El Concejo Municipal del Cantón de Goicoechea, en Sesión Ordinaria 17-2023, celebrada el día el 24 de abril de 2023, Artículo VIII.XXIV, se aprobó por unanimidad y con carácter firme el dictamen 43-2023 de la Comisión de Gobierno y Administración, acordándose:

**POLITICAS PARA LA SEGURIDAD DE LA INFORMACION**

1. **Introducción**

El auge de las tecnologías de Información y comunicación no sólo ha transformado sustantivamente nuestra vida cotidiana, también ha cambiado aceleradamente la forma en que nos comunicamos entre los seres humanos a través de las tecnologías de información y comunicación, desarrollo que nos hace trazar estrategias ante las oportunidades y desafíos que tenemos en la actualidad, para gestionar la información con los funcionarios de la Municipalidad de Goicoechea.

La información es uno de los componentes más sustanciales para la conducción de nuestra institución, indispensable en la consecución de los objetivos, debiendo ser visualizada como un eje transversal en los proyectos, planes y programas de desarrollo que proponga nuestra municipalidad, razones por las cuales es necesario establecer un marco regulatorio en el cual se asegure la protección de la información de forma adecuada.

La información resulta muy vulnerable ante las distintas amenazas que puedan atentar contra ella, sin importar si es impresa, digitalizada, transmitida por medios electrónicos o almacenada en sistemas de información. Por ello la protección de la información debe ser considerada una prioridad institucional, la cual se aborda en esta política aportando una serie de lineamientos y buenas prácticas, por tanto, es responsabilidad de todos los funcionarios de la Municipalidad de Goicoechea velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada uno de estos lineamientos

Este documento "Política para la Seguridad de la Información", pone a disposición una serie de lineamientos para garantizar de manera razonable la confidencialidad, integridad, y la disponibilidad de la información de la Municipalidad de Goicoechea.

## **Alcance de la Política**

Esta política, aplica para todos los funcionarios municipales, y la información a la que se refiere es, toda aquella que se genere como resultado de los procesos administrativos, operativos o técnicos de la Municipalidad de Goicoechea, mediante el uso de los recursos informáticos, transmitida por correo electrónico o utilizando los medios electrónicos institucionales, presentada en imágenes, o expuesta en conversaciones, cualquiera que sea la forma o los medios por los cuales se puede almacenar o distribuir.

## **Objetivo General**

Conservar, proteger, preservar y administrar la información producida en los procesos de la Municipalidad de Goicoechea, minimizando las eventuales amenazas como: el acceso no autorizado, divulgación, manipulación, pérdida, deterioro, o uso indebido, que se pueda producir de manera intencional o accidental, como mecanismos de control para su disponibilidad, integridad y confidencialidad.

## **Objetivos Específicos**

* 1. Proporcionar a los funcionarios los lineamientos y buenas prácticas como medidas de control, para gestionar un nivel de riesgo aceptable en la protección de la información.
	2. Lograr que el personal de la Municipalidad de Goicoechea adquiera un compromiso con la protección de la información.

 4.3 Minimizar el riesgo ante las posibles amenazas a ias que se ve expuesta la información, para garantizar niveles aceptables en la continuidad de los servicios, el cumplimiento de

los objetivos organizacionales y las obligaciones legales de conformidad con la normativa vigente.

## **Compromisos de la Administración**

5.1administración es responsable de apoyar la gestión de Seguridad de la Información y proveer los recursos necesarios para la implementación de esta política, garantizando que todas las dependencias de la Municipalidad cumplan con la misma.

5.2La administración y el personal de la Municipalidad de Goicoechea deben demostrar su compromiso a través de:

I . La revisión y aprobación de la Política de Seguridad de [a Información contenidas en este documento.

* + 1. La promoción activa de una cultura de seguridad de la información,
		2. Facilitar la divulgación de esta política a todos los funcionarios del gobierno local.
		3. El aseguramiento de los recursos adecuados para implementar y mantener vigentes las políticas de seguridad de la información

## **Compromisos del Personal**

 6.1 El personal de la Municipalidad de Goicoechea se compromete a cumplir y a acoger con integridad la presente política de seguridad de la información y seguir las buenas prácticas para la preservación de la información:

6.2 Los propietarios de activos de información son responsables de la clasificación, mantenimiento y actualización de la misma; definiendo qué usuarios deben tener permisos de acceso a la información de acuerdo a sus funciones y competencia. En general, tienen la responsabilidad de mantener íntegro, confidencial y disponible el activo de información mientras que es desarrollado, producido, mantenido y utilizado.

 6.3 Para los activos de información digital será responsabilidad del Proceso de Servicios Informáticos brindar las herramientas y mecanismos necesarios para que los responsables logren mantener los niveles aceptables de confidencialidad, Integridad y disponibilidad de la información.

## **Responsabilidades**

* 1. El cumplimiento de la Política de Seguridad de la Información es obligatorio, en caso de inobservancia, la administración municipal podrá tomar las medidas que amerite de conformidad con las disposiciones del Reglamento Interno de Organización y Servicios.

## **Identificación y clasificación de los Activos de Información**

* 1. Cada dependencia de la Municipalidad, será la encargada de identificar cuáles son sus activos de información y deberán acatar los lineamientos propuestos en esta política para asegurar la confidencialidad, disponibilidad e integridad

## **Seguridad física y ambiental**

 9-1 Acceso a la Información

* + 1. Se debe tener acceso controlado y restringido a los espacios donde se disponen los servidores principales y secundarios, así como a los cuartos de comunicaciones. El proceso de Servicios Informáticos mantendrá las normas, controles y registros de acceso a dichas áreas.
		2. Los departamentos que poseen información en soporte físico, deberán crear y mantener sus propios registros de acceso, y en todo caso el acceso a los mismos será autorizado únicamente para el personal custodio de la información.

 9.1.3 El acceso a los sitios donde se ubican los servidores sólo será permitido para las siguientes tareas:

 1.Desarrollo de operaciones tecnológicas.

 2.Aseo de los sitios bajo supervisión del personal autorizado

  3.Implementación o mantenimiento de los controles ambientales.

###  9.2 Seguridad en los equipos

 9.2.1 Sera, responsabilidad de. todos los funcionarios, bloquear la sesión cuando amerite alejarse de su espacio de trabajo.

 9.2.2 Los servidores de la Municipalidad deberán contar con las siguientes condiciones:

1.Seguridad física y Control de acceso

2.Detectores de humo y sistemas de extinción que no dañen los equipos

3.Deben estar en un lugar donde exista bajo riesgo de inundación

4.Deben de estar en circuito eléctrico con regulación de voltaje y alimentados por equipos que ayuden a la continuidad de servicios (UPS, Generador eléctrico).

 9.2.3 Las estaciones de trabajo deben estar conectadas a la red interna, correctamente aseguradas y operadas por personal de la institución el cual debe estar capacitado acerca del contenido de esta política y de las responsabilidades personales en el uso y administración de la información institucional.

 9.2.4 Sin excepción alguna, todas las estaciones de trabajo deberán poseer:

 1.Software de protección contra software malicioso.

 2 Sistemas de detección de prevención de intrusos.

 3. Cifrado para todos los activos portátiles que contengan información o credenciales de acceso donde se encuentre la información institucional.

9.2.5 Para los equipos de trabajo que, por la naturaleza de las funciones del personal, deban ser fácilmente trasladados fuera de la institución (portátiles, tablets, dispositivos móviles) el personal deberá tomas las siguientes medidas:

1. Mantener las políticas de acceso a internet y protección contra malware
2. Mantener las políticas de dominio institucional.
3. Se debe utilizar cifrado para información contenida en los equipos
4. Contar con autorización del jefe inmediato para trasladar fuera de la institución cualquier equipo de tecnología de información.

9.2.6 Los medios que alojan copias de seguridad deben ser conservados de forma correcta de acuerdo a las políticas y estándares que para tal efecto elabore y mantenga el Proceso de Servicios Informáticos.

9.2.7 Todas las dependencias institucionales deben adoptar y cumplir las políticas definidas para la creación y manejo de copias de seguridad.

## **Seguridad de la información en soporte impreso**

10.1 Se deben observar y cumplir las medidas de preservación y control de los documentos en soportes tradicionales, establecidos en los artículos 82, 83 y 84 y 93 del Decreto Ejecutivo NO 40554-C del 29 de junio de 2017, reglamento a la Ley 7202,

"Ley del Sistema Nacional de Archivos", así como la Norma Técnica para la Digitalización de Documentos en Soporte Físico y la Autenticidad de imágenes" publicada en el Alcance N O 105 a la Gaceta N O 92 del 17 de mayo de 2017

## **Seguridad de la información en soporte electrónico y en soporte magnético**

 11 .1 Se deben observar y cumplir las medidas de preservación y control de los documentos en soportes tradicionales, que se establecen en los artículos 77, 78, 87, 88, y 93 del Decreto Ejecutivo N° 40554-C del 29 de junio de 2017, así como la

Norma Técnica pare Gestión de Documentos Electrónicos en el Sistema Nacional de Archivos, publicada en el Alcance NO 105 a la Gaceta NO 92 del 17 de mayo de 2017.

## **Seguridad de operaciones y comunicaciones**

 12.1 El Proceso de Servicios Informáticos, definirá los controles que garanticen la adecuada operación tecnológica. Los controles que se establezcan incluirán al menos los siguientes procedimientos:

1. Copias de seguridad.

1. Recuperación de datos y reversión de cambios.
2. Administración de sistemas contra software malicioso.
3. Administración de usuarios y contraseñas.
4. Administración de acceso a los recursos.
5. Administración de acceso remoto.
6. Medición de desempeño.
7. Capacidad y disponibilidad de los recursos de Tl.
8. Gestión de pistas de auditoria y sistemas de registro de información.
9. Aseguramiento de plataformas.

## **Protección contra software malicioso e intruso**

13.1 El Proceso de Servicios Informáticos implementará los controles para detener, prevenir y recuperar y protección frente al software malicioso.

13.2 Todos los equipos y sistemas informáticos, sin excepción, deben ser protegidos teniendo en cuenta un enfoque multinivel que involucre controles humanos, físicos técnicos y administrativos.

13.3 En todo caso y como control mínimo, las estaciones de trabajo de la Municipalidad, deben estar protegidas por software antivirus con capacidad de actualización automática. En cuanto a firmas de política de virus, los usuarios no están autorizados a deshabilitar este control.

13.4 En la Municipalidad de Goicoechea no se permite en ningún caso el uso de software no licenciado y su instalación en cualquiera de los equipos institucionales.

## **Correo Electrónico**

* 1. La Municipalidad de Goicoechea regulará de manera específica el uso, gestión y protección del correo electrónico.

## **Acceso a internet.**

 15.1 El uso de Internet debe estar destinado exclusivamente a la ejecución de las actividades de la Municipalidad y debe ser utilizado por el usuario únicamente para realizar las funciones establecidas para su cargo.

 15.2 El acceso a internet se debe realizar a través de equipos de seguridad perimetral que cuenten con bloqueo de amenazas, perfiles de accesos, control de aplicaciones y detección de intrusos entre otros.

 15.3 El Proceso Servicios Informáticos será el encargado de definir y administrar los perfiles de acceso, además de tomar [as medidas necesarias para fa protección de la información y la calidad de servicio en los enlaces.

 15.4 Está prohibido el uso de internet con fines comerciales, políticos, particulares o cualquier otro que no sea estrictamente laboral y que dio origen a la habilitación del servicio.

 15.5 Las descargas de contenido serán reguladas acorde a su tipo y contenido, bloqueándose en caso de ser necesario.

 15.6 Las video-conferencias de la Municipalidad, serán de uso exclusivo para asuntos relacionados con el municipio. Cualquier excepción a esta política debe ser autorizada por el Alcalde Municipal.

 15.7 No se permitirá el acceso a internet en dispositivos que no cuenten la debida protección de perímetro y protección en la estación de trabajo.

 15.8 El Proceso de Servicios Informáticos brindará los manuales y herramientas para realizar las copias de seguridad, así como la capacitación que requieran los usuarios para estos fines.

 15.9 El Proceso de Servicios Informáticos realizará diariamente los respaldos de [os sistemas de información que se encuentren almacenados en el centro de datos de la municipalidad.

## **Recursos compartidos**

 16.1 El uso de carpetas compartidas en los equipos de cómputo de los usuarios es una práctica que, aunque es muy útil en nuestro entorno de trabajo, tiene implícitos algunos riesgos que pueden afectar los principios de integridad y disponibilidad de la información, por cuanto su uso, debe ser controlado. Con este propósito la Municipalidad define los siguientes lineamientos para uso seguro:

1.Los administradores de la red establecen e implementan, en los casos aprobadas, la configuración de acceso a la carpeta, previo requerimiento de la misma a través de cada Coordinador de Proceso, Subproceso, Actividad o Subactividad.

2.El usuario que autoriza y dispone el recurso compartido es el responsable por las acciones y los accesos a la información contenida en dicha carpeta.

3.Se debe definir el tipo de acceso y los roles estrictamente necesarios sobre la carpeta (lectura, escritura, modificación y borrado).

4.El acceso a carpetas compartidas debe delimitarse a los usuarios que las necesitan y deben ser protegidas con contraseñas.

5.No se debe permitir el acceso a dichas carpetas a usuarios que no cuenten con antivirus actualizado.

##  **Copias de seguridad**

 17.1 Toda la información de importancia y de interés institucional debe ser respaldad en copias de seguridad conforme a los procesos documentados por el Procesos Servicios  Informáticos. Las copias de seguridad deben estar almacenadas en medios seguros y protegidos. La frecuencia de los respaldos debe realizarse según la necesidad de cada dependencia.

 17.2 Cada dependencia deberá realizar pruebas controladas para asegurar que las copias de seguridad pueden ser correctamente leídas y restauradas.

 17.3 El Proceso Servicios Informáticos brindará las herramientas y procedimientos para este apartado.

## **Computación en nube.**

 18.1 Ninguna dependencia de la Municipalidad, podrá fizar tecnologías de computación y aplicación en la nube si no está previamente autorizado por el Proceso de Servicios

 Informáticos.

## **Intercambio de información**

* 1. Se debe establecer mecanismos de acceso y solitud de información donde se detalle la  debida justificación y motivo para contar con la información.

## **Instalación de software**

 20.1 Todo software que se pretenda adquirir, debe ser aprobado e instalado por el Proceso de Servicios Informáticos.

 20.2 Queda prohibido la instalación de software, que viole los derechos de autor o acuerdos de licenciamiento.

## **Acceso Remoto y Teletrabajo**

 21.1 El acceso remoto y teletrabajo estarán sujetos a medidas de control establecidas por el Procesos Servicios Informáticos, procesos que serán debidamente reglamentados. Este acceso será a través de Una red privada virtual y con infraestructura de escritorios virtuales para no exponer a los riesgos de seguridad que se puedan presentar en los equipos no controlados por la Municipalidad

 21.2 El Proceso de Asesoría en Servicios Informáticos, debe implementar las medidas necesarias para protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado asegurar que no se comprometa la información municipal, teniendo en cuenta los riesgos que conlleva el trabajar con el  equipo móvil en entornos desprotegidos.

 21.3 La utilización de los servicios móviles conectados a las redes, deben tener una protección idónea. El acceso remoto a la información de la Municipalidad a través de redes públicas usando servicios de computación móvil, sólo debería tener lugar después de la identificación y autenticación exitosa y con el establecimiento de los mecanismos adecuados del control del acceso.

1. **Monitoreo de servicios**
	1. El Proceso de Servicios Informáticos efectuará los monitoreos y efectuará controles con alertas para todos los servicios brindados para atender de mejor manera los incidentes que se puedan presentar en los servicios, así mismo poder hacer una detección temprana de los incidentes.
2. **Sincronización de relojes.**
	1. Los relojes de los sistemas de la Municipalidad de Goicoechea estarán sincronizados con una zona horaria internacional GMT/UTC-6
3. **Control de acceso**

### Perfiles

24.1.1 Los accesos a los recursos de tecnologías de información institucionales serán restringidos según los perfiles de usuario definidos por el Procesos Servicios Informáticos. Esta dependencia será la encardada de brindar y administrar los mismos y herramientas para otorgar acceso a los usuarios. Se debe realizar una solitud formal por usuario, la misma se podrá realizar de forma física o electrónica para brindar los accesos correspondientes a cada usuario.

 24.1.2 Los procedimientos para brindar el acceso a los usuarios, deben cubrir todas las etapas del ciclo de vida del usuario, desde que es contratado hasta que deje su puesto de trabajo.

 24.1.3 Para toda persona que ingrese a laborar o sea contratada por Servicios Profesionales Temporales o interinos, a la Municipalidad de Goicoechea, el Proceso de Recursos Humanos debe asegurar las responsabilidades sobre seguridad de la información, de manera previa a la contratación. Esta tarea debe reflejarse en una adecuada descripción del cargo y en los términos y condiciones de la contratación.

 24.1.4 Los programas de capacitación institucional promoverán la concientización de protección de la información para todo el personal.

 24.1.5 El Proceso de Recursos Humanos informará por escrito al Proceso de Servicios Informáticos, ante la contratación, salida, traslado horizontal, o ascenso de los funcionarios, ya sea temporal o permanente, para que se lleve a cabo la devolución de todos los activos y cancelación de los derechos de acceso.

### 24.2Claves y nombres de usuario

 24.2.1 Todos los usuarios de los recursos de tecnologías de información y comunicación de la Municipalidad requieren de una identidad intransferible, compuesta por un código de usuario y una contraseña secreta o bien un certificado digital reconocido en los casos donde se permita,

 24.2.2 El usuario es el responsable de todas las acciones que se realicen con la identidad que le fue asignada, salvo en los casos en que se demuestre que ese mecanismo de identificación ha sido vulnerado

 24.2.3 El Proceso Servicios Informáticos podrá revocar de oficio los permisos y claves de acceso cuando se detecte que la clave ha sido compartida o la conozca un tercero o cuando se encuentre en riesgo la información institucional

 24.2.4 Cada jefatura será la encargada de autorizar los accesos y perfiles que deben tener sus usuarios, además de solicitar una debida desactivación cuando los mismos no laboren bajo su responsabilidad

1. **Trazabilidad de la información**

25.1Todos los sistemas de información y medios de acceso a los respectivos servicios deben contar con bitácoras y registros para determinar cuándo, dónde y cómo fue accedida, modificada o eliminada la información.

1. **Seguridad en Desarrollo y Mantenimiento de Software de Infraestructura**
	1. El proceso Servicios Informáticos deberá crear los métodos y mecanismos para asegurar la implementación de desarrollo y mantenimiento de software teniendo en cuenta los principios de seguridad y acceso a información.
	2. Todo proyecto de desarrollo de software interno, cuando el Proceso de Asesoría en Servicios Informáticos así lo determine, deberá contar el análisis, identificación y valoración de Riesgos. La Municipalidad no emprenderá procesos de desarrollo — o mantenimiento — de sistemas software que tengan asociados riesgos altos no mitigados.
	3. Se debe controlar el acceso al sistema de archivos y al código fuente de los programas. La actualización del software aplicativo, las aplicaciones y las librerías, sólo debe ser llevada a cabo por los administradores.
	4. Se debe comprobar periódicamente que los sistemas de información cumplen con las normas de implementación de seguridad.
	5. Se prohíbe el uso de programas que puedan ser capaces de invalidar [os controles del sistema y de la aplicación.
2. **Continuidad de los servicios**

27.1Se deben establecer lineamientos para contar una continuidad de los servicios tecnológicos.

27.2 El Proceso Servicios Informáticos deberá contar con un plan de contingencia que permitía el restablecimiento de los servicios y garantizar de manera razonable la continuad de todos los servicios ofrecidos.

27.3 Se debe identificar todos los riesgos y amenazas y mitigarlos o tomar las medidas de control interno necesarias hasta que podamos tener niveles de riesgo aceptables.

1. **Definiciones**
2. Seguridad de la información

La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos y de la misma.

1. Información

La información es un conjunto organizado de datos procesados: que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. Existen diversos enfoques para el estudio de la información

3. Activo de información

Cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de la Municipalidad y, en consecuencia, debe ser protegido,

4. Confidencialidad

La confidencialidad es la garantía de que la información personal será protegida para que no sea divulgada sin consentimiento de la persona. Dicha garantía se lleva a cabo por medio de un grupo de reglas que limitan el acceso a esta información. Cada individuo tiene derecho a proteger su información personal.

5. Disponibilidad

La disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

6. Evaluación del Riesgo

Proceso normalizado, que permite comparar el riesgo estimado contra criterios de riesgo dados, para determinar los parámetros de aceptabilidad.

7. Integridad

Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas, a Groso modo, la integridad es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

8. Riesgo

Posibilidad de que se produzca un contratiempo o una desgracia, de que alguien o algo sufran perjuicio o daño.

9. Centro de Datos

Ubicación donde se concentran los recursos necesarios para el procesamiento de la información de una organización.

10. Cifrado

En criptografía, el cifrado es un procedimiento que utiliza un algoritmo de cifrado con cierta clave (clave de cifrado) transforma un mensaje, sin atender a su estructura lingüística o

significado, de tal forma que sea incomprensible o, al menos, difícil de comprender a toda persona que no tenga [a clave secreta (clave de descifrado) del algoritmo.

11. Control

conjunto de los mecanismos, acciones y herramientas realizadas para detectar la presencia de errores

12. Licencia de Software

Es un contrato entre el licenciante (autor/titular de los derechos de explotación/distribuidor) y el licenciatario (usuario consumidor/usuario profesional o empresa) del programa informático, para utilizar el software cumpliendo una serie de términos y condiciones establecidas.

13. Medios Extraíbles

En el campo del almacenamiento de datos, los medios extraíbles son aquellos soportes de almacenamiento diseñados para ser extraídos de la computadora sin tener que apagarla.

14. Perfiles de Usuario

Un perfil es un entorno personalizado específicamente para un usuario. Contiene los permisos o accesos predeterminados en relación al perfil.

15. Antimalware

El antimalware (anti-malware) es un tipo de programa diseñado para prevenir, detectar y remediar software malicioso en los dispositivos informáticos individuales y sistemas Tl.

16.Infraestructura de escritorios virtuales

La infraestructura de escritorios virtuales (VDI) es la práctica de hospedar un sistema operativo para computadoras de escritorio en una máquina virtual (VM) que opera desde un servidor centralizado

17. Política

Intención o directriz emitida por el Jerarca institucional

18. Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información, además puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

19.Tl

se refiere a tecnologías de la información

20. TIC

se refiere a tecnologías de la información y comunicaciones

21. Vulnerabilidad

debilidad de un activo o grupo de activos, que puede ser aprovechada por una o más amenazas.

Control de Formalización y cambios en la política

|  |  |  |
| --- | --- | --- |
| VERSION | FECHA | JUSTIFICACION DE LA VERSION |
|  | Julio, 2022 | Formalización de la Política de Seguridad de la Información. Jenny Ulate Rojas |

Licda. Yoselyn Mora Calderón

Depto. Secretaría