APRUEBA REGLAMENTO MUNICIPAL SOBRE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL Y USO SEGURO DE ELEMENTOS ELECTRÓNICOS DE LA ILUSTRE MUNICIPALIDAD DE COINCO

Coinco, 06 JUN. 2022

Con esta fecha se establece lo siguiente:

VISTOS:

Lo dispuesto en el DFL Nº 1-19.653 que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.575, Orgánica Constitucional de Bases Generales de la Administración del Estado; lo dispuesto en el DFL Nº 1 de 2006, que fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.695, Orgánica Constitucional de Municipalidades; lo consagrado en la Ley Nº 19.880 de Bases de los Procedimientos Administrativos que Rigen los Actos de los Órganos de la Administración del Estado;

CONSIDERANDO:

1. Lo indicado por la Ley Orgánica Constitucional de Municipalidades en su artículo 1º, en el sentido que la administración local de cada comuna o agrupación de comunas corresponde a una municipalidad; y que de acuerdo al artículo 2º de la Ley Orgánica Constitucional de Municipalidades la máxima autoridad del municipio será el alcalde;

2. Lo indicado en el artículo 12 de la Ley Orgánica Constitucional de Municipalidades que prescribe que la manifestación de la voluntad del municipio se traduce en ordenanzas, reglamentos municipales, decretos alcaldicios o instrucciones;

3. Que, según la Ley Orgánica Constitucional de Municipalidades, en su artículo 12, inciso tercero, se señala que los reglamentos municipales serán normas generales obligatorias y permanentes, relativas a materias de orden interno de la municipalidad;

4. Que se tiene que dar fuerza a lo señalado por al artículo 56 de la Ley Orgánica Constitucional de Municipalidades en el sentido de que el alcalde es la autoridad máxima del municipio y en tal calidad le corresponderá su dirección y administración superior y la supervigilancia de su funcionamiento;

5. Que el artículo 3º de la Ley de Bases de la Administración del Estado indica que la Administración del Estado deberá observar los principios de responsabilidad, eficiencia, eficacia, coordinación, probidad y control, entre otros;

6. Que, el artículo 31, inciso segundo, de la Ley Nº 18.575 prescribe que a los jefes de servicio les corresponderá dirigir, organizar y administrar el correspondiente servicio; controlarlo y velar por el cumplimiento de sus objetivos; responder de su gestión, y desempeñar las demás funciones que la ley les asigne;

7. Que, el artículo 5º de la Ley Nº 18.575 establece que las autoridades y funcionarios deberán velar por la eficiente e idónea administración de los medios públicos y por el debido cumplimiento de la función pública;

8. Que, el artículo 40 de la Ley N° 18.695, Orgánica Constitucional de Municipalidades, señala que será el estatuto administrativo de los funcionarios municipales el que regulará la carrera funcionaria y considerará especialmente el ingreso, los deberes y derechos, la responsabilidad administrativa y la cesación de funciones;

9. Que, a partir de la entrada en vigencia de la Ley N° 21.180 de Transformación Digital del Estado, el próximo mes de junio de 2022, los órganos de la Administración del Estado deberán avanzar progresivamente en transformar sus procedimientos administrativos a medios electrónicos, con el objeto de mejorar la gestión y entrega de servicios a la ciudadanía;

10. Que, el Decreto con Fuerza de Ley N° 1, de 2020, del Ministerio Secretaría General de la Presidencia, que Establece Normas de Aplicación del Artículo 1° de la Ley N° 21.180, de

Transformación Digital del Estado, respecto de los procedimientos administrativos regulados en leyes especiales que se expresan a través de medios electrónicos y determina la gradualidad para la aplicación de la misma ley, a los órganos de la Administración del Estado que indica y las materias que les resultan aplicables;

11. Que, el artículo 11 del Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, prescribe que deberá establecerse una política que fije las directrices generales que orienten la materia de seguridad dentro de cada institución, que refleje claramente el compromiso, apoyo e interés en el fomento y desarrollo de una cultura de seguridad institucional;

12. Que, el informe final N° 1009, de fecha 31 de marzo de 2022, de la Contraloría Regional del Libertador General Bernardo O'Higgins, ordena que producto de auditoría al macroproceso de tecnologías de la información, la Ilustre Municipalidad de Coinco debe nombrar un comité de seguridad que asesore a la autoridad administrativa en las materias relativas a seguridad de los documentos electrónicos;

13. Que, por tanto, en uso de mis facultades legales, vengo en dictar el siguiente:

REGLAMENTO: Nº 0030

1. **APRUÉBESE** en todas sus partes el Reglamento Municipal sobre Política de Seguridad de la Información Digital y Uso Seguro de Elementos Electrónicos de la Ilustre Municipalidad de Coinco, de acuerdo al siguiente texto:

REGLAMENTO MUNICIPAL SOBRE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DIGITAL Y USO SEGURO DE ELEMENTOS ELECTRÓNICOS DE LA ILUSTRE MUNICIPALIDAD DE COINCO

INTRODUCCIÓN

La información es un recurso estratégico, que tiene valor para los procesos que realiza diariamente la Municipalidad y por consiguiente debe ser debidamente protegida, garantizando la continuidad de los sistemas de información, la operación de los equipos computacionales, minimizando los riesgos de daño y hurto de información, además de contribuir y facilitar la gestión administrativa de la Municipalidad.

En el entendido de que los riesgos que se logren identificar estarán siempre presentes, ya que no se pueden eliminar, la Municipalidad se compromete a gestionar la seguridad de la información como un proceso continuo en el tiempo, a través de un programa de mantención del "Sistema de Gestión de Seguridad de la información (SGSI)", basado en la norma chilena NCh-ISO 27001:2013 y en los lineamientos de ciberseguridad entregado por Presidencia y por el encargado municipal de seguridad de la información, tendiente a homogeneizar los criterios de seguridad y ciberseguridad, con el objetivo de preservar los activos de información institucional.

Para que estos principios de la Política de Seguridad de la Información sean efectivos, es necesario que como documento forme parte de la cultura organizacional de la Municipalidad, y contar con el compromiso de todos los funcionarios municipales, para contribuir con la difusión, conocimiento e integración.

DOCUMENTOS DE REFERENCIA

i. Norma Chilena NCh-ISO 27001:2013, Sistemas de gestión de la seguridad de la información – Requisitos; y en la norma chilena NCh-ISO 27002:2013 código de prácticas para los controles de seguridad de la información.
ii. Decreto Supremo N° 83, de 2005, del Ministerio Secretaria General de la Presidencia, Aprueba Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos.
iii. Ley N° 20.285, de 2008, del Ministerio Secretaria General de la Presidencia, Sobre Acceso a la Información Pública.
iv. Ley N° 19.223, de 1993, del Ministerio de Justicia, Tipifica Figuras Penales Relativas a la Informática.
v. Ley N° 19.927, de 2004, del Ministerio de Justicia, Modifica el Código Penal, el Código de Procedimiento Penal y el Código Procesal Penal en materia de Delitos de Pornografía Infantil.

vi. Ley N° 18.883, de 1989, del Ministerio del Interior, Aprueba Estatuto Administrativo para Funcionarios Municipales.

vii. Decreto con Fuerza de Ley 1/19.653, de 2001, del Ministerio Secretaria General de la Presidencia, Fija texto refundido, coordinado y sistematizado de la ley 18.575 Orgánica Constitucional de Bases Generales de la Administración del Estado.

viii. Ley N° 19.628 sobre Protección de la Vida Privada regula el tratamiento de datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares.

ix. La Ley N° 19.799 sobre Firma Digital y Firma Electrónica en Chile.

TÍTULO I: DEFINICIONES

Artículo 1°: Para efectos de la presente política se deberán tener en cuenta los siguientes conceptos:

a) **Activo de Información**. Aquellos elementos relevantes en la producción, emisión, almacenamiento, comunicación, visualización y recuperación de información, de valor para la Institución. Se distinguen 3 niveles básicos de activos de información:
   a. La Información propiamente tal, en sus múltiples formatos, a modo de ejemplo, papel, digital, texto, imagen, audio, video.
   b. Los Equipos, Sistemas de Información e Infraestructura que soportan esta información, que son actualmente ingresados como conjunto independientemente sean activos que operen en grupo.
   c. Las Personas que utilizan la información, y que tienen el conocimiento de los procesos institucionales.

b) **Autenticación**. Proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.

c) **Comité de Seguridad de la Información Institucional**. Agrupación de personas que tienen como misión validar y aprobar las políticas de seguridad de la información, y los controles tendientes a regular el uso y manejo de la información. Arbitrar conflictos que se generen en materias de seguridad de la información, apoyar planes de difusión y formación de la cultura de la seguridad de la información.

d) **Confidencialidad**. Aseguramiento de que el documento electrónico sea conocido sólo por quienes están autorizados para ello.

e) **Contenido del documento electrónico**. Información, ideas y conceptos que un documento expresa.

f) **Disponibilidad**. Aseguramiento de que los usuarios autorizados tengan acceso oportuno al documento electrónico y sus métodos de procesamiento.

g) **Documento electrónico**. Toda representación de un hecho, imagen o idea que sea creada, enviada, comunicada o recibida por medios electrónicos y almacenada de un modo idóneo para permitir su uso posterior.

h) **Documentos públicos**. Aquellos documentos que no son ni reservados ni secretos, cuyo conocimiento no está circunscrito.

i) **Documentos reservados**. Aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley, que les confiere tal carácter.

j) **Documentos secretos**. Los documentos que tienen tal carácter de conformidad al artículo 13 de la Ley Orgánica Constitucional de Bases Generales de la Administración del Estado y su Reglamento.

k) **Encargado de Seguridad y Ciberseguridad**. Persona responsable por la implementación de medidas de control que garanticen la seguridad de la información, así como también aplicar las medidas de ciberseguridad que promueve el Estado.

l) **Identificador formal de autenticación**. Mecanismo tecnológico que permite que una persona acredite su identidad utilizando técnicas y medios electrónicos.

m) **Incidentes de seguridad**. Situación adversa que amenaza o pone en riesgo un sistema informático.

n) **Integridad**. Salvaguardia de la exactitud y totalidad de la información y de los métodos de procesamiento del documento electrónico, así como de las modificaciones realizadas por entes debidamente autorizados.

o) **Política de seguridad**. Conjunto de normas o buenas prácticas, declaradas y aplicadas por una organización, cuyo objetivo es disminuir el nivel de riesgo en la realización de un conjunto de actividades de interés, o bien garantizar la realización periódica y sistemática de este conjunto.

p) **Repositorio**. Estructura electrónica donde se almacenan documentos electrónicos.

q) **Riesgo**. La posibilidad de sufrir daños o perdidas, la amenaza es un componente del riesgo y se puede considerar coma: un agente de amenazas ya sea humano o no humano.

r) **Seguridad de la Información.** Es el nivel de certeza y confianza que la organización desea tener de su capacidad para preservar la confidencialidad, factibilidad de autenticación, integridad y disponibilidad de la información. De esta forma, proteger el recurso o activo de información de una amplia gama de amenazas, asegurando la continuidad de las operaciones de la Municipalidad, minimizando el daño y cumpliendo su misión y objetivos estratégicos.

s) **Sistema de Gestión de Seguridad de la Información**. Parte del sistema de gestión, basada en un enfoque hacia los riesgos de una institución, cuyo fin es establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información. El sistema de gestión considera la estructura organizacional, políticas, actividades de planificación, responsabilidad, prácticas, procedimientos, procesos y recursos.

t) **Sistema informático**. Conjunto de uno o más computadores, software asociado, periféricos, terminales, usuarios, procesos físicos, medios de transferencia de información y otros, que forman un todo autónomo capaz de obtener, almacenar, tratar, administrar, controlar, procesar, transmitir o recibir datos, para satisfacer una necesidad de información.

u) **Usuario**. Entidad o individuo que utiliza un sistema informático.

TÍTULO II: ROLES Y RESPONSABILIDADES

PÁRRAFO I: COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

Artículo 2º: El Comité de Seguridad de la Información es responsable del ciclo de vida de las políticas de seguridad de la información y tiene las siguientes atribuciones:

a) Velar por la implementación de los controles de seguridad en la plataforma tecnológica.
b) Fomentar planes de difusión, capacitación y formación de la cultura de la seguridad de la información.
c) Arbitrar conflictos que se generen en materias de seguridad de la información.
d) Revisar, al menos una vez al año, el funcionamiento del Sistema de Gestión de Seguridad de la Información (SGSI).

PÁRRAFO II: ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN

Artículo 3°: El encargado de seguridad de la información tendrá las siguientes responsabilidades:

a) Proponer, desarrollar y actualizar las políticas de seguridad de la información al interior de la institución, coordinar su implementación y evaluación, velando por su correcta aplicación.
b) Monitorear el correcto funcionamiento de los procedimientos vinculados al Sistema de Gestión de la Seguridad de la Información (SGSI).
c) Mantener coordinación con otros departamentos y unidades de la Municipalidad para apoyar el cumplimiento de los objetivos de seguridad.
d) Establecer enlaces con encargados de seguridad de la información de otros organismos públicos, con las instancias gubernamentales encargadas de la Seguridad de la Información y con especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos de seguridad de la información y ciberseguridad pertinentes.
e) Mantener actualizado el inventario de activos de información de la Municipalidad, según el requerimiento de que cada activo fijo que opere en grupo debe de ser detallado de manera completa todos sus periféricos o conjunto de activos fijos.

f) Mantener informado periódicamente al Comité de Seguridad de la Información acerca del estado del Sistema de Gestión de Seguridad de la información en la Municipalidad.
g) Promover acciones tendientes a la difusión y sensibilización respecto a la Seguridad de la Información y Ciberseguridad a los funcionarios, trabajadores y practicantes vinculados a la institución.
h) Ejecutar, aplicar e implementar las medidas de Ciberseguridad que sean instruidas por el Alcalde, el Administrador Municipal, el Director de Control, el Director de Administración y Finanzas o el órgano de la Administración del Estado con competencia sobre materias de seguridad de la información.

PÁRRAFO III: USUARIOS

Artículo 4°: Los usuarios son las personas, funcionarios, trabajadores, practicantes o personal externo que preste servicios permanentes o temporales, que usan los activos de información y los sistemas computacionales de la institución. Son responsables de conocer, dar a conocer, cumplir y hacer cumplir la política de seguridad de la información vigente, así como las políticas específicas, manuales y procedimientos asociados a la ciberseguridad y, además, tienen la obligación de reportar cualquier incidente o evento de seguridad del que tengan conocimiento.

PÁRRAFO IV: DIRECTIVOS Y JEFATURAS DE LA MUNICIPALIDAD

Artículo 5°: Las jefaturas de las Direcciones, Departamentos y Unidades deberán supervisar que el personal de su dependencia cumpla con la presente política, así como de las políticas específicas, manuales y procedimientos asociados al SGSI, ciberseguridad, transparencia y uso de datos personales y bases de datos.

TÍTULO III: OBJETIVOS DE LA PRESENTE POLÍTICA

PÁRRAFO I: OBJETIVO GENERAL

Artículo 6°: El propósito de esta Política es definir el objetivo, dirección, principios y reglas básicas para la gestión de la seguridad de la información para la Municipalidad. La Autoridad Comunal reconoce la importancia y el valor de los activos de información como un elemento crítico al proceso de toma de decisiones para el cumplimiento de su Misión Institucional y, por tanto, establece la Política del Sistema de Gestión de la Seguridad de la Información. En el marco de este Objetivo, se establecen las características mínimas obligatorias de seguridad y confidencialidad que deben cumplir los documentos electrónicos, como también, estándares mínimos de seguridad en el uso, almacenamiento, acceso y distribución del documento electrónico, y facilitar la relación electrónica al interior de la Municipalidad con otros órganos de la Administración del Estado, la ciudadanía y el sector privado.

PÁRRAFO II: OBJETIVOS ESPECÍFICOS

Artículo 7°: Como objetivos específicos que se propone lograr la presente política, en consonancia con su objetivo general, son los siguientes:

1) Proteger los recursos de información de la Municipalidad y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los conceptos de confidencialidad, integridad y disponibilidad, partes claves de la seguridad de la información y la protección de datos.
2) Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
3) Mantener la Política de Seguridad del Municipio actualizado, para asegurar su vigencia y nivel de eficacia ante nuevas amenazas.
4) Proteger eficientemente los activos de información institucionales, asegurando su confidencialidad, integridad y disponibilidad.
5) Establecer procedimientos, instrucciones u otros documentos para la clasificación y catastro de los activos de información de la Municipalidad.
6) Establecer procedimientos para efectuar una evaluación anual de riesgos destinada a proteger eficazmente los activos de información de la Municipalidad y prevenir la ocurrencia de incidentes de seguridad de la información.
7) Establecer los mecanismos de difusión de la presente política para el conocimiento de todos los funcionarios de planta y a contrata y personal a honorarios del Municipio, especialmente en lo referente a capacitaciones periódicas en materias de seguridad de la información.

8) Establecer los mecanismos de difusión de la presente Política para el conocimiento de terceras partes, especialmente en lo referente a la confidencialidad de la información de la que tome conocimiento mientras dure el contrato y convenios, sus derechos y obligaciones en materia de seguridad de la información del Municipio y las consecuencias en caso de no cumplimiento, que se establecen en los respectivos contratos y convenios.
9) Ejecutar, aplicar e implementar las medidas de ciberseguridad instruidas mediante el Instructivo Presidencial N° 8, del 23 de octubre de 2018, del Presidente de la República, que Imparte Instrucciones Urgentes en Materia de Ciberseguridad, para la Protección de Redes, Plataformas y Sistemas Informáticos de los Órganos de la Administración del Estado.

TÍTULO IV: DISPOSICIONES GENERALES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Artículo 7°: Principios de la seguridad de la información: La seguridad de la información se entiende como la preservación de los activos de información institucional con respecto a:

a) La Confidencialidad: que la información se accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
b) La Integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
c) La Disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Artículo 8°: La presente política será evaluada en el Municipio al menos una vez al año, o bien, cuando se produzca un cambio significativo que la impacte, esto con la finalidad de asegurar su continua idoneidad, eficiencia y efectividad. Ello incluye que el Encargado de Seguridad de la Información y Ciberseguridad realice las revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la Información, de manera que la materia cumpla con mantener su vigencia y se puedan llevar a cabo los planes de acción necesarios para realizar mejoras e integrar nuevas ideas.

Una vez que el documento entre en vigencia el Encargado de Seguridad de la Información y Ciberseguridad deberá difundir al personal y externos considerado en el alcance mediante cualquier vía que permita comunicar la creación o modificaciones efectuadas. Estas vías podrán ser página web institucional, intranet, correo electrónico al personal, capacitaciones, difusiones, etc.

Artículo 9°: Todos los usuarios de la Municipalidad sean planta, contrata, honorarios, asesores, consultores, practicantes, y otros trabajadores, deben aceptar esta política y procedimientos relacionados.

Para el caso de terceros y solo por el hecho de participar en algún proceso de compras del servicio, el oferente debe dar cumplimiento a la política, manuales y procedimientos vigentes de seguridad de la información, publicados en el sitio web de la municipalidad y sus correspondientes modificaciones, la cuales se presumen conocidas por el contratista o adjudicatario para todos los efectos legales.

La presente política, y las políticas específicas asociadas, admitirán excepciones en su aplicación, siempre y cuando, existan casos con razones fundadas, los cuales serán documentados por el Encargado de Seguridad de la Información y Ciberseguridad y debidamente autorizados por la autoridad.

Artículo 10°: Sanciones por incumplimiento de la política: El incumplimiento de las disposiciones establecidas por la Política de Seguridad de la Información, procedimientos u otros documentos que se deriven de estos, debidamente acreditado, conlleva la aplicación de medidas disciplinarias previstas en el Estatuto Administrativo, respecto a los funcionarios de la Municipalidad o al término anticipado del contrato por incumplimiento de obligaciones, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

Artículo 11: El Encargado de Seguridad de la Información y Ciberseguridad será quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información del Municipio, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente política.

Asimismo, el Encargado de Seguridad de la Información y Ciberseguridad será el encargado de coordinar los conocimientos y las experiencias disponibles al Municipio, a fin de brindar ayuda en la toma de decisiones en materia de seguridad. Éste podrá obtener asesoramiento de otros Municipios o asistir a capacitaciones para incrementar el conocimiento sobre esta materia.

TÍTULO V: POLÍTICA DE USO DE MEDIOS REMOVIBLES Y DISPOSITIVOS MÓVILES

Artículo 12: El objetivo de la presente política es mantener un estándar de seguridad coherente con el fin de establecer las normas que regulen el uso de los dispositivos móviles y medios removibles, dentro y fuera de la Municipalidad, permitiendo minimizar los riesgos asociados a estos y con el fin de evitar incidentes de seguridad con los datos contenidos en estos.

Los dispositivos móviles y medios removibles permiten facilitar las actividades relacionadas con la Municipalidad, no obstante, el uso de dichos dispositivos también implica algunos riesgos, que deben ser analizados y gestionados. Principalmente tener el cuidado de asegurar que la información institucional no se vea comprometida, evitando así la divulgación, modificación o la destrucción no autorizada de la información almacenada y/o procesada en ellos.

Esta política se aplica a todas las áreas de la Municipalidad y a todos los procesos de provisión de bienes y servicios, normando la utilización de medios removibles (conectados por puerto USB, bluetooth u otro medio) y dispositivos móviles que son entregados por la Municipalidad a los usuarios (funcionarios, colaboradores, practicantes o personal externo que preste servicios permanentes o temporales, y/o aquellos utilizados dentro de las dependencias de la Municipalidad), específicamente y sin ser la siguiente una lista taxativa:

- Pendrive.
- Discos duros portátiles.
- Dispositivos de banda ancha móvil.
- Teléfonos móviles.
- Tabletas.
- Cámaras fotográficas.
- Grabadora de audio.
- Cámara de video.

Los medios removibles no son alternativa de respaldo de información de la Municipalidad, siendo responsabilidad del usuario almacenar y mantener la información en la nube institucional o almacenamiento autorizado. Está restringido el uso de dispositivos de almacenamiento removibles conectados a puertos USB tales como discos externos, celulares, cámaras, etc., exceptuando aquellos dispositivos necesarios para la operación como mouse, teclados, impresoras que únicamente poseen puerto USB como mecanismo de conexión a la red y también exceptuando el uso de estos dispositivos por parte del administrador de red. Se incluyen en esta política equipos que, mediante una solicitud, se deriva al Encargado de Seguridad de la Información y Ciberseguridad para que autorice su acceso.

Se debe contar con protección para evitar el acceso no autorizado o la divulgación de la información almacenada y procesada por estos dispositivos, protegiendo el acceso con claves, tokens, huella digital o el mecanismo que permita el dispositivo.

Los usuarios deben dar un buen uso a los medios removibles y dispositivos móviles asignados para el cumplimiento de sus funciones y en caso de que éstos presenten cualquier deterioro o evento de seguridad, deben informarlo oportunamente al encargado de Seguridad de la Información y Ciberseguridad.

En caso de pérdida o robo del equipamiento asignado por la Municipalidad, el usuario afectado, debe informar a su jefatura directa y posteriormente a Carabineros de Chile dejando en la constancia del robo o pérdida la información relativa al equipo (marca, característica, número de serie).

Artículo 13: el marco de utilización de los dispositivos móviles y medios removibles de almacenamiento será el siguiente:

a) Los dispositivos móviles y medios removibles son asignados a los funcionarios para apoyar la relación de su trabajo y deben ser utilizados solamente para estos fines.
b) Los usuarios que hagan uso de su móvil personal para apoyar su trabajo, deben tomar los resguardos que estén a su alcance, en relación a tener el cuidado de asegurar que la información institucional no se vea comprometida, evitando así la divulgación, modificación o la destrucción no autorizada de la información almacenada en el móvil.
c) El uso de un medio removible debe ser autorizado y justificado por la jefatura directa del usuario, quien debe solicitarlo por correo electrónico al Encargado de la Seguridad de la Información y Ciberseguridad, quien una vez que reciba este requerimiento, habilitará el acceso al medio removible.

d) La asignación de un medio removible debe ser autorizado, justificado y solicitado por la jefatura directa del usuario por correo electrónico al Encargado de la Seguridad de la Información y Ciberseguridad quien evaluará que se cumpla con el estándar asignado para este tipo de medio, el que, en caso de contar con disponibilidad, será asignado al usuario, previa firma de recepción conforme, y registrado en el sistema de activos.
e) Es responsabilidad de cada usuario el buen uso y traslado de los dispositivos que tiene a su cargo.
f) Es responsabilidad de cada jefatura que solicita uso de medio removible y asignación de medio removible resguardar que el funcionario a su cargo realice un buen uso y cuidado en el traslado de los dispositivos a cargo.
g) Los dispositivos móviles y medios de almacenamiento removibles no se deben exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).
h) Cualquier falla o deterioro de los componentes o dispositivos móviles asignados, debe ser informada la jefatura directa, que informará a su vez por correo electrónico al Encargado de la Seguridad de la Información y Ciberseguridad.

Artículo 14: Respecto del uso de los teléfonos móviles, se deben seguir las siguientes directrices:
a) Los usuarios deben evitar la difusión de información confidencial o privada por vía telefónica cuando se está en lugares públicos o fuera de las dependencias de la Municipalidad. Si se hace, se debe procurar tratar los temas en forma general y sin mencionar información sensible o confidencial.
b) Los usuarios deben procurar no almacenar información confidencial en los teléfonos móviles institucionales. Asimismo, y entendiendo que, dado el uso del teléfono móvil institucional, existe la posibilidad de que terceros accedan a la información contenida en él, se sugiere la utilización de claves de acceso al equipo con un número limitado de intentos, de manera de minimizar el riesgo de acceso no autorizado.
c) Los usuarios no deben participar de juegos, concursos, cadenas u otros similares, utilizando el teléfono móvil otorgado por la Municipalidad.
d) Es responsabilidad del usuario dar buen uso y cuidado al teléfono móvil asignado.
e) Los usuarios no deben exponer el teléfono móvil a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).
f) El Encargado de la Seguridad de la Información y Ciberseguridad deberá resguardar que los equipos proporcionados por la Municipalidad tengan, por defecto, bloqueados los servicios de mensajería de texto y roaming internacional.
g) Cuando un equipo móvil es utilizado en lugares públicos o privados, y es conectado a una red no administrada por la Municipalidad, el usuario de dicho equipo es responsable de la seguridad física y lógica del mismo y de la información que comparta con terceros a través de dicha red.
h) Terceras personas no están autorizadas a utilizar el dispositivo móvil que la Municipalidad asigne a un usuario
i) El usuario debe seguir las indicaciones de los fabricantes tanto en la utilización y actualización, como en el cuidado del equipo móvil asignado para el cumplimiento de sus funciones.

Artículo 15: Respecto del uso de cámaras fotográficas, de video y grabadoras, se deben seguir las siguientes directrices:
a) Para los dispositivos que ya estén en la institución y que han sido asignado a usuarios, no se deben exponer a condiciones ambientales que puedan afectar su buen funcionamiento (humedad, temperatura, etc.).
b) El usuario debe cuidar el equipamiento y guardarlo en lugares seguros cuando no lo esté utilizando, preferentemente muebles con llave.
c) El usuario debe seguir las indicaciones de los fabricantes tanto en la utilización como en el cuidado del equipo

TÍTULO VI: POLÍTICA DE USO DE INTERNET, CORREO ELECTRÓNICO INSTITUCIONAL, INSTALACIÓN Y USO DE SOFTWARE

Artículo 16: Todo usuario de la Municipalidad deberá poseer una cuenta de usuario personal, que actuará como credencial que lo identifique unívocamente, y que le permita tener acceso a los recursos de la red informática institucional. Para todo sistema informático de la Municipalidad, el usuario debe señalar quién es (identificación) y luego debe comprobar que es quien dice ser (autenticación). La identificación se realizará normalmente por un "nombre de usuario" que permite acceso el sistema informático de la institución y la autentificación se realiza mediante algo que solo el usuario conoce (contraseña) y que es algo que solo él posee.

Es importante señalar que el uso inapropiado de software, expone a la Municipalidad contra riesgos legales y de seguridad informática, tales como la pérdida de información, filtración de datos, infracción de derechos de autor, exposición de los sistemas de uso interno a códigos maliciosos, interrupciones o degradación de servicios de red, suplantación de identidad, daños de sistemas, entre otros.

Lo anterior es aplicable a todos los funcionarios, personal a honorarios y contrata, ayudantes, que utilicen equipamiento computacional inventariado por la Municipalidad o que hayan sido adquiridos por medio de proyectos, programas, en las mismas condiciones de seguridad y control que un equipo computacional inventariado.

Artículo 17: Sobre el uso de Internet deberán seguirse las siguientes directrices:

a) Los sistemas de comunicación y acceso a Internet de la Municipalidad, deberán ser utilizados exclusivamente como una herramienta de trabajo conforme a las funciones de trabajo establecidas por la institución y no para actividades personales.
b) Los usuarios de la Red Municipal deben utilizar, como primera opción para conectarse a Internet, los medios dispuestos por la propia Municipalidad. De existir problemas con la conexión principal, los usuarios pueden acceder a través de otros canales de proveedores de servicios de Internet externos.
   Cuando se use la opción alternativa, esta debe ser resguardada con medidas de seguridad tales como firewall entre la institución y la salida a Internet, equipos de escritorio actualizados en cuanto a antivirus, firewall del equipo, antimalware y parches de seguridad. Todas herramientas que serán provistas e instaladas por el Encargado de Seguridad de la Información y Ciberseguridad.
c) Las operaciones realizadas a través de Internet por los usuarios de la Municipalidad podrán ser intervenidas y auditadas, tanto por el Encargado de Seguridad de la Información y Ciberseguridad, debidamente autorizado por el Alcalde de la comuna o el Director de Control Interno de la Municipalidad, en cuanto a los accesos realizados en la red, a internet y el contenido de lo accedido.
d) Las soluciones inalámbricas deben contar con portales cautivos para que los invitados o externos de la Municipalidad que necesiten conexión a Internet solo puedan usar de manera controlada este medio, además de asegurar que la red de trabajo de la institución se mantenga aislada de los mismos.
e) Toda información entrante y saliente a Internet, es monitoreada y registrada por el Encargado de Seguridad de la Información y Ciberseguridad, con el propósito de garantizar el nivel de servicio de navegación a internet y priorizando las comunicaciones que la institución requiere mantener con otras entidades gubernamentales y privadas, necesarias para el funcionamiento de los Sistemas Informáticos.
f) Los usuarios de la Municipalidad no deben almacenar contraseñas en los navegadores web.
g) El Encargado de Seguridad de la Información y Ciberseguridad debe asegurarse que el sitio web institucional cuente con su correspondiente certificado de seguridad.

Artículo 18: Sobre el uso de cuentas de usuario y contraseñas deberán seguirse las siguientes directrices:

a) El usuario es responsable del mantenimiento de la seguridad tanto de su propia información como de sus cuentas asignadas y contraseñas.
b) Las cuentas y contraseñas son asignadas a usuarios individuales y no pueden ser compartidas con otras personas o funcionarios de Municipalidad ni con externos a la institución. Los usuarios son responsables también por el tráfico y el contenido de la información de las cuentas asignadas. La violación de una cuenta y contraseña puede conllevar la revocación de cualquier tipo de privilegio de uso.
c) El uso de la red se encuentra disponible para todos los funcionarios de la Municipalidad, pero los permisos para el uso de Internet, estarán limitados por la necesidad de acceso que requiera el desarrollo de la función de cada funcionario o según lo soliciten los jefes de la institución al Encargado de Seguridad de la Información y Ciberseguridad.
d) La asignación de perfiles de usuario es realizada por cada Director, de acuerdo al perfil de cargo de cada funcionario, este perfil de usuario es informado al Encargado de Seguridad de la Información y Ciberseguridad, quien realizará la asignación de privilegios de acuerdo a lo indicado por cada jefatura.

Artículo 19: Respecto de las restricciones al uso de Internet, se deben seguir las siguientes directrices:

a) Se prohíbe descargar desde Internet, material que infrinja el Ordenamiento Jurídico Nacional o en la normativa interna establecida en la Municipalidad.

b) No está permitido almacenar información institucional en sitios o nubes de almacenamiento virtual provisto por terceros (Dropbox, etc.), la institución provee de recursos específicos para ello y contratos asociados.
c) No está permitido copiar y distribuir software que secretamente recoge o difunde información acerca de la institución.
d) No está permitido utilizar los equipos computacionales entregados por la Municipalidad para actividades no relacionadas con las asignadas a su función. El cumplimiento de estas restricciones, se regularán de acuerdo al perfil de cada Usuario, en particular se debe evitar:
    a. Descargar sistemas de audio/video vía Internet (radios online, Spotify, Netflix, entre otros). Se excluyen de esta condición a los medios de prensa de la institución.
    b. Cargar y/o descargar archivos de música.
    c. Cargar y/o descargar archivos de imágenes y videos.
    d. Cargar y/o descargar juegos o jugar juegos online.
    e. Instalar sistemas de telecomunicaciones ajenos a los corporativos.
    f. Construcción y/o hosting de sitios web personales o ajenos a la institución.
    g. Transferencia de archivos a través de protocolo SFTP, FTP, u otros no autorizados bajo convenios de interoperabilidad.
    h. Está prohibido ingresar a páginas con contenidos pornográficos, pedófilos y otros relacionados.
e) Cuando el usuario requiera el acceso a un sitio que se encuentre bloqueado, debe ser autorizado y solicitado por la jefatura directa vía correo electrónico al Encargado de Seguridad de la Información y Ciberseguridad, quien evaluará que el sitio no esté catalogado como malicioso, en lista negra o vulnere una política de seguridad, antes de dar acceso al usuario. Los casos que no entren en la anterior clasificación, serán evaluados y revisados por el Encargado de Seguridad de la Información y Ciberseguridad.
f) En cuanto al uso de redes sociales, están autorizadas sólo para los funcionarios que sus funciones se relacionen con comunicaciones y fiscalizaciones internas de la Municipalidad o cuando su jefatura lo disponga.

Artículo 20: Sobre el uso del correo electrónico institucional, se deben seguir las siguientes directrices:

a) Está prohibido el uso de correos personales para fines laborales, solo se debe utilizar las herramientas provistas por la Municipalidad para la comunicación electrónica. Ocasionalmente los funcionarios utilizarán los sistemas de correo electrónico para propósitos personales siempre y cuando esto no interrumpa el normal desarrollo de sus funciones. Esto está permitido siempre que no afecte el trabajo para el cual fue contratado ni su contenido pueda afectar negativamente a los intereses y/o lineamientos generales de la institución. Es importante que se tenga en cuenta que este tipo de comunicación se genera bajo el nombre de la Municipalidad y esto puede afectar la imagen de la institución.
   El uso de correos electrónicos es un recurso compartido, por lo tanto, los mensajes y archivos personales deben manejarse en el rango mínimo de almacenamiento de espacio.
b) Los correos electrónicos enviados y recibidos están almacenados en los equipos informáticos de la Municipalidad y serán retenidos por el tiempo necesario de acuerdo a criterios legales y administrativos.
   Correos personales no deben estar archivados en el sistema por más tiempo del estrictamente necesario.
c) Toda casilla de correo electrónico institucional está directamente vinculada al funcionario y es responsable del contenido y de los archivos adjuntos a cada mensaje.
d) El resguardo de las claves de acceso al correo electrónico es de exclusiva responsabilidad del funcionario, no se deben divulgar, compartir ni anotarlas en lugares visibles y/o de fácil acceso.
e) Los funcionarios tienen prohibido intentar acceder en forma no autorizada a la cuenta de correo de otro usuario y tratar de tomar su identidad, salvo su expresa autorización escrita.
f) Los funcionarios de la Municipalidad deberán usar un lenguaje respetuoso en sus mensajes con usuarios internos o externos y estos mensajes de ninguna forma podrán ser de contenido difamatorio, insultante, injurioso, amenazados, ofensivo, obsceno, racista o sexista.

Artículo 21: Toda información de la Municipalidad no debe ser compartida con terceros sin la debida autorización de la respectiva Jefatura y Encargado de Seguridad de la Información y Ciberseguridad. Siempre se debe tener en cuenta que existe un alto riesgo de intercepción de la información, por esta razón se recomienda no enunciar el contenido de información confidencial o sensible en el título de un correo electrónico.

Cualquier información que contenga datos personales o información sensible, debe ser encriptada con una contraseña para su envío, la que se entregara por parte del remitente vía telefónica, sin dejar registro escrito de ella en el correo electrónico. Si los Usuarios tienen dudas respecto a la información que se enviará, debe consultar con su jefatura o con el Encargado de Seguridad de la Información y Ciberseguridad.

Artículo 22: El funcionario debe identificar en el correo sus datos (nombre, apellido, unidad) para que el receptor del mensaje identifique con certeza la identidad del remitente y la unidad de su procedencia. Para la utilización del web mail solo podrá ser accedido mediante la herramienta institucional provista para acceder a los recursos informáticos desde cualquier lugar o equipo con conexión a internet con la cuenta de usuario que se utiliza para el acceso al sistema informático de la Municipalidad.

Artículo 23: Si un funcionario se ausenta de sus labores por un tiempo considerable (uso de feriado legal, licencias médicas, Comisión de servicio, etc.), debe dejar su correo electrónico con respuesta automática, donde comunique que estará ausente por un periodo de tiempo, especificando las fechas e indicando el nombre y correo electrónico del funcionario que lo reemplazará.

Artículo 24: La creación de cuentas genéricas, destinada a representar un servicio de envío de mensajería electrónica colectiva, se gestionará a través de la jefatura del área solicitante, quien lo requerirá vía correo electrónico al Encargado de Seguridad de la Información y Ciberseguridad, con un mínimo de dos días hábiles de aviso para gestionarla. Las cuentas genéricas no reemplazan a ningún correo electrónico de funcionario, solo se utilizan como listas de distribución masiva.

Artículo 25: Respecto a las restricciones en el uso del correo electrónico y su contenido, se deben seguir las siguientes directrices:

a) Los usuarios deben respetar la naturaleza confidencial de los datos que puedan ser de su conocimiento ya sea como parte de su trabajo o accidente.
b) El funcionario tiene prohibido el uso de seudónimos u otros sistemas para ocultar su identidad. En todos los mensajes debe estar claramente identificado el origen y propietario del mensaje.
c) Se prohíbe el envío de publicidad o cualquier información de tipo comercial por correo institucional.
d) Los mensajes contenidos en el correo institucional no podrán ser contrarios a las disposiciones del orden público y al respeto de los derechos fundamentales de las personas.
e) No se debe enviar por correo institucional, contenidos que no tengan relación con el trabajo o que excedan al tamaño asignado tales como videos, imágenes, archivos de audio (mp3), etc., a fin de no sobrecargar la red institucional.
f) Se prohíbe utilizar la cuenta de correo electrónico institucional para emitir opiniones en foros de discusión externas a la institución, listas temáticas u otras instancias de naturaleza polémica, que pueda crear conflictos al interior de la institución.
g) El usuario de correo electrónico institucional debe evitar la instalación y ejecución de archivos adjuntos que sean desconocidos, cualquier duda que tenga respecto de la seguridad de algún adjunto, debe consultarla al Encargado de Seguridad de la información y Ciberseguridad.
h) El uso del listado de contactos difundidos por los sistemas de la institución es solo para consultas y de uso exclusivo dentro de la Municipalidad. Este prohibido difundir cualquier listado (ejemplo: correos, teléfonos u otro tipo de información publicada) por cualquier medio electrónico o impreso para propósitos que no sean de uso institucional.

Artículo 26: Si las necesidades de la institución obligan al envío de información reservada, sensible o privada mediante el sistema de correo, los usuarios deben enviarlo únicamente a las personas que lo requieren. Es importante considerar que un mensaje de correo electrónico puede ser impreso o reenviado a personas no autorizadas.

Artículo 27: Será incluido en el pie de firma de cada correo electrónico información sobre el resguardo de confidencialidad de los datos personales de los funcionarios y usuarios municipales, así como la información institucional del Municipio que permita desincentivar la filtración de información.

Artículo 28: Sobre uso del correo electrónico en caso de desvinculaciones, renuncias y otras situaciones similares, deberá estarse a las siguientes directrices:

a) La repartición encargada de recursos humanos de la Municipalidad, informará mediante correo electrónico institucional al Encargado de Seguridad de la Información y Ciberseguridad, cuando un funcionario sea desvinculado.
b) Se procederá a respaldar y deshabilitar la cuenta de correo electrónico institucional e informará a través de respuesta automática que el usuario ya no pertenece a la institución, acompañado de los

datos de contacto de la persona que lo reemplace. El contenido del correo respaldado será resguardado como información institucional

c) La deshabilitación de la cuenta de correo electrónico, será por un periodo de 6 meses, al término de este periodo, la cuenta será cerrada.

Artículo 29: Respecto al uso e instalación de software en los equipos institucionales, deberán seguirse las siguientes directrices:

a) Todo software debe ser instalado por el personal autorizado de la municipalidad, lo cual debe ser revisado en forma periódica.
b) Los funcionarios no pueden descargar software desde internet, o traer el software de su casa sin autorización.
c) Cuando un funcionario detecta la necesidad de utilizar un software en particular, debe solicitarlo a su jefatura directa, quien mediante correo electrónico envía solicitud de evaluación al Encargado de Seguridad de la Información y Ciberseguridad.
d) Los privilegios para la instalación de software por parte de los usuarios deben ser limitados a un mínimo, estos privilegios deben ser revisados cada cierto tiempo, ya que un funcionario puede cambiar de área, departamento.
e) El Encargado de Seguridad de la Información y Ciberseguridad tiene que determinar si la Municipalidad tiene licencia del programa solicitado. Si no existe licencia, notifica al funcionario.
f) No se podrá instalar software protegido por derechos de autor, sin la respectiva licencia en los equipos computacionales que estén inventariados por la Municipalidad, con la excepción de licencias que permitan su uso y distribución libre.
g) Los requerimientos de instalación de software que no cuenten con una licencia valida, deberán ser canalizados formalmente a través de la jefatura directa al que está adscrito el funcionario, quien deberá escalar y evaluar el requerimiento junto al Encargado de Seguridad de la Información y Ciberseguridad para analizar si existen alternativas de software libre, si es posible asignar una licencia disponible o se gestiona la compra.
h) Todos los equipos contarán con una instalación de software básico correspondiente a funciones administrativas como: sistema operativo, software de oficina, antivirus y utilidades de uso libre.

TÍTULO VII: POLÍTICA PARA EL USO DE CONTRASEÑAS

Artículo 30: Esta política se aplica a todas las áreas de la Municipalidad a los procesos de provisión de bienes y servicios definidos. Es aplicable a todos los usuarios ya sean funcionarios de planta, contrata, honorarios, asesores, consultores, practicantes y otros trabajadores, incluyendo empresas que presten servicios y que necesiten tener acceso a los recursos de la red institucional.

Esta política contempla los siguientes controles definidos en la norma NCh-ISO 27001:2013 Uso de información & de autenticación secreta.

Artículo 31: Para el correcto uso de las contraseñas, se deben seguir las siguientes directrices:

a) El nombre de usuario y su contraseña deben ser individuales, es decir, debe ser privada, única e intransferible, no debe ser compartida, el usuario será el único responsable de las acciones efectuadas bajo el uso de su cuenta personal.
b) Se debe mantener la información de autenticación secreta como confidencial, está prohibida su divulgación, sin excepciones.
c) Se debe evitar mantener un registro (es decir, en papel, archivo de software o en un dispositivo de mano) de la información de autenticación secreta.
d) Cada vez que un usuario se ausente de su estación de trabajo, bloquear su computador para proteger el acceso a las aplicaciones, servicios e información de la institución de personal no autorizado.
e) Se debe tener presente que en ningún momento se solicitará contraseñas por correo electrónico o mensaje de texto de modo que debería ignorar cualquier petición recibida por estas vías de comunicación. En caso de que se presente un evento de este tipo se puede reportar al Encargado de Seguridad de la Información y Ciberseguridad.
f) Está prohibido compartir la información de autenticación secreta de usuario, ya sea propia o de un tercero.
g) Se debe evitar escribir la contraseña en computadores públicos, compartidos o aquellos en que se desconozca su nivel de seguridad o se estime que pueda estar monitorizados de forma remota, por ejemplo, desde un cibercafé o un terminal de acceso a internet de un aeropuerto.
h) No emplear la cuenta de identificación y contraseña para registrarse en ningún servicio de redes sociales y/o servicios de almacenamientos online distinto a los dispuestos por la Municipalidad

(Twitter, por ejemplo). Si se expone su cuenta a servicios externos, pueden existir incidentes de seguridad que pueden poner en riesgo su identificación en los sistemas informáticos y los sistemas de la Municipalidad.

Artículo 32: Respecto de la identificación y contraseñas requeridas, se deberán seguir las siguientes directrices:

a) Antes de tener acceso a cualquier recurso de la red de la Municipalidad todos los usuarios deben ser identificados exitosamente mediante su nombre de usuario y su contraseña.
b) Se debe cambiar la información de autenticación secreta cuando exista alguna indicación de su posible compromiso de seguridad.
c) Aparte de cambiar la clave en forma semestral, es recomendable cambiarla de forma periódica la contraseña (cada 3 meses), dado que esto ayudara a prevenir accesos no autorizados a la cuenta de usuario asignada por la institución. En caso de que existan problemas con el cambio de contraseña se puede solicitar apoyo al Encargada/o de Seguridad de la Información.
d) Los usuarios no deben emplear la misma contraseña que usan para la cuenta de la Municipalidad en otros servicios o aplicaciones (Por ejemplo: cuenta de correos electrónicos personales, redes sociales, aplicaciones móviles, entre otros).
e) Evitar el autoguardado de contraseñas en los exploradores de internet o en cualquier aplicación que lo solicite.
f) Se sugiere seleccionar contraseñas con una longitud mínima suficiente (que tenga como mínimo 8 caracteres) y posean las siguientes características:
    a. Fáciles de recordar.
    b. Pueda contener al menos un símbolo y una letra mayúscula. Como, por ejemplo:
        i. Símbolos de Teclados i@-%&.,0 i?1,
        ii. Letras Mayúsculas A, B, C, D, E, F, G
    c. Que no se basen en nada que otra persona pueda adivinar u obtener fácilmente mediante la información relacionada con la persona, es decir, nombres, números de teléfono y fechas de nacimiento, etc.
    d. Que no sean vulnerables a ataques de diccionario (es decir, que no conste de palabras incluidas en los diccionarios).
    e. Que estén libre de caracteres idénticos consecutivos, que sean todos numéricos o alfabéticos.

2. **PUBLÍQUESE**, en la plataforma de transparencia activa, relativa a "Otros Antecedentes", sección "Reglamentos";

3. **ESTABLÉZCASE** que este reglamento entrará en vigencia, una vez totalmente tramitado el presente acto administrativo;

Anótese, Comuníquese y Archívese.

I. MUNICIPALIDAD DE COINCO SECRETARIO MUNICIPAL

ALEJANDRO AGUIRRE CUADRA
SECRETARIO MUNICIPAL
ILUSTRE MUNICIPALIDAD DE COINCO

I. MUNICIPALIDAD DE COINCO ALCALDE

JUAN ABARCA PADILLA
ALCALDE
ILUSTRE MUNICIPALIDAD DE COINCO

JAD/jad
Distribución:
Dirección de Control
Dirección de Administración y Finanzas
Secretaría Municipal

DIRECCIÓN DE CONTROL V°B° I. MUNICIPALIDAD DE COINCO