Municipalidad de
Tierra Amarilla
22 Diciembre 1891

DIRECCION DE ADMINISTRACION Y FINANZAS

APRUEBA POLITICA DE SEGURIDAD DE LA INFORMACION Y MANUAL DE CREACION Y ACTUALIZACION DE CONTRASEÑAS __/

DECRETO N.° 2796 **/**

TIERRA AMARILLA, 09 DIC 2022

V I S T O S :

1. Acta de Instalación del Concejo Municipal, periodo 2021-2024 de Tierra Amarilla y las facultades que me confiere la Ley N°18.695 de 1988 "Orgánica constitucional de Municipalidades y sus modificaciones posteriores".
2. El Decreto Alcaldicio N°1164 de fecha 29 de junio del año 2021, que reconoce el acta de proclamación del tribunal electoral de atacama, que señala que don Cristóbal Zúñiga Arancibia es electo como Alcalde de la Ilustre Municipalidad de Tierra Amarilla en el periodo alcaldicio que indica.
3. Norma Chilena 2777, sobre Tecnología de la información - Código de práctica para la gestión de seguridad de la información.
4. Decreto N° 83 de fecha 12 de Enero del 2005, Aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.
5. Ley 21.180 Transformación Digital del Estado de fecha 11 de Noviembre del 2019.
6. Ley 21.464 que modifica diversos cuerpos legales, en materia de transformación digital del estado, del 09 de Junio del 2022.
7. Decreto Alcaldicio N°2529 del 17/12/2021, que aprueba el Programa anual de Mejoramiento de la gestión Municipal de la Ilustre Municipalidad de Tierra Amarilla para el año 2022.
8. Ley N°21.395, Ley de Presupuesto del Sector Público correspondiente al año 2022.

C O N S I D E R A N D O:

1.- Que, la norma Chilena 2777, indica en el punto 4.1.1 que se debe considerar la conformación de un Comité para la Gestión de la Seguridad de la información.
2.- Que, la Ley N° 19.880, que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado.
3.- Que, la Ley N°21.180 sobre Transformación Digital del Estado, que implica que cada proceso administrativo debe orientarse a ser gestionado de una forma electrónica y que establece un estándar de uso de los medios tecnológicos (Sistemas Informáticos), internet, equipos computacionales y medios digitales, tratando de prevenir incidentes que puedan desencadenar en posibles riesgos o pérdida de información sensible.
4.- Que, en el articulo N° 12 del Decreto N° 83, el cual aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

D E C R E T O:

1.- : **APRUEBASE** La Política de Seguridad de la Información en base a la Ley N°21.180 sobre Transformación Digital del Estado, que implica que cada proceso administrativo debe orientarse a ser gestionado de una forma electrónica y que establece un estándar de uso de los medios tecnológicos (Sistemas Informáticos), internet, equipos computacionales y medios digitales, tratando de prevenir incidentes que puedan desencadenar en posibles riesgos o pérdida de información sensible

2.- : **APRUEBASE** Manual de Creación y Actualización de Contraseñas el cual Garantiza la integridad, confidencialidad y disponibilidad de toda la información perteneciente a la Ilustre Municipalidad de Tierra Amarilla asegurando la continuidad de los servicios de la Institución frente a incidentes.

3.- NOMBRASE a un Encargado de Seguridad de la información, según el articulo N°12 del Decreto N° 83, que aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos.

4.- NOMBRASE a los integrantes del Comité de Seguridad de la información, según lo establece la normativa vigente.

ANOTESE, COMUNIQUESE Y ARCHIVESE

I. MUNICIPALIDAD DE TIERRA AMARILLA
SECRETARIO MUNICIPAL Y ALCALDE

MARCIA LATORRE MORENO
SECRETARIA MUNICIPAL
MINISTRA DE FE

I. MUNICIPALIDAD DE TIERRA AMARILLA
ALCALDE

CRISTOBAL ZUÑIGA ARANCIBIA
ALCALDE

CZA/EVD/MLM/AMQH/LGA/cmb.

Distribución:
- Siaper
- Oficina TIR
- Archivo

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

OCTUBRE DE 2022

CRISTIAN MONTENEGRO BARRAZA – INGENIERO EN INFORMÁTICA
MANUEL YAÑEZ CABRERA – TÉCNICO EN INFORMÁTICA

ILUSTRE MUNICIPALIDAD DE TIERRA AMARILLA

Oficina de Tecnologías de la Información y Comunicación

Contenido

1. Introducción

La Política de alto nivel y/o Política general de Seguridad de la Información, aborda la necesidad de la implementación de un sistema de gestión de seguridad de la información (SGSI) en base a la Ley N°21.180 sobre Transformación Digital del Estado, que implica que cada proceso administrativo debe orientarse a ser gestionado de una forma electrónica, para que de esta manera se mejoren los tiempos de los procesos administrativos, que la documentación sea almacenada y resguardada con estándares que eviten la pérdida de información, y por sobre todo que los usuarios principales de nuestro Municipio, sean atendidos con mayor eficiencia.

Es así, teniendo en cuenta la importancia que tiene que la Oficina de Tecnologías de la Información y Comunicación (TIC) defina las necesidades de sus grupos de interés y la valoración de los controles precisos para mantener la seguridad de la información, se establece una política que tenga en cuenta el marco general del funcionamiento de la Ilustre Municipalidad de Tierra Amarilla, sus objetivos institucionales, sus procesos misionales y que este adaptada a las condiciones específicas y particulares de cada una según corresponda para que sea aprobada y guiada por la Dirección.

De esta forma, una buena política es concisa, fácil de leer y comprender, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción. Son cortas, y enmarcan los principios que guían las actividades dentro del Municipio.

2. Objetivos

2.1 Objetivo General

Establecer un estándar de uso de los medios tecnológicos (Sistemas Informáticos), internet, equipos computacionales y medios digitales, tratando de prevenir incidentes que puedan desencadenar en posibles riesgos o pérdida de información sensible.

2.2 Objetivo Específico

Garantizar la integridad, confidencialidad y disponibilidad de toda la información perteneciente a la Ilustre Municipalidad de Tierra Amarilla garantizando la continuidad de la Institución frente a incidentes.

3. Alcance

Esta política de seguridad incluye a todo el personal que tiene a su cargo algún equipo computacional que trabaje con algún sistema informático, correo corporativo, o que administre el sitio web corporativo de nuestro Municipio y/o que tenga acceso a la red de datos de esta institución.

4. Definiciones

Política: Declaración de alto nivel que describe la posición de la entidad sobre un tema específico.

Estándar: Regla que especifica una acción o respuesta que se debe seguir a una situación dada. Los estándares son orientaciones obligatorias que buscan hacer cumplir las políticas. Los estándares son diseñados para promover la implementación de las políticas de alto nivel de la entidad antes de crear nuevas políticas.

Mejor Práctica: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Guía: Una guía es una declaración general utilizada para recomendar o sugerir un enfoque para implementar políticas, estándares y buenas prácticas. Las guías son esencialmente, recomendaciones que deben considerarse al implementar la seguridad. Aunque no son obligatorias, serán seguidas a menos que existan argumentos documentados y aprobados para no hacerlo.

Procedimiento: Los procedimientos, definen específicamente como las políticas, estándares, mejores prácticas y guías que serán implementadas en una situación dada. Los procedimientos son independientes de la tecnología o de los procesos y se refieren a las plataformas, aplicaciones o procesos específicos. Son utilizados para delinear los pasos que deben ser seguidos por una dependencia para implementar la seguridad relacionada con dicho proceso o sistema específico. Generalmente los procedimientos son desarrollados, implementados y supervisados por el dueño del proceso o del sistema, los procedimientos seguirán las políticas de la entidad, los estándares, las mejores prácticas y las guías tan cerca como les sea posible, y a la vez se ajustarán a los requerimientos procedimentales o técnicos establecidos dentro del a dependencia donde ellos se aplican.

Información: Se denomina al conjunto de datos organizados y procesados que funcionan como mensajes, instrucciones y operaciones o cualquier otro tipo de actividad que tenga lugar en una computadora.

Auditoría: La verificación independiente de cualquier actividad o proceso. Esta actividad persigue la mejora continua de los procesos internos del área auditada.

Firewall: Dispositivo o programa que controla el flujo de tráfico entre redes.

Identificación: Los medios por los cuales un usuario reclama una identidad especifica sin validación a un sistema.

Activo: Un recurso, procedimiento, sistema u otra cosa que tenga un valor para una organización y por lo tanto deba de ser protegida, los Activos pueden ser bienes físicos tales como equipos de cómputo y maquinaria, también puede ser la Información y propiedad intelectual.

Antivirus: Software diseñado para la detección, prevención y eliminación de Software mal intencionado o dañino para los sistemas.

Ataque Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Delito Informático: Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Encriptación: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Router: Enrutador, dispositivo que permite enviar o encaminar paquetes de datos en una red a otra, es decir interconectar subredes.

Switch: Conmutador, dispositivo que permite interconectar dos o más segmentos de red.

5. Política

5.1.1 Definición de la Política de Seguridad de Información

La Oficina de Tecnologías de la Información y Comunicación (TIC), entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de una Política de Seguridad de la Información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de este Municipio.

Para la Oficina de Tecnologías de la Información y Comunicación (TIC) de la Ilustre Municipalidad de Tierra Amarilla, la protección de la información busca la disminución del impacto generado sobre sus activos de información por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.
De acuerdo con lo anterior, esta política aplica a la Ilustre Municipalidad de Tierra Amarilla, según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes del Municipio.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes de la Ilustre Municipalidad de Tierra Amarilla.
- Garantizar la continuidad de la Institución frente a incidentes.
- Definir, implementar, operar y mejorar de forma continua una Política de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de la Institución y a los requerimientos regulatorios.

Finalmente es de gran ayuda incluir la descripción general de otras políticas relevantes para el cumplimiento de los objetivos planteados dentro del proyecto de esta Política de Seguridad de la Información. Además, éstas deben ser descritas de forma sencilla, puntual y muy efectiva.

5.1.2 Alcance / Aplicabilidad

Todo el personal de la Ilustre Municipalidad de Tierra Amarilla y sus dependencias, funcionarios, contratistas, terceros y a la ciudadanía en general.

5.1.3 Nivel de Cumplimiento

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a esta política en su totalidad.

A continuación, se establecen 12 puntos base que serán los que darán forma a esta Política de Seguridad de la Información:

1.- La Oficina de Tecnologías de la Información y Comunicación (TIC) ha decidido definir, implementar y actualizar esta Política de Seguridad de la Información, de acuerdo con lo que exija la ley vigente y además en conjunto al avance tecnológico que día a día nos impulsa a mejorar y perfeccionar nuestros procesos internos.

2.- La Oficina de Tecnologías de la Información y Comunicación (TIC) protegerá toda la información generada, procesada y almacenada por los procesos de negocio y activos de información de la Ilustre Municipalidad de Tierra Amarilla.

3.- La Oficina de Tecnologías de la Información y Comunicación (TIC) protegerá la información creada, procesada y transmitida por sus sistemas informáticos con el fin de minimizar impactos financieros, operativos o legales que pudieran generarse debido a un mal uso de esta. Para ello es fundamental la aplicación de controles y monitoreo de procesos de acuerdo con la clasificación de la información, de su propiedad o de su custodia.

4.- La Oficina de Tecnologías de la Información y Comunicación (TIC) protegerá la información de las amenazas que puedan generarse por parte del personal, generando respaldos periódicos y además con un trabajo constante de almacenamiento en la nube de OneDrive en cada equipo.

5.- La Oficina de Tecnologías de la Información y Comunicación (TIC) protegerá las instalaciones de la central de datos, las cuales son críticas y fundamentales para el correcto desempeño del Municipio, además de los activos importantes que resguardan los respaldos de Bases de Datos de todos los sistemas informáticos. La forma de control será vía acceso con clave numérica o con lector de huella dactilar, además de una cámara externa ubicada en la puerta principal, resguardando de esta manera el acceso restringido a las instalaciones.

6.- La Oficina de Tecnologías de la Información y Comunicación (TIC) se encargará de monitorear todos los procesos de negocio del Municipio, garantizando la seguridad de los recursos tecnológicos y de las redes de datos. Dicha supervisión se hará en base a un direccionamiento IP fijo, y

con nombre de cada equipo computacional (referido al usuario de dicho equipo). Se tendrá una constante revisión de la documentación generada y gestionada a través de un Gestor Documental. Además de la capacidad de poder monitorear cada transacción realizada en los sistemas informáticos, de ser requerido.

7.- La Oficina de Tecnologías de la Información y Comunicación (TIC) implementará un control de acceso a la información a través de contraseñas únicas e intransferibles, para los sistemas informáticos y redes de datos.

8.- La Oficina de Tecnología de la Información y Comunicación (TIC) garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información. Dicha seguridad se basa en el uso personal e intransferible de las cuentas de usuario, uso personal de computadores, y además el uso por departamento o por usuario de la nube de Microsoft, lugar en el que se mantiene un respaldo constante de toda la información perteneciente al Municipio.

9.- La Oficina de Tecnologías de la Información y Comunicación (TIC) garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información, tales como: mal uso o divulgación de credenciales de acceso a los sistemas informáticos, abrir correos de remitentes desconocidos, mal utilización de información relevante, difusión de contraseñas de puntos de acceso Wifi sin consentimiento del Municipio, Extracción de información sensible en medios extraíbles, Respaldos semanales de Bases de datos para evitar pérdida de información ante eventuales catástrofes o accidentes.

10.- La Oficina de Tecnologías de la Información y Comunicación (TIC) garantizará la disponibilidad de sus procesos de negocio y la continuidad operacional basado en el impacto que puedan generar los eventos.

11.- La Oficina de Tecnología de la Información y Comunicación (TIC) garantizará el cumplimiento de las obligaciones legales, regulatorias, y contractuales establecidas.

12.- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, contratistas o terceros que tengan un vínculo directo con la Ilustre Municipalidad de Tierra Amarilla.

NOTA: **El incumplimiento a la Política de Seguridad de la Información, traerá consigo, consecuencias legales aplicadas por la Ilustre Municipalidad de Tierra Amarilla, incluido, el marco legal regulatorio del Gobierno de la República de Chile.**

5.1.4 Fase de implementación

Para realizar una correcta implementación de esta Política de seguridad de la información, y de otras Políticas anexas, es necesario cumplir con una serie de fases que se sugieren en este documento, las cuales tienen como objetivo que la Oficina de Tecnologías de la Información y Comunicación (TIC) desarrolle, apruebe, implemente, socialice e interiorice las políticas para un uso efectivo por parte de todos los funcionarios, contratistas y/o terceros de este Municipio.

Para cada institución ya sea pública o privada, es importante contar con políticas de seguridad, ya que es en base a estas, como se guiará el comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad, así mismo las políticas permitirán que la entidad trabaje bajo las mejores prácticas de seguridad y cumpla con los requisitos legales.

Etapas de la Fase de implementación

1.- Desarrollo de la política: Esta etapa será responsabilidad de la Oficina de Tecnologías de la Información y Comunicación (TIC). En esta fase se debe crear la política, estructurarla, escribirla y revisarla; En el contexto del desarrollo de esta política se deben conocer algunos puntos importantes como lo son las actividades de Justificación, Definición de Roles y Responsabilidades, y Aprobación.

- Justificación de la creación de Política: En la actualidad existen innumerables riesgos potenciales que pueden desencadenar en pérdida de información, ya sea voluntaria o involuntaria. Desde eliminación de información sensible por parte de funcionarios, contratistas, entre otros, fallas críticas de discos duros por subas o bajas de voltaje inesperados e inclusive ciber ataques con la intención de dañar el buen funcionamiento de esta institución. Además de factores externos que pueden afectar el correcto desempeño de todos los procesos internos de este Municipio.

- Roles y Responsabilidades: Será responsabilidad de cada director/Jefe/Encargado de unidad, el informar sobre esta política e indicar las posibles consecuencias legales que deriven de su incumplimiento.

- Aprobación de la Política: Tras realizar el análisis de esta política y de someter a votación para su aprobación, se debe aceptar y posteriormente formalizar.

2.- Cumplimiento: En esta etapa se debe asegurar que se interiorice en cada funcionario el cumplimiento de la política y de que se cree una conciencia del buen uso de la información.

3.- Comunicación: Es de vital importancia, no sólo publicar esta o futuras políticas, sino que se deben difundir a través de cada unidad, sobre todo de la oficina de Tecnologías de la Información y Comunicación (TIC) y así dar a conocer en detalle la política a los funcionarios, contratistas y/o terceros del Municipio. Esta fase es muy importante, ya que del conocimiento del contenido de la política depende gran parte del cumplimiento de esta. En esta fase de la implementación se permitirá obtener retroalimentación de la efectividad de la política, permitiendo así realizar excepciones, correcciones y/o ajustes pertinentes.
Todos los funcionarios contratistas y/o terceros de este Municipio deben conocer la existencia de la política, la obligatoriedad de su cumplimiento y la ubicación física de tal documento o documentos, para que sean consultados en el momento que se requiera.

4.- Monitoreo: Es importante que la política sea supervisada por el Encargado de Seguridad de la Información y por un comité de seguridad de la información para determinar la efectividad y cumplimiento de esta, para ello deberán crearse indicadores que permitan verificar de forma periódica y con evidencias que esta política funcione y así ajustarse a la realidad de este Municipio.

5.- Mantenimiento: Esta fase es la encargada de asegurar que la política se encuentre actualizada, íntegra y que contenga los ajustes necesarios y obtenidos de la retroalimentación. Se realizarán formularios con consultas de forma periódica, los cuales serán responsabilidad de la oficina de Tecnologías de la Información y Comunicación (TIC), de esta forma se recabará información necesaria para generar mejoras a la política inicial.

5.1.5 Gestión de Activos de Información

En este apartado se debe hacer referencia a todas aquellas directrices mediante las cuales se indica a los funcionarios los límites y procedimientos frente a la identificación, uso, administración y responsabilidad frente a los activos de Información. La gestión de activos debe contemplar como mínimo:

- **Identificación de Activos:** Se debe determinar la periodicidad con la cual se va a realizar al interior de este Municipio la identificación y/o actualización del inventario de Activos de Información. Se entiende por activo de información a todo archivo digital que haya sido generado al interior de la Ilustre Municipalidad de Tierra Amarilla, Bases de Datos, así como también a todo dispositivo que almacene a su vez estos archivos.

- **Designación de Encargado:** Se debe designar a un Encargado de activo de información, el cual será responsable de realizar la actividad periódica de respaldo, además se debe determinar bajo que instrumento se va a realizar la actividad, dicho instrumento debe permitir identificar el propietario del activo de información.

- **Clasificación Activos:** Se determinan los siguientes tipos de activos de información de acuerdo con la criticidad, sensibilidad y reserva de esta.

CONFIDENCIALIDAD	SENSIBILIDAD	DISPONIBILIDAD
INFORMACIÓN PUBLICA CLASIFICADA	ALTA	MEDIA
INFORMACIÓN PÚBLICA	BAJA	ALTA

Tabla: Criterios de Clasificación.

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.

Tabla 2: Niveles de Clasificación.

- **Etiquetado de la Información:** Se deberá determinar el mecanismo, el responsable y la obligatoriedad para el etiquetado o rotulación de Activos de información. La idea es implementar un instructivo que indique la forma de almacenar y rotular los documentos, por ejemplo un Decreto de pago "DP_001_MUN_PAGOPREVISION05_21062022", esto hace referencia al Decreto de Pago 001 del área Gestión Municipal, referente a pago de previsional mes de Mayo del 2022.

- **Devolución de los Activos:** Se deberá determinar el instrumento y responsable del cumplimiento, mediante el cual se genera obligatoriedad para que los funcionarios, contratistas y/o terceros realicen la entrega de activos físicos y de la información una vez finalizado el empleo, acuerdo o contrato que se tenga con la Ilustre Municipalidad de Tierra Amarilla.

- **Gestión de medios removibles:** Se deberá contemplar los usos y permisos que tienen los usuarios y/o funcionarios de la Ilustre Municipalidad de Tierra Amarilla frente a los medios removibles, entendiendo como medio removible a todos aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. Se debe determinar por cada Director/Jefe/Encargado de unidad en qué casos se autoriza y en

los que no, el uso de medios removibles y los procedimientos en los cuales se determinen las autorizaciones; indicando con algún tipo de documento de respaldo quienes estarán autorizados para la utilización de medios removibles y bajo la supervisión de Jefatura directa. El uso de medios removibles en el Municipio debe ir alineado con las clasificaciones de activos dispuestas en el punto "**Clasificación de Activos**".

- **Disposición de los activos:** Se deberá determinar la obligatoriedad para la construcción y cumplimiento de un procedimiento mediante el cual se realice de forma segura y correcta la eliminación, retiro, traslado o reutilización, cuando ya no se requieran los activos. De esta forma se debe estandarizar la toma de respaldos de los activos evitando así el acceso o borrado no autorizado de la información. El responsable de esto será la Oficina de Tecnologías de la Información
  y Comunicación (TIC), previa instrucción directa de cada Director/Jefe/Encargado de unidad.

5.1.6 Control de Acceso

En este apartado, se hace referencia a todas aquellas directrices mediante las cuales la Oficina de Tecnologías de la Información y Comunicación (TIC) determina los mecanismos de protección, los límites y procedimientos frente a la administración y responsabilidad, relacionados con los accesos a la información, sin importar si estos accesos sean electrónicos o físicos. De tal forma se deberá contemplar como mínimo:

- **Control de acceso con usuario y contraseña:** Se ha elaborado un Manual sobre control de acceso a redes, aplicaciones, y/o sistemas de información de la Ilustre Municipalidad de Tierra Amarilla, mediante la cual se determinen los responsables y los procedimientos formales de autorización de creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas.

- **Suministro del control de acceso:** Se deberá determinar los procedimientos formales y directrices para la gestión de asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados, también deben tenerse en cuenta en esta política los casos especiales como lo son usuarios (ID) con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas informáticos de la Ilustre Municipalidad de Tierra Amarilla.

- **Perímetros de Seguridad:** Se deberán definir los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información a los cuales los funcionarios, contratistas o terceros, tienen acceso y a cuáles no. Además, se deberá definir los responsables de autorizar o no, los ingresos a las áreas delimitadas como de acceso restringido.

5.1.7 No Repudio

Para comprender de una forma clara en que consiste el no repudio, se define lo siguiente, el no repudio en la seguridad de la información es la capacidad de demostrar o probar la participación de las partes (origen y destino, emisor y receptor, remitente y destinatario), mediante su identificación, en una comunicación o en la realización de una determinada acción.

Para garantizar el no repudio en seguridad informática se necesitan establecer los siguientes mecanismos:

Identificación: mecanismo o proceso que provee la capacidad de identificar a un usuario de un sistema.
Autenticación: permite verificar la identidad o asegurar que un usuario es quien dice ser.

La Política de seguridad de la información comprende la capacidad de no repudio con el fin de que los usuarios nieguen haber realizado alguna acción, en base a cuatro puntos importantes:

- **Trazabilidad:** Esta política permitirá que por medio de la trazabilidad de las acciones se haga seguimiento a la creación, origen, recepción, entrega de información y otros.
- **Retención:** Se mantendrán respaldos de la información de cada usuario en la cuenta asignada de la nube de Microsoft. Esto permitirá contar con distintas versiones para cada documento almacenado. Esto en cada caso de asignación de equipos computacionales, deberá ser informado a los funcionarios, contratistas y/o terceros de la Entidad.
- **Auditoría:** La política incluye la realización de auditorías realizadas por el comité de Seguridad de la información, como procedimiento para asegurarse que las partes implicadas nieguen haber realizado una acción. El comité de Seguridad de la información, se recomienda que al menos como inicio sea constituido por: Encargado de Seguridad de la información, Director de Finanzas, Directora de Control, Administrador Municipal y Secretaria Municipal.

- **Intercambio electrónico de información**: La política incluye en los casos que aplique, que los servicios de intercambio electrónico de información son garantía de no repudio.

5.1.8 Privacidad y Confidencialidad

La Política de seguridad de la información contiene una descripción del tratamiento y protección de datos personales que deben ser aplicados, conforme a lo establecido en la normativa vigente. Para que se cumpla con todo lo referente a privacidad y confidencialidad, la política de seguridad de la información cuenta como mínimo con lo siguiente:

Tratamiento de datos personales:

- Principio de la Legalidad: El tratamiento de datos personales debe estar sujeto a lo establecido en la normativa vigente.
- Principio de finalidad: Indicar la finalidad del tratamiento de datos personales, la cual debe ser informada al titular.
- Principio de libertad: El tratamiento sólo puede hacerse con el consentimiento previo, expreso e informado del titular de los datos.
- Principio de veracidad o calidad: La información a tratar debe ser veraz, completa, exacta, actualizada, comprobable y comprensible.
- Principio de transparencia: Garantizar al titular de los datos el derecho a obtener información que le concierna del encargado del tratamiento.
- Principio de acceso y circulación restringida: El tratamiento sólo podrá hacerse por personas autorizadas por el titular o por personas previstas en la normativa vigente.
- Principio de seguridad: La información sujeta a tratamiento, se debe manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Principio de confidencialidad: Todas las personas que participen en el tratamiento de datos Personales deben garantizar la reserva de dicha información.

Derechos de los titulares:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar la prueba de su autorización para el tratamiento de sus datos personales.
- Ser informado respecto del uso que se les da a sus datos personales.
- Revocar la autorización y/o solicitar la supresión de sus datos personales de las bases de datos o archivos cuando el titular lo considere.
- Presentar quejas ante la entidad administrativa encargada de la protección de los datos personales.

Autorización del titular: Esta política indica cómo obtener autorización del titular para el tratamiento de sus datos personales, así como los casos en los cuales no se requiere autorización del titular.

Deberes de los responsables del Tratamiento: Se deberá indicar cuales son los deberes de los responsables y/o encargados del tratamiento de los datos personales.

Para que la aplicación de la Política de Seguridad de la Información se cumpla lo referente a confidencialidad, se deberá firmar un compromiso o acuerdo de confidencialidad, por medio del cual todo funcionario, contratista y/o tercero vinculado a la Ilustre Municipalidad de Tierra Amarilla, se compromete a no divulgar la información interna y externa que conozca del Municipio, así como la relacionada con las funciones que desempeña en la misma.
La firma del acuerdo implica que la información conocida por todo funcionario, contratista y/o tercero, en ninguna circunstancia deberá ser revelada por ningún medio electrónico, verbal, escrito u otro, ni total ni parcialmente, sin contar con previa autorización.
Este documento se deberá firmar al momento de la contratación del funcionario, sea cual sea su calidad contractual, aun cuando sea a honorarios.

5.1.9 Integridad

La Clausula referente a la seguridad de la información debe ser conocida y aceptada por todos los funcionarios, contratistas y/o terceros que sean parte de la Ilustre Municipalidad de Tierra Amarilla, la cual se refiere al manejo íntegro de la información tanto interna como externa, conocida o administrada por los mismos.
De esta manera, toda información verbal, física o electrónica, debe ser adoptada, procesada, entregada y/o transmitida integral, coherente y exclusivamente a las personas correspondientes a través de los medios correspondientes, sin modificaciones ni alteraciones, salvo que así lo determinen las personas autorizadas y/o responsables de dicha información. En el caso de vinculación contractual, el compromiso de administración y manejo íntegro de la información interna y externa para cada funcionario deberá hacerse presente en el momento de la firma del respectivo contrato, bajo la denominación de Cláusula de Integridad de la Información. Además, deberá establecer asimismo la vigencia de la misma acorde al tipo de vinculación del personal al cual aplica el cumplimiento.

5.1.10 Disponibilidad del servicio de información

La Oficina de Tecnologías de la Información y Comunicación (TIC), se comprometerá a cumplir con la continuidad operacional del Municipio con el fin de asegurar, recuperar o restablecer la disponibilidad de los procesos que soportan el Sistema de Gestión de Seguridad de la Información, ante el evento de un incidente de seguridad de la información.

Para cumplir con lo establecido, se tomará en cuenta los siguientes puntos:

- **Niveles de disponibilidad:** Se deberá velar por el cumplimiento de cada servicio y/o información acordados con usuarios de sistemas, proveedores y/o terceros en función de las necesidades del Municipio, los acuerdos de nivel de servicios ofrecidos y evaluaciones de riesgos.
- **Planes de recuperación:** La información almacenada en cada equipo computacional tiene una cuenta de la nube de OneDrive, de esta forma se logra evitar cualquier posible pérdida de información, ya sea voluntaria o involuntaria, así como, referente a catástrofes naturales.
- **Acuerdos de nivel de servicio:** Se debe tener en cuenta los acuerdos de niveles de servicios (ANS) provistos por los proveedores de servicios críticos como lo son Telefónica, Íntesis, Microsoft y CAS Chile. Dentro de los cuales se establecerá como tiempo de resolución de incidentes un período no mayor a 4 horas. Además de atención telefónica de Lunes a Viernes desde las 08:15 hrs. hasta las 19:00 hrs.

5.1.11 Capacitación y Sensibilización en Seguridad de la información

Para asegurar la implementación satisfactoria de esta Política de seguridad de la información, se deben concentrar los esfuerzos en disminuir las vulnerabilidades y amenazas relacionadas con el recurso humano. De esta forma esta política debe contener los siguientes parámetros.

- El compromiso de la alta dirección en destinar los recursos suficientes para desarrollar los programas.
- ¿Quiénes deberán ser entrenados? ¿Quiénes deberán ser sensibilizados?
- Revisión periódica de resultados de capacitaciones para mejoramiento de los procesos.
- Definir los roles y responsabilidades de quienes diseñarán los programas, quienes los comunicarán.
- Documentación sobre planes de estudio y desarrollo de los programas.

- Compromisos y obligaciones por parte del personal capacitado.
- Contener políticas adicionales relacionadas directamente con el debido comportamiento de los usuarios como las siguientes:
  1. Política De Escritorio Limpio.
  2. Política De Uso Aceptable.
  3. Ética Empresarial.

MANUAL DE CREACIÓN Y ACTUALIZACIÓN DE CONTRASEÑAS

OCTUBRE DE 2022

CRISTIAN MONTENEGRO BARRAZA – INGENIERO EN INFORMÁTICA
MANUEL YAÑEZ CABRERA – TÉCNICO EN INFORMÁTICA

ILUSTRE MUNICIPALIDAD DE TIERRA AMARILLA

Oficina de Tecnologías de la Información y Comunicación

Contenido

1. Introducción

Hoy en día la información de toda institución, sea esta privada o pública es el activo más importante, ya que ayuda en la toma de decisiones y además permite evaluar el desempeño de las distintas áreas que la componen a lo largo del tiempo.

Debido a que los sistemas de Información están cada día más presentes en cada institución, se hace vital mantener un almacenamiento, gestión y administración de los datos y además contar con estrategias de alto nivel.

En nuestro Municipio, los Sistemas de información y la Red de conexión a internet enfrentan amenazas de seguridad que incluyen; fraude, espionaje, sabotaje, vandalismo, fuego, robo y posibles inundaciones. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes.

Con el siguiente manual de creación y protección de contraseñas la Ilustre Municipalidad de Tierra Amarilla formaliza su compromiso con el proceso de gestión responsable de información.

2. Objetivos

2.1 Objetivo General

- Garantizar la integridad, confidencialidad y disponibilidad de toda la información perteneciente a la Ilustre Municipalidad de Tierra Amarilla garantizando la continuidad de la Institución frente a incidentes.

2.2 Objetivos Específicos

- Establecer un estándar de uso de contraseñas seguras, la protección de esas contraseñas y su frecuencia de cambios.
- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Fortalecer la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y usuarios de la Ilustre Municipalidad de Tierra Amarilla.

3. Alcance

El alcance de este manual incluye a todo el personal de la Ilustre Municipalidad de Tierra Amarilla que tiene o es responsable de una cuenta de cualquier sistema informático (o cualquier forma de acceso que requiera una contraseña) en cualquier sistema que resida en las instalaciones del Municipio y que tenga acceso a la red y centros de atención.

4. Definiciones

Información: Se denomina al conjunto de datos organizados y procesados que funcionan como mensajes, instrucciones y operaciones o cualquier otro tipo de actividad que tenga lugar en una computadora.

Auditoría: La verificación independiente de cualquier actividad o proceso. Esta actividad persigue la mejora continua de los procesos internos del área auditada.

Firewall: Dispositivo o programa que controla el flujo de tráfico entre redes.

Identificación: Los medios por los cuales un usuario reclama una identidad especifica sin validación a un sistema.

Activo: Un recurso, procedimiento, sistema u otra cosa que tenga un valor para una organización y por lo tanto deba de ser protegida, los Activos pueden ser bienes físicos tales como equipos de cómputo y maquinaria, también puede ser la Información y propiedad intelectual.

Antivirus: Software diseñado para la detección, prevención y eliminación de Software mal intencionado o dañino para los sistemas.

Ataque Web: Es un ataque que se comete contra una aplicación cliente y se origina desde un lugar en la Web, ya sea desde sitios legítimos atacados o sitios maliciosos que han sido creados para atacar intencionalmente a los usuarios de ésta.

Delito Informático: Comportamientos ilícitos que se llevan a cabo mediante herramientas electrónicas para atacar contra la seguridad de los datos informáticos.

Encriptación: Es el proceso para volver ilegible información considera importante. La información una vez encriptada sólo puede leerse aplicándole una clave.

Router: Enrutador, dispositivo que permite enviar o encaminar paquetes de datos en una red a otra, es decir interconectar subredes.

Firewall: Cortafuegos, dispositivo que permite bloquear el acceso no autorizado, como también permitiendo acceso a comunicaciones autorizadas.

Switch: Conmutador, dispositivo que permite interconectar dos o más segmentos de red.

5. Estrategias

5.1 Creación de Contraseñas

5.1.1 La primera contraseña creada para un usuario es creada de forma aleatoria con un sistema automatizado que genera una clave de letras mayúsculas y números con una longitud de 10 caracteres para los sistemas .NET y una longitud de 6 caracteres para los sistemas. BASIC que es lo máximo que soportan estos últimos. El acceso al portal informático se solicita crear mediante correo a la empresa Íntesis y el usuario y clave de los sistemas informáticos pertenecientes al Municipio es creado por personal de la Oficina de Tecnología de Información y Comunicación (TIC).

5.1.2 Cuando el usuario sea forzado a cambiar su contraseña deberá respetar el esquema de utilizar letras mayúsculas y números en su nueva contraseña, y no utilizar iniciales de su nombre, familiares, etc.

5.1.3 Los usuarios no deben usar la misma contraseña para acceso a cuentas del Municipio que para otro tipo de accesos no relacionados con esta institución (por ejemplo, cuentas de Correo personal, Redes Sociales, etc.).

5.1.4 Siempre que sea posible, los usuarios no deben usar la misma contraseña para diferentes necesidades de acceso del Municipio.

5.1.5 Las cuentas de usuario que requieran distintos niveles de privilegios deberán ser solicitados por los jefes de cada Dirección o Departamento, mediante correo electrónico o mediante documento físico. Además, dichos jefes serán los encargados de informar a la Oficina de Tecnología de Información y Comunicación (TIC) cuando algún funcionario sea desvinculado de nuestro Municipio para la suspensión o eliminación de la cuenta de los Sistemas informáticos.

5.1.6 Los horarios de trabajo extendidos para algunos funcionarios específicos, deberán ser solicitados por los jefes de cada Dirección o Departamento mediante correo electrónico o mediante documento físico.

5.1.6 Todas las contraseñas de los sistemas informáticos utilizados por la Ilustre Municipalidad de Tierra Amarilla serán cambiadas al menos cada trimestre. El forzado de cambio de contraseñas será activado por la Oficina de Tecnología de Información y Comunicación (TIC) en los períodos señalados.

5.1.7 Todas las contraseñas de nivel de usuario (por ejemplo: de Correo Electrónico, Navegación Web, Computadoras de Escritorio, etc.) serán cambiadas al menos cada seis meses, y será responsabilidad de cada usuario asignado a cada equipo la renovación de dichas contraseñas.

5.1.8 La Oficina de Tecnología de Información y Comunicación (TIC) podrá realizar eliminación de contraseñas de Windows sólo si es solicitado por algún jefe de Dirección o Departamento, en virtud de que algún funcionario haya sido desvinculado o si es que algún funcionario se encuentra de vacaciones y si es que su jefe directo necesita buscar o utilizar algún archivo específico.

5.1.9 La Oficina de Tecnología de Información y Comunicación (TIC) será la única encargada de administrar las claves de las cuentas de la nube de Office 365, esto con la finalidad de que no se pierda ningún tipo de información perteneciente a la Ilustre Municipalidad de Tierra Amarilla.

5.2 Protección de Contraseñas

5.2.1 Las contraseñas no deben de compartirse con nadie. Todas las contraseñas deben ser tratadas como sensibles, es decir, como Información confidencial de la Ilustre Municipalidad de Tierra Amarilla.

5.2.2 Las contraseñas no deben ser reveladas por teléfono a nadie.

5.2.3 No debe revelar contraseñas en cuestionarios o formularios de seguridad o de ningún tipo.

5.2.4 No deje pistas del formato de una contraseña (por ejemplo, "nombre de mi familia").

5.2.5 No comparta contraseñas de la Ilustre Municipalidad de Tierra Amarilla con nadie, incluyendo asistentes, administrativos, secretarias, directivos, jefes, compañeros de trabajo durante las vacaciones, amigos o miembros de la familia.

5.2.6 No escriba ni guarde contraseñas en post-its o papel en cualquier lugar de su oficina. No guarde las contraseñas en archivos en su computadora o dispositivos móviles (teléfonos, tablets) sin cifrado.

5.2.7 No utilice la función "Recordar Contraseña" de aplicaciones (por ejemplo, navegadores web).

5.2.8 Cualquier usuario que sospeche que su contraseña puede haber sido comprometida debe reportar el incidente inmediatamente y cambiar todas sus contraseñas a la brevedad.

6. Cumplimiento

6.1 Medidas de Cumplimiento

La Oficina de Tecnología de Información y Comunicación (TIC), verificará el cumplimiento de este procedimiento a través de diversos métodos, incluyendo, pero no limitado a, revisiones periódicas presenciales y remotas, auditorías internas, así como la retroalimentación al Encargado de la Oficina de Tecnologías de la información y comunicación (TIC). Las revisiones y/o auditorías deberán ser realizadas por el Comité de Seguridad de la información.

6.2 Excepciones

Cualquier excepción específica debe ser aprobada por la Oficina de Tecnología de Información y Comunicación (TIC) con antelación.

6.3 Incumplimiento

El incumplimiento de este manual puede estar sujeto a medidas disciplinarias establecidas en la ley 18.883. Dichas medidas podrán ser tomadas por la Jefatura directa, además de sugerencias realizadas por la Oficina de Tecnología de Información y Comunicación (TIC).