cada dos años desde el momento de su publicación.

3 Alcance

La política es aplicable a todos los activos de información de la Municipalidad que incluyen: procesos, sistemas, aplicaciones, software, equipamiento computacional y no computacional, instalaciones físicas, y adicionalmente aplicará a los funcionarios municipales, independiente de su condición contractual (planta, contrata, honorario, practicante u otro) y trabajadores de otras empresas que presenten servicios a las Municipalidad, siendo las jefaturas del Municipio responsables de propender el cumplimiento.

Esta política, incluirá los alcances de cumplimiento, tomando en consideración las recomendaciones normativas del DS N° 83 de 2004, Decreto Supremo que establece la norma técnica para los órganos de la Administración del Estado, sobre seguridad y confidencialidad de los documentos electrónicos; y además los señalados en el artículo 3°, inciso segundo de la Ley N° 19.880, sobre Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado.

4 Definición de Términos

Para efectos del presente documento, se entenderá por:

- **Activo de Información**: todo recurso y/o elemento relevante en la generación, distribución, visualización, almacenamiento y recuperación de información que tiene un valor sustancial para la Municipalidad de Providencia y, por lo tanto, debe protegerse. Se distinguen cuatro niveles:
  - La información propiamente tal, que puede ser estructurada, no estructurada y en múltiples formatos: impresa, escrita, digital, audio, video u otros.
  - Las instalaciones y equipos, computacionales o no, que la soportan.
  - Los procesos internos que generan y manipulan información.
  - Las personas que hacen uso o generan la información.
- **Riesgo**: la probabilidad de ocurrencia de un evento que produce algún nivel de daño. Se mide combinando la probabilidad de ocurrencia y su impacto.
- **Amenaza**: Acción de personas o programas que constituyen una posible causa de riesgo o perjuicio para los sistemas de información, sean físicos o digitales.
- **Vulnerabilidad**: debilidad de un activo o grupo de ellos, que podría permitir materializar una o más amenazas.
- **Seguridad de la Información**: conjunto de medidas que adopta una Organización para resguardar y proteger la información buscando mantener la confidencialidad, disponibilidad e integridad de datos. No debe confundirse con seguridad informática, cuyo alcance se limita a los sistemas tecnológicos.
- **Contramedida**: representa todas las acciones que se implementan para prevenir la amenaza.
- **TI**: Tecnologías de la Información

5 Descripción

5.1 Declaración de la Organización

La Municipalidad de Providencia (en adelante "la Municipalidad"), mantendrá una Política de Seguridad de la Información (en adelante, "PSI") que aúne todos los esfuerzos institucionales en tal sentido, con el fin de disminuir riesgos y evitar incidentes que pudieran traducirse en pérdidas de información, económicas y de imagen para la Municipalidad, así como infracciones regulatorias o vulneraciones de derechos y perjuicios a los ciudadanos. Esta política sustentará los siguientes principios:

- Asegurar prácticas tendientes a cautelar la integridad, confiabilidad y disponibilidad de la información administrada en todos los ámbitos de gestión municipal, propendiendo así a mantener la continuidad de los servicios que entrega la Institución.
- Mantener políticas, normativas y procedimientos de seguridad de información actualizados.
- Comprometer e involucrar a todo el personal municipal de la Municipalidad y sus proveedores, a la correcta difusión, implementación y cumplimiento de esta política.
- Promover una cultura organizacional orientada a la seguridad de la información.

5.2 Seguridad de activos de información

Los activos de información deben tener un dueño (Ver punto 6.4, letra (a)) responsable de identificar, registrar, clasificar y valorizar el activo, según su impacto en los objetivos municipales. Esta información será vital para la implementación del Plan de continuidad Operacional. Asimismo, debe definir los roles que pueden acceder al activo y sus niveles de autorización sobre el mismo.

Para aquellos activos considerados de alta criticidad, se debe mantener un análisis periódico de las amenazas y/o vulnerabilidades que puedan aparecer, así como la evaluación del riesgo y gestionar la mitigación o eliminación de los mismos.

Las gestiones que se deben realizar sobre los activos de información son:

1. **Inventario de los Activos**. Debe existir un registro general de todos los activos asociados a la información institucional, los que deben ser revisados y actualizados en forma periódica por quien corresponda, de acuerdo a la reglamentación vigente en la Municipalidad.
2. **Clasificación de la Información**. La información debe ser clasificada y etiquetada de acuerdo a su valor, requisitos legales y grado crítico para la Municipalidad.
3. **Generar y administrar los Protocolos**, como acciones conducentes a optimizar y actualizar las tareas cotidianas.

5.2.1 Riesgos y vulnerabilidades

Algunos de los riesgos y vulnerabilidades más comunes, y que deben ser gestionados por los responsables respectivos, son los siguientes:

- **Asociados a Sistemas tecnológicos**:
  - Cambios no controlados en el sistema
  - Adulteración de los registros del sistema, modificación no autorizada
  - Adulteración de los registros de actividades del operador y del administrador del sistema
  - Sistema de información y/o infraestructura TI vulnerable
  - Desarrollo inseguro de sistemas

- Incorrecta actualización o versionamiento de los sistemas
- Uso desprotegido de datos sensibles en pruebas.
- Acceso no autorizado.

- **Asociados a información digital o en soporte de papel**:
  - Manipulación indebida de información
  - Acceso no autorizado a la información
  - Pérdida, daño o deterioro del medio de Información
- **Asociados a personas**:
  - Fuga de información confidencial, por error o desconocimiento
  - Incorrecta asignación de funciones, lo que podría causar un mal uso de la información a su cargo
  - Conocimiento insuficiente de las responsabilidades y correcto uso de los activos de información a cargo
  - Capacitación insuficiente en seguridad de la información
  - Transgresión a las políticas de seguridad de la información por parte del funcionario
  - Acceso no autorizado a activos de información de personas desvinculadas de la institución. Robo de equipos, medios y/o documentos.
  - No devolución de dispositivos y/o activos de información a la institución una vez terminada la relación laboral
  - Uso de contraseñas inseguras y fáciles de deducir
- **Asociados a Equipos tecnológicos**
  - Daño por amenazas ambientales. Acceso no autorizado
  - Robo, daño o pérdida del equipo fuera de las dependencias de la institución
  - Eliminación insegura de la información contenida en el equipo
  - Contaminación con malwares
  - Instalación no autorizada de Software

5.2.2 Cuidado de la información confidencial

Respecto de los cuidados generales de protección de datos y de la información, y que aplican tanto a la información existente en formato digital como también en soporte de papel, las definiciones serán las siguientes:

1. La información de la Municipalidad debe ser protegida con controles acordes a la categoría de clasificación asignada de acuerdo a su nivel de confidencialidad, independientemente del medio en que se almacene o transporte. Esto se aplicará a todas las acciones y medios de almacenamiento y transporte de información confidencial.
2. Los documentos confidenciales deben ser protegidos de cualquier tipo de lectura casual, por ende, si son documentos físicos deben quedar almacenados en muebles con llave; los funcionarios que porten estos documentos confidenciales fuera de la oficina deben maximizar el cuidado para no extraviarlos o exponer su contenido.
3. La información confidencial enviada por correo interno o externo, debe ir en sobre sellado y con la frase "Sólo para ser abierto por el Destinatario".
4. El servicio de correo utilizado debe permitir el rastreo de la carta o paquete.
5. El método de distribución de información confidencial, o de uso interno, debe permitir que exista un acuse de recibo formal, por parte del destinatario.
6. Previo a enviar a un tercero un documento confidencial, o de uso interno, el emisor y el receptor deben firmar un Acuerdo de No-Divulgación de Información.
7. La Municipalidad protege la información confidencial que ha sido confiada por terceros. Los funcionarios tienen la obligación de no divulgar dicha información, a menos que el originador entregue una autorización por escrito, o exista un requerimiento legal.
8. Se debe evitar la discusión de información confidencial o privada por vía telefónica pública. Si se hace, se debe procurar tratar los temas en forma general y sin mencionar datos confidenciales.
9. No se debe discutir información confidencial o privada usando el altavoz del aparato telefónico o usando teléfonos inalámbricos o celulares.

10. Si los funcionarios de la Municipalidad viajan en transporte público colectivo, no deben llevar consigo información confidencial municipal. En caso de que esto sea estrictamente necesario, la Municipalidad proveerá un medio de transporte seguro.
11. La información confidencial no debe ser expuesta, leída o discutida en aviones, restaurantes, transporte colectivo u otros sitios públicos.
12. Todos los funcionarios que porten información confidencial en dispositivos portátiles, deben almacenarla cifrada, proteger el acceso lógico a la información o proteger el acceso físico al dispositivo.
13. Si se viaja en bus o avión, el dispositivo portátil debe ir como equipaje de mano, siempre bajo la supervisión del usuario, y no en el compartimiento de equipaje.
14. Cuando una empresa externa, un consultor o contratista se desvincula de la Municipalidad, no puede llevar consigo la información confidencial, o de uso interno a la cual ha tenido acceso.
15. Cuando un funcionario se desvincula de la Municipalidad, no debe llevar consigo información confidencial o de uso interno de la institución.
16. La divulgación voluntaria o involuntaria de información confidencial de la Municipalidad, o que atente contra la Ley de Protección de Datos Personales podría llevar a acciones disciplinarias y/o la respectiva denuncia a la autoridad competente.

5.2.3 Seguridad en el acceso a la información digital

Los detalles operativos tocantes al acceso a información en formato digital, se encuentran en la "Política de Control de Acceso, Identificación y Autenticación (N02)", la cual se sujeta específicamente al DS N°83 del año 2004 del Ministerio Secretaría General de la Presidencia, en su artículo N°28.

No obstante, en forma adicional a lo indicado en dicho documento, deberán implementarse mecanismos de bloqueo automático en las estaciones de trabajo que están desatendidas por un plazo prudente que evite o minimice la acción de un tercero. Asimismo, los usuarios serán responsables de mantener sus zonas de trabajo limpias, evitando que terceros puedan acceder a información confidencial.

Para las personas que utilicen teléfonos celulares entregados por la Municipalidad o configuren sus propios equipos con cuentas de la Municipalidad, deberán adherir a las políticas de seguridad acá establecidas y la "Política de uso de equipos y medios portátiles (N05)".

5.3 Seguridad de la Infraestructura informática

Para servicios de terceros que manejan activos de información será obligatorio contar con acuerdos de confidencialidad, niveles de servicio y disponibilidad comprometidos, asimismo su monitoreo y revisión permanente por parte de la Municipalidad. Además de lo anterior, todo proveedor de tecnología y/o transporte de equipamiento, debe conocer y cumplir con estas políticas de seguridad de la información en su totalidad, debiendo justificar sólidamente cualquier excepción necesaria a través de medios formales al encargado de seguridad tecnológica de la Municipalidad.

Para garantizar un óptimo cumplimiento de las políticas de seguridad, se definirán los siguientes instructivos complementarios, que permitirán clarificar a los usuarios lo que se entiende como conductas adecuadas o inadecuadas, así como sus niveles de responsabilidad personal en el no cumplimiento u omisión.

1. N01 - Uso de Infraestructura informática.
2. N02 - Control de acceso, identificación y autenticación.
3. N03 - Utilización de correo electrónico.
4. N04 - Utilización del servicio de internet.
5. N05 - Política de uso aceptable de equipos y/o medios portátiles asignados por la Municipalidad.
6. N06 - Utilización de Accesos Remotos para teletrabajo (VPN).
7. N07 - Uso de Recursos Compartidos.

El cumplimiento de estas políticas de seguridad requiere que se sigan protocolos formales de operación. Estos protocolos deben ser estructurados y descritos en detalle en procedimientos operativos.

Los procedimientos operativos deben estar documentados, actualizados y ser conocidos por los involucrados. Las responsabilidades deben estar individualizadas y con una adecuada segregación de funciones que impida cambios no autorizados o hacer mal uso de los activos de información.

Los procedimientos operativos serán los siguientes:

1. P01 - Creación de usuarios.
2. P02 - Eliminación o inactivación de usuarios.
3. P03 - Solicitud de instalación de software adicional al estándar.
4. P04 - Atención de usuarios.
5. P05 - Acceso al o los sistemas de información y/o gestión documental.
6. P06 - Traslado de información de usuarios.
7. P07 - Respaldo de información de usuarios.
8. P08 - Creación de accesos VPN para teletrabajo.

Además, deberán existir adecuados controles para hacer cambios en los sistemas y plataformas tecnológicas que impidan modificaciones no autorizadas o erróneas, que afecten la integridad de la información. Para ello deben existir los siguientes procedimientos:

9. P09 - Paso a producción y/o Control de Cambios.
10. P10 - Mantención de sistemas aplicativos y/o infraestructura. (Incluído en P09)
11. P11 - Creación de reglas en Firewall, Switches, Servidores Web y otros.

Y para los activos tecnológicos y sus movimientos:

12. P12 - Incorporación, desvinculación, traslado y baja de Activos Tecnológicos.

En la constante implementación de mejoras, el Comité de Seguridad puede aprobar nuevas políticas complementarias y/o procedimientos operativos, los cuales serán debidamente difundidas y publicadas para su cumplimiento.

5.3.1 Adquisición, desarrollo y mantenimiento de sistemas TI

1. Todo nuevo sistema de información deberá contar con controles de seguridad que eviten acceso no autorizado, pérdida o corrupción de información según la "Política de Control de Acceso, Identificación y Autenticación (N02)".
2. La información sensible debe disponer de controles criptográficos, siempre que tecnológica y operativamente sea posible. Las excepciones deben ser debidamente informadas al Comité de Seguridad a través del Encargado de Seguridad de la Información.
3. Los datos de prueba deben ser cuidadosamente tratados y en lo posible enmascarados para evitar acceso de terceros a datos reales que se encuentran en producción.
4. Los programas fuentes que dan origen a los sistemas deben contar con mecanismos robustos de protección y resguardo que impidan su pérdida, daño o copia no autorizada.
5. Los sistemas y plataformas periódicamente deben ser sometidos a pruebas de vulnerabilidades que permitan revelarlas y ejecutar planes de acción para mitigarlas. Cualquier prueba de explotación de vulnerabilidades debe ser supervisada y autorizada por el encargado de seguridad de la información e informada al Comité de Seguridad de la Municipalidad especificando los riesgos y el alcance posible de éstos. La realización de pruebas de explotación de vulnerabilidades o escaneo de las redes sin autorización podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N°18.883,

sobre estatuto administrativo municipal. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

5.4 Gestión de incidentes de seguridad

Los eventos e incidentes de seguridad detectados, deberán ser registrados y comunicados a los responsables para su atención y resolución en el menor plazo posible. Asimismo, las debilidades y vulnerabilidades conocidas en los sistemas y plataformas, deberán ser informadas al Encargado de Seguridad y dueño de información que pudiera ser afectado.

Deberán existir procedimientos conocidos para la detección, atención y resolución de los eventos e incidentes de seguridad junto con un mecanismo que permita recopilar información relacionada para los análisis y mejoras respectivas.

5.4.1 Planes de contingencia.

Las medidas del plan de contingencia están sujetas al estatuto administrativo de la Municipalidad de Providencia y, por ende, las medidas o sanciones en caso de incidente, serán decididas según el Estatuto vigente.

El plan de contingencia se llevará a cabo según los siguientes pasos:

1. **Reporte de eventos de seguridad**: Cualquiera sea el incidente ocurrido que infrinja la política o se considere una falla de infraestructura, debe ser reportado inmediatamente al Encargado de Seguridad de la Información a través del formulario dispuesto para estas situaciones en la intranet municipal y/o el correo institucional dedicado a recolectar estos reportes. Posteriormente, el caso será discutido con la Comisión para tomar las medidas pertinentes. El encargado de Seguridad deberá reportar los antecedentes recopilados a la Dirección responsable para la gestión correctiva necesaria.
2. **Recopilación de evidencia**: En el caso de que el incidente ocurra en un sistema informático, la Dirección de Tecnología y Gestión Digital debe poner en marcha los procedimientos necesarios para poder revisar las acciones realizadas en el sistema vulnerado, con el fin de recopilar información necesaria para ser usada como evidencia del incidente.
3. **Documentar Eventos de Seguridad**. De acuerdo a la información entregada por quien denuncie y la evidencia recopilada, se procede a tomar una decisión por parte del comité respecto al procedimiento que se debe seguir, la cual será determinada por simple mayoría. Luego de lo anterior, se debe registrar formalmente lo ocurrido, incluyendo todos los antecedentes reunidos y la decisión final, a través del formulario correspondiente.
4. **Pruebas de Vulnerabilidades**. En caso de que el incidente involucre sistemas informáticos, se deberá realizar por parte de la Dirección de Tecnología y Gestión Digital, los procedimientos necesarios para evaluar la vulnerabilidad y desarrollar un protocolo en caso de ser necesario.
5. **Generar y administrar los Protocolos**: En relación al incidente ocurrido, se deben revisar los protocolos existentes y actualizarlos para evitar una recurrencia de este tipo de incidentes o crear un procedimiento, en caso de que no exista actualmente.
6. **Caso de pérdida de información**: En caso que el incidente genere pérdidas de cualquier tipo de información, se debe comunicar inmediatamente a los directores de la Municipalidad de Providencia, al (a la) alcalde(sa) en ejercicio, y a cualquier persona a la cual dicha falla pueda afectar directamente.

5.5 Gestión de la continuidad de negocio

Una vez al año se deberán mantener y evaluar los planes de continuidad de negocio y de recuperación de desastres que permitan restaurar la continuidad y disponibilidad de los activos de información considerados críticos. Junto con lo anterior, evaluar anualmente sus riesgos. Esto es exigible a proveedores de plataformas y sistemas de misión crítica para la Municipalidad.

5.6 Gestión del cumplimiento normativo

La PSI, adhiere al marco normativo que regulan las leyes chilenas en esta materia y todas las disposiciones legales relativas al manejo y resguardo de datos personales, persistencia en el tiempo de ciertos datos que indique la normativa, documentos electrónicos, firma digital y propiedad intelectual.

La Municipalidad deberá realizar auditorías periódicas y selectivas, a cualquiera de sus activos de información y cooperar activamente con los organismos estatales pertinentes en cuanto a auditorías externas se oficialicen. Sin perjuicio de lo anterior, la Municipalidad tomará los resguardos necesarios para evitar que la información pueda ser expuesta a un mal uso o se genere interrupción en los sistemas y procesos de negocio.

En el caso de los funcionarios que trabajen con información sensible o tengan acceso a ella, es necesario crear cláusulas de confidencialidad en los contratos, ya que podrían hacer mal uso de la información, de manera voluntaria o involuntaria.

6 Responsabilidades

6.1 Encargado de Seguridad de la Información

Se define al Encargado de Seguridad de la Información, como el funcionario municipal responsable de mantener actualizada la PSI, monitorear su aplicación, promover su difusión y proponer mejoras.

6.2 Comité de Seguridad de la Información

Se define un Comité de Seguridad de la Información (desde ahora, "Comité"), que será una instancia permanente conformada por un titular y su respectivo suplente:

a) Encargado/a de Seguridad de la Información.
b) Administrador/a Municipal o quien éste/a designe como suplente.
c) Director/a de Control o quien éste/a designe como suplente.
d) Director/a de Tecnología y Gestión Digital o quien éste/a designe como suplente.
e) Director/a de Jurídica o quien éste/a designe como suplente.

Las responsabilidades del Comité serán:

a) Aprobar las Políticas de Seguridad de la información, velar por su cumplimiento, difusión y mejoras.
b) Pronunciarse y aprobar todas las resoluciones en aspectos de Seguridad, que sean de alcance estratégico y transversal a la Municipalidad.

El Comité se reunirá regularmente en forma trimestral para revisar el funcionamiento general de la PSI, analizar posibles incidentes del período y revisar otras materias relativas a la Seguridad de la Información, según necesidad.

Deberá existir un suplente para cada uno de los miembros integrantes del Comité, que lo reemplazará en sus funciones con derecho a voz y voto para aquellos casos en que el titular se encuentre impedido de participar en alguna reunión. Los suplentes podrán asistir a las reuniones, conjuntamente con su respectivo titular, pero en este caso, sólo tendrán derecho a voz. Esta designación deberá constar en acta de sesión.

En caso que ocurra algún incidente en relación a la información, el Encargado de Seguridad debe gestionar las medidas de mitigación necesarias y luego informar de lo acontecido a los miembros de Comité, pudiendo para ello, de ser necesario, citar a sesión extraordinaria, de tal forma que se pueda tomar decisiones tendientes a evitar eventos futuros de la misma naturaleza.

6.3 Responsabilidades del Encargado de Seguridad

Sin perjuicio de lo ya indicado en secciones anteriores, las responsabilidades del Encargado de Seguridad serán las siguientes:

a) Definir los controles necesarios para revisar el cumplimiento de la PSI.
b) Revisar y mantener actualizada la PSI, según los requerimientos de la municipalidad.
c) Velar por la implementación de los procesos y procedimientos de seguridad.
d) Monitorear el cumplimiento de los procedimientos establecidos.
e) Generar capacitaciones para los funcionarios municipales en temas relativos a Seguridad de Información.
f) Asesorar a la alcaldesa de la Municipalidad en las materias relativas a seguridad de los documentos electrónicos.
g) Coordinar la respuesta ante incidentes de seguridad de la información, manteniendo un registro actualizado de éstos.
h) Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.
i) Mantener un inventario actualizado de los Activos de Información, en conjunto con los dueños de la información.
j) Proponer mejoras al Comité, organizar periódicamente sus sesiones y dar seguimiento a los planes de acción que se deriven.
k) Actuar como secretario en las sesiones de Comité y tomar nota de acuerdos y temas relevantes, generando las actas respectivas y posteriormente enviarlas a cada integrante para su aprobación.

6.4 Responsabilidades generales de funcionarios y proveedores

Se definen los siguientes roles respecto de los activos de información:

a) **Dueño de la información**: persona responsable de un activo de información (o grupo), que incluye su valorización, clasificación y definiciones en torno a la protección, autorización y uso de la información.
b) **Administrador de la información**: persona encargada de resguardar la información y administrar las definiciones establecidas por el dueño de la información.
c) **Usuario de la información**: persona que tiene acceso a la información según los niveles de autorización definidos por el dueño de la información.

Todos los funcionarios de la Municipalidad deberán cooperar, contribuir y cumplir permanentemente con la PSI, así como denunciar las infracciones bajo los canales municipales establecidos. También es deber de cada funcionario municipal, preocuparse

de conocer y comprender el contenido de todas las disposiciones que en materia de Seguridad de la Información se oficialicen por parte de la Municipalidad.

Respecto del personal externo que presta servicios a la Municipalidad, se le dará a conocer y se hará exigible el cumplimiento de la PSI, en lo que sea atingente a sus labores, incluyendo en todos los contratos cláusulas para asegurar el cumplimiento.

Todos los funcionarios municipales que manipulen o accedan a activos de información de la Municipalidad deben firmar acuerdo de confidencialidad y responsabilidad en el uso de la información. Así mismo se debe mantener un programa de difusión y capacitación permanente a los funcionarios en los temas de Seguridad de la Información.

El incumplimiento de las Políticas de Seguridad de la Información por parte de los funcionarios, dará lugar a la aplicación de medidas administrativas, disciplinarias, civiles o penales a las que haya lugar.

Los funcionarios que cambien de funciones o asuman nuevos roles o cargos, deberán ser actualizados en cuanto al acceso y autorización a los activos de información según sus nuevas funciones. En caso de ausencias prolongadas de los funcionarios, deberán ser suspendidos en sus accesos a los activos de información. Por último, los funcionarios que cesen sus contratos con la Municipalidad deberán ser revocados en todos sus accesos a los activos de información según los procedimientos implementados para dichos propósitos.

6.5 Roles y responsabilidades específicos

Por último, se detallan las siguientes responsabilidades específicas, con el propósito de cumplir los objetivos de la PSI:

6.5.1 Dirección de Tecnología y Gestión Digital

a) Velar por el cumplimiento de esta política y los 3 principios mencionados en el inicio: integridad, Confidencialidad y Disponibilidad. (Ver punto V, inciso 1)
b) Responder a los avisos de incorporación o desvinculación de funcionarios de la Municipalidad de Providencia, para mantener actualizados accesos y permisos a los sistemas.
c) Proporcionar y recibir información respecto a los activos de información, con el fin de mantener el inventario de activos actualizado.
d) Mantener actualizado el registro de permisos de accesos a cada sistema de información.

6.5.2 Directivos

a) Velar por el cumplimiento de los puntos indicados en la presente política según sus atribuciones y facultades.
b) Promover un ambiente de buenas prácticas con respecto a sistemas de la información en sus áreas.
c) Concientizar a los trabajadores respeto de sus responsabilidades, en materias de seguridad de la información.
d) Orientar a los funcionarios al cumplimiento de la PSI.
e) Informar al encargado de seguridad de la información sobre las Bases de Datos de sus respectivas direcciones y jefaturas, avisando si estas incluyen o no información sensible.
f) Mantener actualizada la información de sus bases de datos.
g) Administrar el uso de los Sistemas de Información relacionados con su negocio.
h) Autorizar o Denegar los permisos a las Bases de Datos de sus respectivas unidades, informando a la Dirección de Tecnología y Gestión Digital cuando sea necesario.

6.5.3 Dirección de Personas y DIDECO

Además de lo contemplado en el punto 6.5.2 del presente documento, es responsabilidad de las Direcciones de Personas y de Desarrollo Comunitario (DIDECO) notificar de forma consolidada y oportuna a la Dirección de Tecnología y Gestión Digital, sobre las vinculaciones y desvinculaciones del personal de cada área de la Municipalidad integrando esta actividad como parte importante de sus procedimientos de operación.

6.5.4 Usuarios de sistemas de información

Todos los funcionarios usuarios de Sistemas de Información Municipales, ya sean de planta, contrata u honorarios, estarán afectos a lo establecido en esta política debiendo asegurar su estricto cumplimiento. Además, los usuarios deben velar por el cumplimiento de los tres principios mencionados al inicio de la política: Integridad, Confidencialidad y Disponibilidad, alertando de manera oportuna y adecuada, cualquier incidente que atente contra la seguridad de la información.

7 Normativa Legal y Reglamentaria

El marco normativo sobre el cual descansa la presente política está compuesto por las siguientes leyes, decretos e instrucciones:

- Ley Nº 19.628 sobre protección de la vida privada.
- Ley Nº19.553 que concede asignación de modernización y otros beneficios que indica.
- Ley Nº 19.799 sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma.
- Ley Nº 20.285 sobre acceso a la información pública.
- Ley Nº 19.223 tipifica figuras penales relativas a la informática.
- Ley Nº 19.880 establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.
- Ley Nº 21.096, consagra el derecho a protección de los datos personales.
- Decreto Supremo Nº 83 de 2005, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
- Decreto Supremo Nº 93 de 2006, norma técnica para la adopción de medidas destinadas a minimizar los efectos perjudiciales de los mensajes electrónicos masivos no solicitados recibidos en las casillas electrónicas de los órganos de la administración del estado y de sus funcionarios.
- Decreto Supremo Nº181 Aprueba reglamento de Ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma.
- Decreto Supremo Nº 14 de 2014 modifica decreto Nº 181, de 2002, que aprueba reglamento de la ley 19. 799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma, y deroga los decretos que indica.
- Decreto Supremo Nº158 de 2007. Modifica D.S. Nº 81 sobre norma técnica para la interoperabilidad de los documentos electrónicos.
- Instrucción General Nº2, mayo de 2009, del Consejo para la Transparencia: Designación de Enlaces con el Consejo para la Transparencia.
- Instrucción General Nº3, mayo de 2009, del Consejo para la Transparencia: Índice de Actos o Documentos calificados como secretos o reservados.

8 Difusión y Revisión

La difusión de esta política, se realizará mediante correo electrónico a todo el personal de la Municipalidad y terceros relacionados directamente, además quedará a disposición en el sitio Web de la Municipalidad para facilitar el acceso y su conocimiento. Junto a lo anterior, se realizarán capacitaciones a las personas que sean contratadas por la municipalidad.

La revisión se realizará durante las reuniones del Comité de Seguridad de la Información, sin embargo, en el caso de circunstancias excepcionales, la política podrá ser revisada y modificada con la aprobación del Comité.

9 Historial de Cambios

Versión	Fecha	Cambio	Responsable / Dirección
0	25-Oct-2018	- Creación del Documento	Felipe Frez / Administración Municipal.
1.0	25-May-2019	- Modificaciones menores.	Felipe Frez / Administración Municipal
2.0	24-Feb-2021	- Incorpora mayor detalle en políticas de seguridad, roles y responsabilidades. - Reestructuración general del documento	Juan Carlos Lillo M. / Dirección de Tecnología y Gestión Digital.
2.1	24-Feb-2022	- Cambio de estructura que se solicita en el Decreto EX N°1 sin fecha del año 2021 de la Dirección de Control	Juan Carlos Lillo M. / Dirección de Tecnología y Gestión Digital.

soyprovidencia

DIRECCIÓN TECNOLOGÍA Y GESTIÓN DIGITAL
DEPARTAMENTO GESTION TI

PROVIDENCIA, 31 MAR 2022

EX. D.T.G.D. N° 70 /

VISTOS: las facultades otorgadas en los artículos 5° letra d), 12° y 63° letra i) letra j) de la Ley Orgánica Constitucional de Municipalidades; y lo dispuesto en el artículo N°36 del Decreto Alcaldicio EX N°79 de fecha 1 febrero de 2021, que fijo el texto refundido y sistematizado del Reglamento sobre "DELEGACION DE FACULTADES DEL ALCALDE" y lo dispuesto en el Decreto EX Dirección de Control N°1 de fecha 1 de octubre de 2021.

CONSIDERANDO:

1.- Decreto EX Control N°1 sin fecha que aprueba el Procedimiento "Elaboración de documentos de gestión de la Municipalidad de Providencia"

2.- La necesidad de uniformar y estandarizar la metodología y contenidos para la elaboración de documentos operacionales o de gestión, como los manuales, procedimientos, instructivos y protocolos, esta Dirección de Tecnología y Gestión Digital, ha definido el siguiente instructivo para la confección de documentos de gestión.

3.- El presente Instructivo, establece el resguardo de la información en custodia de la Municipalidad bajo medios físicos y digitales, por lo cual el acceso a los sistemas municipales será otorgado a usuarios identificados y autentificados. La Municipalidad establecerá los procedimientos y controles para otorgar, cambiar y finalizar accesos a los sistemas de información.

DECRETO:

1.- Apruébese a contar de esta fecha el **"INSTRUCTIVO CONTROL DE ACCESO, IDENTIFICACION Y AUTENTIFICACION"** versión 1.1 de fecha 24 febrero de 2022, el que se adjunta al presente decreto.

2.- Publíquese el presente Decreto, en el Sistema de Documental Municipal en **CLASE: Decreto EX DTGD -SUBCLASE: Instructivos - GRUPO: Documento de Gestión.**

MUNICIPALIDAD DE PROVIDENCIA * DIRECTOR *

JUAN PABLO MUÑOZ GALLARDO
DIRECCION TECNOLOGIA Y GESTION DIGITAL

MUNICIPALIDAD DE PROVIDENCIA * CONTRALOR * DIRECCIÓN

V°B° CONTROL

CGV/agg

soyprovidencia

Instructivo

"Control de Acceso, Identificación y Autenticación"

Decreto EX DTGD N°

Fecha:

Juan Carlos Lillo Molina
Encargado de Seguridad de la Información

Juan Pablo Muñoz Gallardo
Director Tecnología y Gestión Digital

VERSIÓN	1.1
FECHA	24 DE FEBRERO DE 2022

1. Objetivo.

El objetivo de este documento es resguardar la información en custodia de la Municipalidad bajo medios físicos y digitales. Ésta es una de las labores más importantes a realizar, por lo cual el acceso a la información de los sistemas de la Municipalidad de Providencia será sólo otorgado a usuarios identificados y autentificados. La Municipalidad de Providencia establecerá los procedimientos y controles para otorgar, cambiar y finalizar accesos a los sistemas de información.

El uso inapropiado de los recursos dispuestos para los usuarios, expone a la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, filtración de información, como también problemas jurídicos tanto nacionales como internacionales.

2. Alcance

Aplica a todos los funcionarios y proveedores que estén vinculados con la Municipalidad. Se incluye, además, todas las dependencias que son parte de la institución o que utilicen las redes del municipio.

3. Descripción

a. Perfiles de usuarios y privilegios de acceso

i. Todos los sistemas municipales deben soportar la especificación de perfiles de usuarios. Dichos perfiles deben incluir un conjunto de privilegios de acceso a la información, de tal forma que facilite la administración de usuarios según las labores contractuales que le sean encomendadas sobre los sistemas de información.

ii. Los privilegios definidos sobre la información deben ser referidos a las acciones de leer, escribir y modificar datos.

iii. Un perfil de usuario debe ser definido según la labor que se realizará sobre los sistemas de información municipal. De esta forma, las acciones que puede realizar un perfil implicará un conjunto de privilegios sobre la información de manera segregada, es decir, para cierto tipo de información, el perfil definirá las acciones de lectura, escritura y/o modificación, según sea el caso.

iv. Para la creación de cuentas de usuario sobre los sistemas de información, es obligatorio definir el perfil de usuario que se asignará.

b. Identificación y autentificación

i. Cada sistema debe incorporar la autenticación de usuario y la identificación para garantizar que el acceso no se concederá a personas no autorizadas. Los usuarios no tendrán el acceso a los recursos de información de la Municipalidad sin identificarse y autenticarse en ellos.

ii. Todas las cuentas deben tener contraseñas fuertes u otros métodos alternativos de autenticación robusta. Usar contraseñas con caracteres en minúscula, mayúsculas, números y símbolos y de ser posible, palabras que no tengan significado y con una longitud de más de ocho caracteres. Ejemplo de una

contraseña fuerte podría ser "Sfr628$uR34!&" así como diferentes combinaciones del ese estilo.

iii. Desarrollar y seguir procedimientos detallados para la creación, eliminación, y modificación de las cuentas de usuario y credenciales de autenticación para todo sistema que se use en la Municipalidad.

iv. Las cuentas de usuario deben cumplir con las siguientes directrices:

a. Permitir sólo un usuario por cada cuenta. Los identificadores de usuario no deben ser compartidos. (Nombre de usuario, ID's). En el caso que por fuerza mayor se utilice algún tipo de usuario genérico, éste debe ser monitoreado y controlado permanentemente por el área de infraestructura tecnológica del municipio.

b. Nunca se debe activar/habilitar una cuenta de invitado a menos que sea estrictamente necesario (Ver letra a). Eliminar todas las cuentas que son creadas de forma predeterminada por el sistema, a menos que sea absolutamente necesario y aprobado por el administrador de los sistemas.

c. No utilizar cuentas predefinidas fáciles de predecir, tales como:

- Anónimo
- Invitado
- Admin
- FTP
- Telnet
- Usuario
- Test
- Otros por defecto

v. Las cuentas que están presentes por defecto en la instalación inicial del sistema, se deberán eliminar o cambiar de nombre a menos que sea técnicamente requerida por el sistema, debiendo dar aviso para tomar el resguardo necesario.

vi. Para las labores específicas que requieran cuentas de acceso (ya sea para algún funcionario o contratista), se deberán desactivar inmediatamente después del término de su utilización. La jefatura o funcionario responsable de dichas labores debe informar del inicio y del término de las actividades para que la Dirección de Tecnología y Gestión Digital coordine las activaciones e inhabilitaciones adecuadas.

vii. Las cuentas deben ser desactivadas inmediatamente después del término de una labor específica que sea ejecutada por un empleado o contratista.

viii. Las cuentas no utilizadas serán desactivadas. Para esto se generará una calendarización, que se ejecute al menos una vez al mes.

ix. Las cuentas de administrador (Usuario con facultades de generar cambios de configuración en equipos y/o sistemas informáticos) deben cumplir con las siguientes directrices:

1. Objetivo.

El objetivo de este documento es resguardar la información en custodia de la Municipalidad bajo medios físicos y digitales. Ésta es una de las labores más importantes a realizar, por lo cual el acceso a la información de los sistemas de la Municipalidad de Providencia será sólo otorgado a usuarios identificados y autentificados. La Municipalidad de Providencia establecerá los procedimientos y controles para otorgar, cambiar y finalizar accesos a los sistemas de información.

El uso inapropiado de los recursos dispuestos para los usuarios, expone a la institución a riesgos innecesarios como los virus informáticos, interrupción de las redes y sus sistemas, filtración de información, como también problemas jurídicos tanto nacionales como internacionales.

2. Alcance

Aplica a todos los funcionarios y proveedores que estén vinculados con la Municipalidad. Se incluye, además, todas las dependencias que son parte de la institución o que utilicen las redes del municipio.

3. Descripción

a. Perfiles de usuarios y privilegios de acceso

i. Todos los sistemas municipales deben soportar la especificación de perfiles de usuarios. Dichos perfiles deben incluir un conjunto de privilegios de acceso a la información, de tal forma que facilite la administración de usuarios según las labores contractuales que le sean encomendadas sobre los sistemas de información.

ii. Los privilegios definidos sobre la información deben ser referidos a las acciones de leer, escribir y modificar datos.

iii. Un perfil de usuario debe ser definido según la labor que se realizará sobre los sistemas de información municipal. De esta forma, las acciones que puede realizar un perfil implicará un conjunto de privilegios sobre la información de manera segregada, es decir, para cierto tipo de información, el perfil definirá las acciones de lectura, escritura y/o modificación, según sea el caso.

iv. Para la creación de cuentas de usuario sobre los sistemas de información, es obligatorio definir el perfil de usuario que se asignará.

b. Identificación y autentificación

i. Cada sistema debe incorporar la autenticación de usuario y la identificación para garantizar que el acceso no se concederá a personas no autorizadas. Los usuarios no tendrán el acceso a los recursos de información de la Municipalidad sin identificarse y autenticarse en ellos.

ii. Todas las cuentas deben tener contraseñas fuertes u otros métodos alternativos de autenticación robusta. Usar contraseñas con caracteres en minúscula, mayúsculas, números y símbolos y de ser posible, palabras que no tengan significado y con una longitud de más de ocho caracteres. Ejemplo de una

a. Los nombres de las cuentas de administración deben ser cambiadas al menos una vez al año, o una frecuencia que no dificulte la administración de los sistemas.

b. Cada persona que tiene una necesidad legítima de usar los privilegios de administración, debe tener su propia cuenta administrativa que se utilizará para llevar a cabo funciones. El uso de la cuenta de administrador principal para cada uno de los sistemas debe delimitarse a un grupo limitado de usuarios y a situaciones de emergencia. Esto protegerá a la cuenta de administrador principal, proporcionando una pista de auditoría de las actividades administrativas.

d. Otros métodos de autenticación de contraseñas distintas de claves alfanuméricas (por ejemplo, sistemas biométricos, tarjetas inteligentes, tokens, otros), deben ser aprobados por el Dirección de Tecnología y Gestión Digital de la Municipalidad.

Para evitar ataques del tipo "fuerza bruta" (programa que prueba distintas combinaciones de letras hasta que encuentre una válida), una función de bloqueo de intrusos debe ser implementado en cada sistema, suspendiendo temporalmente la cuenta después de tres intentos de inicio de sesión no válido. La reactivación de las cuentas bloqueadas deberá realizarse de forma manual por un administrador de sistema de seguridad. Para esto se deberá realizar la solicitud de desbloqueo al área de soporte.

x. La Municipalidad de Providencia restringirá el acceso a los datos de autenticación. Los datos de autenticación deberán ser protegidos con controles de acceso y encriptación para evitar que personas no autorizadas logren obtención de los datos.

xi. Las contraseñas de usuarios para ingreso a sus estaciones de trabajo y al correo electrónico deben ser cambiadas al menos cada 6 meses.

4. Responsabilidades

i. Los funcionarios deben comprender sus responsabilidades para salvaguardar los ID's de identificación (nombre de usuario) y sus contraseñas. Deberá notificar inmediatamente a un supervisor, jefe directo o Dirección Informática si sospechan que una contraseña u otro sistema de credenciales ha sido comprometida.

ii. Los supervisores y jefes directos se asegurarán de que su personal cumpla con todas las directrices que figuran en esta política, además notificarán sin demora a la Dirección de Tecnología y Gestión Digital la información de las cuentas que deben ser desactivadas, y deberán reportar cualquier sospecha de violaciones o compromisos de las credenciales.

iii. La Dirección de Tecnología y Gestión Digital y/o los encargados de la seguridad de la información, implementaran métodos de autenticación para los sistemas de información en su cuidado, instruyendo a los usuarios en cuanto a su uso.

iv. La Dirección de Tecnología y Gestión Digital preparará directrices y las normas para las credenciales de usuario, realizará revisiones de cumplimiento, y aprobará la emisión de las credenciales de administrador.

v. Los desarrolladores de sistemas y/o empresas proveedoras deben garantizar que sus sistemas soportan los procedimientos y directrices especificadas en este documento.

vi. Los dispositivos de firma electrónica, tales como token y otros, deben ser utilizados exclusivamente por el funcionario titular asignado. La "passphrase" o clave de firma electrónica es personal e intransferible. En caso que se sospeche la vulneración de

una firma electrónica o clave debe avisarse de inmediato a soporte informático para tomar las medidas pertinentes. El encargado de seguridad de la información de la Municipalidad tendrá las facultades de revocar, bloquear o eliminar dichas firmas electrónicas, o cuentas de acceso.

a. Monitoreo y registro

La Dirección de Tecnología y Gestión Digital controlará la identificación y autentificación de los usuarios de los sistemas informáticos provistos por el municipio evitando el mal uso de la infraestructura disponible. Además de lo anterior, todo sistema de la Municipalidad debe implementar registros que den cuenta del uso que se hace de la información confiada. Esto implica registros de ingreso, lectura, escritura, modificación de datos, así como registro de generación de reportes y/o bajada masiva de datos.

Lo descrito anteriormente, se realiza con el fin de proporcionar información para el caso de revisiones y auditorias que requiera la organización.

5. Normativa Legal y Reglamentaria

La infracción a las obligaciones establecidas en el artículo anterior, podrá constituir una violación al principio de probidad administrativa, y será sancionada en conformidad a lo dispuesto en la Ley N°18.883, sobre estatuto administrativo municipal. Lo anterior es sin perjuicio de la responsabilidad civil o penal que corresponda.

La Dirección de Tecnología y Gestión Digital no se hará responsable por incidentes producidos por el no cumplimiento de estas políticas de seguridad.

6. Historial de revisiones

Versión	Fecha	Cambio	Responsable / Dirección
1.0	26-abr-2021	- Creación del Documento	J.Carlos Lillo M. / DTGD
1.1	24-feb-2022	- Cambio de estructura que se solicita en el Decreto EX N°1 sin fecha del año 2021 de la Dirección de Control	J.Carlos Lillo M. / DTGD

a. Los nombres de las cuentas de administración deben ser cambiadas al menos una vez al año, o una frecuencia que no dificulte la administración de los sistemas.

b. Cada persona que tiene una necesidad legítima de usar los privilegios de administración, debe tener su propia cuenta administrativa que se utilizará para llevar a cabo funciones. El uso de la cuenta de administrador principal para cada uno de los sistemas debe delimitarse a un grupo limitado de usuarios y a situaciones de emergencia. Esto protegerá a la cuenta de administrador principal, proporcionando una pista de auditoría de las actividades administrativas.

d. Otros métodos de autenticación de contraseñas distintas de claves alfanuméricas (por ejemplo, sistemas biométricos, tarjetas inteligentes, tokens, otros), deben ser aprobados por el Dirección de Tecnología y Gestión Digital de la Municipalidad.

Para evitar ataques del tipo "fuerza bruta" (programa que prueba distintas combinaciones de letras hasta que encuentre una válida), una función de bloqueo de intrusos debe ser implementado en cada sistema, suspendiendo temporalmente la cuenta después de tres intentos de inicio de sesión no válido. La reactivación de las cuentas bloqueadas deberá realizarse de forma manual por un administrador de sistema de seguridad. Para esto se deberá realizar la solicitud de desbloqueo al área de soporte.

x. La Municipalidad de Providencia restringirá el acceso a los datos de autenticación. Los datos de autenticación deberán ser protegidos con controles de acceso y encriptación para evitar que personas no autorizadas logren obtención de los datos.

xi. Las contraseñas de usuarios para ingreso a sus estaciones de trabajo y al correo electrónico deben ser cambiadas al menos cada 6 meses.

4. Responsabilidades

i. Los funcionarios deben comprender sus responsabilidades para salvaguardar los ID´s de identificación (nombre de usuario) y sus contraseñas. Deberá notificar inmediatamente a un supervisor, jefe directo o Dirección Informática si sospechan que una contraseña u otro sistema de credenciales ha sido comprometida.

ii. Los supervisores y jefes directos se asegurarán de que su personal cumpla con todas las directrices que figuran en esta política, además notificarán sin demora a la Dirección de Tecnología y Gestión Digital la información de las cuentas que deben ser desactivadas, y deberán reportar cualquier sospecha de violaciones o compromisos de las credenciales.

iii. La Dirección de Tecnología y Gestión Digital y/o los encargados de la seguridad de la información, implementaran métodos de autenticación para los sistemas de información en su cuidado, instruyendo a los usuarios en cuanto a su uso.

iv. La Dirección de Tecnología y Gestión Digital preparará directrices y las normas para las credenciales de usuario, realizará revisiones de cumplimiento, y aprobará la emisión de las credenciales de administrador.

v. Los desarrolladores de sistemas y/o empresas proveedoras deben garantizar que sus sistemas soportan los procedimientos y directrices especificadas en este documento.

vi. Los dispositivos de firma electrónica, tales como token y otros, deben ser utilizados exclusivamente por el funcionario titular asignado. La "passphrase" o clave de firma electrónica es personal e intransferible. En caso que se sospeche la vulneración de

Providencia
Secretaría Municipal

PROVIDENCIA, 16 FEB. 2021

EX.CGR.N° 422 **/VISTOS:** Lo dispuesto en los artículos 5 letra d), 12 y 63 letra i) de la Ley N°18.695, Orgánica Constitucional de Municipalidades; y

CONSIDERANDO: 1.- Que mediante Decreto Alcaldicio EX. CGR.N°6.579 de 17 de Diciembre de 2018, se designó a contar del 17 de Diciembre de 2018, al funcionario, don **FELIPE ANDRES FREZ ROJAS,** [redacted], profesional de Administración Municipal, Encargado de Seguridad de la Información, en cumplimiento a lo observado por la Contraloría General de la República en el punto 2.1. del Capítulo II del Informe Final N°292/2018.-

2.- Que mediante Decreto Alcaldicio EX.CGR.N°2.456 de 7 de Octubre de 2019, se puso término a los efectos del Decreto Alcaldicio EX.CGR.N°6.579 de 17 de Diciembre de 2018 a contar del 1 de Septiembre de 2019 y se designó a contar del 1 de Septiembre de 2019, al funcionario, don **JUAN PABLO MUÑOZ GALLARDO,** [redacted] profesional de Administración Municipal, Encargado de Seguridad de la Información, en cumplimiento a lo observado por la Contraloría General de la República en el punto 2.1. del Capítulo II del Informe Final N°292/2018.-

3.- Que mediante Decreto EX.CGR.N°2.298 de 31 de Diciembre de 2020, se contrató a contar del 1 de Enero y hasta que sean necesarios sus servicios sin exceder del 31 de Diciembre de 2021, a don **JUAN CARLOS LILLO MOLINA,** [redacted], para desempeñarse como Profesional en la Dirección de Tecnología y Gestión Digital.-

4.- El Memorándum N°2.068 de 8 de Febrero de 2021, del Director de Tecnología y Gestión Digital.-

DECRETO:

1.- Pónese término a los efectos del Decreto Alcaldicio EX.CGR.N°2.456 de 7 de Octubre de 2019 a contar del 1 de Enero de 2021.-

2.- Desígnase a contar del 1 de Enero de 2021, al funcionario, don **JUAN CARLOS LILLO MOLINA,** [redacted] Profesional de la Dirección de Tecnología y Gestión Digital, Encargado de Seguridad de la Información.-

Anótese, comuníquese, regístrese en la Contraloría General de la República, hecho, archívese.

RODRIGO RIELOFF FUENTES
Alcalde (S)

SECRETARIO ABOGADO MUNICIPAL

EDITH NAMUR GONZALEZ ESCUDERO
Secretario Abogado Municipal (S)

PLH/ENGE/IMYJ/vpga.-
Distribución:
Interesado
Dirección de Tecnología y Gestión Digital
Dirección de Personas
Dirección de Control
Contraloría General de la República
Archivo
Decreto en trámite N° 394.-

Providencia

Oficio N°: 1391

Fecha: 04 de marzo de 2024.-

Antecedente: Solicitud MU228T0009367 de fecha 22 de enero de 2024, de la Sra. Daniela Bustamante, Externo N°594 de fecha 22 de enero de 2024.-

Materia: Deriva solicitud de información en conformidad al artículo N°13 de la Ley de Transparencia, Ingreso Externo N°594/2024.-

DE: SECRETARIO ABOGADO MUNICIPAL

A: SRA. SONIA MORENO ARAVENA
SECRETARIA GENERAL
CORPORACION DE DESARROLLO SOCIAL DE PROVIDENCIA

En el marco de la Ley N°20.285, sobre Acceso a la Información Pública, la Sra. Daniela Bustamante ha solicitado *"En relación con la Gestión Municipal, de Educación, Cultura y Salud, se solicita información correspondiente a periodo 2022 a 2024, sobre: 1.- Presupuesto Municipal asignado a: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales, año 2024. 2.- Unidad, Departamento, sección u Oficina Municipal encargada de: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales. 3.- Plan anual de Capacitaciones año 2024. 4.- Lista o nómina o Registro de Incidencias en materia de Ciberseguridad o brecha de seguridad que haya afectado la confidencialidad, integridad o disponibilidad de datos personales, y reporte de la incidencia y medidas adoptadas para el restablecimiento de los sistemas, así como informe de daños. 5.- Inventario de Infraestructura Crítica municipal. 6.- Inventario de Activos de Información sobre Datos Personales que gestiona el Municipio, sobre Funcionarios, Ciudadanos, Proveedores, etc. 7.- Redes Sociales del Municipio. 8.- Medidas de seguridad técnicas y organizativas implementadas en el municipio para garantizar la confidencialidad, disponibilidad, integridad y resiliencia en el procesamiento de datos personales. 9.- Lista o nómina de procedimientos municipales que implican el procesamiento de Datos Personales. 10.- Lista o nómina de actividades de Tratamiento de Datos Personales. 11.- Lista o nómina de Contratos de Servicios contratados que implican el procesamiento de datos personales en manos de terceros distintos al municipio (por ejemplo, contratos de encargo de tratamiento con empresas proveedoras que ayudan en la organización de eventos, seguridad física para el control de ingreso y salida de visitantes, gestión de recaudación de pagos, patentes municipales, entrega de beneficios sociales, etc), y copia de éstos. 12.- Decretos, Instrucciones y/o Reglamentos que aprueben las siguientes Políticas: a) Política de Privacidad; b) Política de Cookies; c) Política de Tratamiento de Datos Personales; d) Política de Seguridad de la Información; y e) Política de Gestión de Incidentes de Ciberseguridad. 13.- Procedimientos sobre gestión de contraseñas y controles de acceso físico o lógico a los programas y sistemas municipales, uso de dispositivos institucionales, uso de dispositivos privados para fines institucionales. 14.- Procedimiento y responsable de la función de atención y respuesta al ejercicio los derechos de los titulares de datos personales, del derecho de acceso, rectificación, cancelación y oposición de los datos. 15.- Procedimientos municipales que impliquen recopilación de datos mediante sistemas biométricos (por ejemplo, captura de huellas digitales para registrar el ingreso de las personas que laboran en el municipio, sistemas de videovigilancia y, de ser el caso, si dicho sistema captura imagen y voz), y copia de los contratos de los respectivos proveedores de los servicios. 16.- Contratos para la instalación y gestión de cámaras de videovigilancia, y Unidad Técnica del Contrato. 17.- Procedimiento de fiscalización efectuado al municipio relativo a la gestión que hace de datos personales ante la Contraloría General de la República, Consejo para la Transparencia o Tribunales de Justicia." [sic]*, respecto

Providencia

de la cual esta Municipalidad no es competente. De conformidad a lo establecido en el artículo 13 de la citada Ley, envío a Ud. la solicitud para su consideración y respectiva tramitación en lo que respecta a su competencia.-

Saluda Atentamente a Ud.,

MUNICIPALIDAD DE PROVIDENCIA
SECRETARIO ABOGADO MUNICIPAL
SECRETARÍA MUNICIPAL

MARIA RAQUEL DE LA MAZA QUIJADA
Secretario Abogado Municipal
Por orden de Sra. Alcaldesa,
Artículo 24 del Decreto Exento N° 1953 de fecha 22 de diciembre de 2023,
Delegación de Facultades del Alcalde.

MINU/MBR/JRJ/prr.-

C.C SRA. DANIELA BUSTAMANTE
FUNDACIÓN CULTURAL DE PROVIDENCIA
ADMINISTRADORA MUNICIPAL
SECRETARÍA MUNICIPAL
DEPARTAMENTO DE TRANSPARENCIA

Providencia

Oficio N°: 1392

Fecha: 04 de marzo de 2024.-

Antecedente: Solicitud MU228T0009367 de fecha 22 de enero de 2024, de la Sra. Daniela Bustamante, Externo N°594 de fecha 22 de enero de 2024.-

Materia: Deriva solicitud de información en conformidad al artículo N°13 de la Ley de Transparencia, Ingreso Externo N°594/2024.-

DE: SECRETARIO ABOGADO MUNICIPAL

A: SR. JORGE ANDRES GONZALEZ GRANIC
DIRECTOR EJECUTIVO DE LA FUNDACION CULTURAL DE PROVIDENCIA

En el marco de la Ley N°20.285, sobre Acceso a la Información Pública, la Sra. Daniela Bustamante ha solicitado *"En relación con la Gestión Municipal, de Educación, Cultura y Salud, se solicita información correspondiente a periodo 2022 a 2024, sobre: 1.- Presupuesto Municipal asignado a: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales, año 2024. 2.- Unidad, Departamento, sección u Oficina Municipal encargada de: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales. 3.- Plan anual de Capacitaciones año 2024. 4.- Lista o nómina o Registro de Incidencias en materia de Ciberseguridad o brecha de seguridad que haya afectado la confidencialidad, integridad o disponibilidad de datos personales, y reporte de la incidencia y medidas adoptadas para el restablecimiento de los sistemas, así como informe de daños. 5.- Inventario de Infraestructura Crítica municipal. 6.- Inventario de Activos de Información sobre Datos Personales que gestiona el Municipio, sobre Funcionarios, Ciudadanos, Proveedores, etc. 7.- Redes Sociales del Municipio. 8.- Medidas de seguridad técnicas y organizativas implementadas en el municipio para garantizar la confidencialidad, disponibilidad, integridad y resiliencia en el procesamiento de datos personales. 9.- Lista o nómina de procedimientos municipales que implican el procesamiento de Datos Personales. 10.- Lista o nómina de actividades de Tratamiento de Datos Personales. 11.- Lista o nómina de Contratos de Servicios contratados que implican el procesamiento de datos personales en manos de terceros distintos al municipio (por ejemplo, contratos de encargo de tratamiento con empresas proveedoras que ayudan en la organización de eventos, seguridad física para el control de ingreso y salida de visitantes, gestión de recaudación de pagos, patentes municipales, entrega de beneficios sociales, etc), y copia de éstos. 12.- Decretos, Instrucciones y/o Reglamentos que aprueben las siguientes Políticas: a) Política de Privacidad; b) Política de Cookies; c) Política de Tratamiento de Datos Personales; d) Política de Seguridad de la Información; y e) Política de Gestión de Incidentes de Ciberseguridad. 13.- Procedimientos sobre gestión de contraseñas y controles de acceso físico o lógico a los programas y sistemas municipales, uso de dispositivos institucionales, uso de dispositivos privados para fines institucionales. 14.- Procedimiento y responsable de la función de atención y respuesta al ejercicio los derechos de los titulares de datos personales, del derecho de acceso, rectificación, cancelación y oposición de los datos. 15.- Procedimientos municipales que impliquen recopilación de datos mediante sistemas biométricos (por ejemplo, captura de huellas digitales para registrar el ingreso de las personas que laboran en el municipio, sistemas de videovigilancia y, de ser el caso, si dicho sistema captura imagen y voz), y copia de los contratos de los respectivos proveedores de los servicios. 16.- Contratos para la instalación y gestión de cámaras de videovigilancia, y Unidad Técnica del Contrato. 17.- Procedimiento de fiscalización efectuado al municipio relativo a la gestión que hace de datos personales ante la Contraloría General de la República, Consejo para la Transparencia o Tribunales de Justicia." [sic]*, respecto de la cual esta Municipalidad no es competente. De conformidad a lo establecido en el

Providencia

artículo 13 de la citada Ley, envío a Ud. la solicitud para su consideración y respectiva tramitación en lo que respecta a su competencia.-

Saluda Atentamente a Ud.,

MARIA RAQUEL DE LA MAZA QUIJADA
Secretario Abogado Municipal
Por orden de Sra. Alcaldesa,
Artículo 24 del Decreto Exento N° 1953 de fecha 22 de diciembre de 2023,
Delegación de Facultades del Alcalde.

MINU/MBR/JRJ/prr.-

C.C SRA. DANIELA BUSTAMANTE
CORPORACIÓN DE DESARROLLO SOCIAL DE PROVIDENCIA
ADMINISTRADORA MUNICIPAL
SECRETARÍA MUNICIPAL
DEPARTAMENTO DE TRANSPARENCIA

Municipalidad de Providencia

TRANSPARENCIA

ACUSE DE RECIBO DE SOLICITUD DE ACCESO A LA INFORMACIÓN
LEY DE TRANSPARENCIA

MU228T0009367

Fecha: 22/01/2024 Hora: 15:47:59

Providencia
120 años

cód. emte. 111058

MUNICIPALIDAD DE PROVIDENCIA
DEPARTAMENTO DE TRANSPARENCIA
INGRESO 594
FECHA 22/01/2024
HORA 15:47

1. Contenido de la Solicitud

Nombre	Daniela
Primer Apellido	Bustamante
Segundo Apellido	
Teléfono de contacto	
Tipo de persona	Natural
Dirección postal y/o correo electrónico	[redacted]
Correo electrónico notificaciones	[redacted]
Nombre de Representante	
Primer Apellido Representante	
Segundo Apellido Representante	

Solicitud realizada	En relación con la Gestión Municipal, de Educación, Cultura y Salud, se solicita información correspondiente a periodo 2022 a 2024, sobre: 1.- Presupuesto Municipal asignado a: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales, año 2024. 2.- Unidad, Departamento, sección u Oficina Municipal encargada de: Tecnologías de la Información, Seguridad de la Información, Programas de Gestión de la Información y Protección de Datos Personales. 3.- Plan anual de Capacitaciones año 2024. 4.- Lista o nómina o Registro de Incidencias en materia de Ciberseguridad o brecha de seguridad que haya afectado la confidencialidad, integridad o disponibilidad de datos personales, y reporte de la incidencia y medidas adoptadas para el restablecimiento de los sistemas, así como informe de daños. 5.- Inventario de Infraestructura Crítica municipal. 6.- Inventario de Activos de Información sobre Datos Personales que gestiona el Municipio, sobre Funcionarios, Ciudadanos, Proveedores, etc. 7.- Redes Sociales del Municipio. 8.- Medidas de seguridad técnicas y organizativas implementadas en el municipio para garantizar la confidencialidad, disponibilidad, integridad y resiliencia en el procesamiento de datos personales. 9.- Lista o nómina de procedimientos municipales que implican el procesamiento de Datos Personales. 10.- Lista o nómina de actividades de Tratamiento de Datos Personales. 11.- Lista o nómina de Contratos de Servicios contratados que implican el procesamiento de datos personales en manos de terceros distintos al municipio (por ejemplo, contratos de encargo de tratamiento con empresas proveedoras que ayudan en la organización de eventos, seguridad física para el control de ingreso y salida de visitantes, gestión de recaudación de pagos, patentes municipales, entrega de beneficios sociales, etc), y copia de éstos. 12.- Decretos, Instrucciones y/o Reglamentos que aprueben las siguientes Políticas: a) Política de Privacidad; b) Política de Cookies; c) Política de Tratamiento de Datos Personales; d) Política de Seguridad de la Información; y e) Política de Gestión de Incidentes de Ciberseguridad. 13.- Procedimientos sobre gestión de contraseñas y controles de acceso físico o lógico a los programas y sistemas municipales, uso de dispositivos institucionales, uso de dispositivos privados para fines institucionales. 14.- Procedimiento y responsable de la función de atención y respuesta al ejercicio los derechos de los titulares de datos personales, del derecho de acceso, rectificación, cancelación y oposición de los datos. 15.- Procedimientos municipales que impliquen recopilación de datos mediante sistemas biométricos (por ejemplo, captura de huellas digitales para registrar el ingreso de las personas que laboran en el municipio, sistemas de videovigilancia y, de ser el caso, si dicho sistema captura imagen y voz), y copia de los contratos de los respectivos proveedores de los servicios. 16.- Contratos para la instalación y gestión de cámaras de videovigilancia, y Unidad Técnica del Contrato. 17.- Procedimiento de fiscalización efectuado al municipio relativo a la gestión que hace de datos personales ante la Contraloría General de la República, Consejo para la Transparencia o Tribunales de Justicia.
Observaciones	
Archivos adjuntos	
Medio de envío o retiro de la información	Correo electrónico
Dirección de envío de la información	, , ,
Formato de entrega de la información	Electrónico/PDF
Sesión iniciada en Portal	NO
Vía de ingreso en el organismo	Vía electrónica

De acuerdo a su requerimiento, este organismo procederá a verificar lo siguiente:

a) Si su presentación constituye una solicitud de información.

b) Si nuestra institución es competente para dar respuesta a ésta.

c) Si su solicitud cumple con los requisitos obligatorios establecidos en el artículo 12 de la Ley de Transparencia.

2. Fecha de entrega vence el: 19/02/2024

El plazo máximo para responder una solicitud de información es de veinte (20) días hábiles. De acuerdo a su presentación la fecha máxima de entrega de la respuesta es el día 19/02/2024. Se informa además que excepcionalmente el plazo referido podrá ser prorrogado por otros 10 días hábiles, cuando existan circunstancias que hagan difícil reunir la información solicitada, conforme lo dispone el artículo 14 de la Ley de Transparencia.

Informamos además que la entrega de información eventualmente podrá estar condicionada al cobro de los costos directos de reproducción. Por su parte, y de acuerdo a lo establecido en el artículo 18 de la Ley de Transparencia, el no pago de tales costos suspende la entrega de la información requerida.

En caso que su solicitud de información no sea respondida en el plazo de veinte (20) días hábiles, o sea ésta denegada o bien la respuesta sea incompleta o no corresponda a lo solicitado, en aquellos casos que la ley lo permite usted podrá interponer un reclamo por denegación de información ante el Consejo para la Transparencia www.consejotransparencia.cl dentro del plazo de 15 días hábiles, contado desde la notificación de la denegación de acceso a la información, o desde que haya expirado el plazo definido para dar respuesta.

3. Seguimiento de la solicitud

Con este código de solicitud: MU228T0009367 , podrá hacer seguimiento a su solicitud de acceso a través de los siguientes medios:

a) Directamente llamando al teléfono del organismo: (02) 26543200 - 26543554

b) Consultando presencialmente, en oficinas del organismo "Municipalidad de Providencia", ubicadas en Av. Pedro de Valdivia Nº 963, en el horario lunes a jueves de 08:30 a 14:00 o 15:00 a 17:00, y viernes de 08:30 a 14:00 o 15:00 a 16:00

c) Digitando código de solicitud en www.portaltransparencia.cl opción 'Hacer seguimiento a solicitudes'

4. Eventual subsanación

Si su solicitud de información no cumple con todos los requisitos señalados en el artículo 12 de la Ley de Transparencia, se le solicitará la subsanación o corrección de la misma, para lo cual tendrá un plazo máximo de cinco (5) días hábiles contados desde lanotificación del requerimiento de subsanación. En caso que usted no responda a esta subsanación dentro del plazo señalado, se letendrá por desistido de su petición.