REPÚBLICA DE CHILE
I. MUNICIPALIDAD DE SANTO DOMINGO

REF.: APRUÉBESE REGLAMENTO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS TI DE LA I. MUNICIPALIDAD DE SANTO DOMINGO

DECRETO ALCALDICIO N° 2047

SANTO DOMINGO, 23 DIC 2022

VISTOS

1. Ley N° 18.695 de fecha 31.03.1988, Ministerio del Interior, ley orgánica constitucional de municipalidades, refundida por Decreto con Fuerza de Ley N° 1 de fecha 26.07.2006, Ministerio del Interior; Subsecretaría de Desarrollo Regional y Administrativo, fija el texto refundido, coordinado y sistematizado de la Ley Nº 18.695, orgánica constitucional de municipalidades;
2. Ley N° 19.653 de fecha 14.12.1999, Ministerio Secretaría General de la Presidencia, sobre probidad administrativa aplicable de los órganos de la administración del estado;
3. Ley N° 19.799 de fecha 12.04.2002, Ministerio de Economía, Fomento y Reconstrucción; Subsecretaría de Economía, Fomento y Reconstrucción, sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma;
4. Ley N° 19.880 de fecha 29.05.2003, Ministerio Secretaría General de la Presidencia, establece bases de los procedimientos administrativos que rigen los actos de los órganos de la Administración del Estado;
5. Decreto N° 83 de fecha 12.01.2005, Ministerio Secretaría General de la Presidencia, aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos;
6. Ley N° 20.285 de fecha 20.08.2008, Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública;
7. Ley N° 20.609 de fecha 24.07.2012, Ministerio Secretaría General de Gobierno, que establece medidas contra la discriminación;
8. Ley N° 20.730 de fecha 08.03.2014, Ministerio Secretaría General de la Presidencia, que regula el lobby y las gestiones que representen intereses particulares ante las autoridades y funcionario;
9. Ley N° 20.880 de fecha 05.01.2016, Ministerio Secretaría General de la Presidencia, sobre probidad en la función pública y prevención de los conflictos de intereses;
10. Ley N° 21.180 de fecha 11.11.2019, Ministerio Secretaría General de la Presidencia, Transformación Digital del Estado;
11. Ley N° 21.459 de fecha 20.06.2022, Ministerio de Justicia y Derechos Humanos, establece normas sobre delitos informáticos, deroga la Ley N° 19.223 y modifica otros cuerpos legales con el objeto de adecuarlos al convenio de Budapest;
12. Política Nacional de Ciberseguridad 2017 del Comité Interministerial sobre Ciberseguridad
13. ISO 19600: Sistemas de gestión de compliance. Directrices;

SECRETARIO MUNICIPAL SANTO DOMINGO

Municipalidad de Santo Domingo
Plaza del Cabildo S/N. (35) 220 06 10
www.santodomingo.cl

14. ISO 27001: Sistemas de Gestión para la seguridad de la información, interpretación y pautas para su implementación;
15. Norma NCH 2777, Norma de Tecnología de la Información – Código de práctica para la gestión de la seguridad de la información;
16. Decreto Alcaldicio N° 141 de fecha 29.01.2019, aprueba reglamento municipal sobre uso de recursos tecnológicos de la Ilustre Municipalidad de Santo Domingo;
17. Decreto Alcaldicio N° 729 de fecha 11.05.2022, apruébese políticas de gestión de las tecnologías de la información y la transformación digital de la I. Municipalidad de Santo Domingo;
18. Decreto Alcaldicio N° 1270 de fecha 22.08.2022, apruébese políticas de privacidad y protección de datos de la I. Municipalidad de Santo Domingo;
19. Decreto Alcaldicio N° 800 de fecha 29.06.2021, Asume funciones como Alcalde Titular de la I. Municipalidad de Santo Domingo el Sr. Dino Paolo Lotito Flores.

CONSIDERANDO

1. Que, para cumplir con el objetivo de la Ley de Transformación Digital de hacer operativo el funcionamiento administrativo de las diversas Unidades Municipales de manera coordinada, en beneficio del cumplimiento de objetivos públicos y actos administrativos decisorios sobre distintas materias de competencia municipal, a fin de dar ejecución a principios públicos de celeridad, de conclusión, de economía procedimental, y otros que informan el ámbito público en general, y de gestión municipal en particular.
2. Que, urge la necesidad de actualizar las políticas existentes relacionadas a recursos tecnológicos y su gestión con el fin de mejorar continuamente el quehacer municipal.
3. Que, la planificación, entendida como un recurso metodológico, debe ser capaz de influir sobre los "cambios naturales" que podría sufrir el entorno físico y social. De ello, surge la necesidad de fijar la situación esperada, o su ideal a alcanzar, frente a lo cual se entrega un conjunto de recursos disponibles para acercarse a la imagen-objetivo.
4. Que, una política pública integra metas, decisiones y acciones que emprende la municipalidad para abordar problemas, proponiendo guías y estrategias a alcanzar.
5. Que, existió una consulta abierta que permitió recoger las opiniones y aportes de los/as funcionarios/as municipales, respecto de las políticas que aluden a la Gestión de las Tecnologías de la Información y la Transformación Digital en la I. Municipalidad de Santo Domingo, cuyas recomendaciones serán un valioso aporte.

DECRETO

1. **APRUÉBESE** el siguiente reglamento sobre la gestión y uso de los recursos tecnológicos y la transformación digital de la I. Municipalidad de Santo Domingo según indica lo siguiente:

REGLAMENTO SOBRE LA SEGURIDAD DE LA INFORMACIÓN Y GESTIÓN DE RIESGOS TI

DE LA I. MUNICIPALIDAD DE SANTO DOMINGO

Objetivo: El objetivo del presente reglamento es establecer procesos e instrucciones para la seguridad de la información y la gestión de riesgos tecnológicos de la I. Municipalidad de Santo Domingo.

Alcance: El presente reglamento deberá ser aplicado por todos los funcionarios y funcionarias municipales, cualquiera sea su jerarquía, escalafón o estamento. Asimismo, a aquellos prestadores de servicios contratados a honorarios, a proveedores externos y terceros que sean autorizados a utilizar los recursos tecnológicos y sistemas de información del municipio.

Definiciones: Para exponer de manera unívoca y con precisión la comprensión de las cualidades esenciales del tema implicado se detallan las siguientes definiciones:

- **Abuso de dispositivos:** El que entregare u obtuviere para su utilización, importare, difundiera o realizare otra forma de puesta a disposición uno o más dispositivos, programas computacionales, contraseñas, códigos de seguridad o de acceso u otros datos similares, creados o adaptados principalmente para la perpetración de delitos.
- **Acceso ilícito:** El que, sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad, acceda a un sistema informático.
- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, locación/edificio, personas) que tenga valor para la organización. (ISO/IEC 27000).
- **Activo TI:** Cualquier componente que pueda contribuir a la entrega de un producto o servicio de TI, generalmente incluye todo el software, hardware, redes, servicios en la nube y dispositivos.
- **Aplicación SQL o Bases de Datos:** Corresponde a una colección de bases de datos, incluye datos del sistema y el registro de transacciones.
- **Ataque a la integridad de datos:** El que indebidamente altere, dañe o suprima datos informáticos.
- **Autenticación:** proceso de confirmación de la identidad del usuario que generó un documento electrónico y/o que utiliza un sistema informático.
- **Comunicaciones:** La red de datos y la infraestructura de comunicaciones municipales son los recursos compartidos y limitados entre activos TI para la entrega de servicios.
- **Confidencialidad:** Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.
- **Continuidad del negocio:** Continuidad de las operaciones municipales y sus servicios.

I. MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

Municipalidad de Santo Domingo
Plaza de Armas [illegible] 10
www.santodomingo.cl

- **Dato:** Secuencia de uno o más símbolos a los que se les da significado mediante actos específicos de interpretación. Los datos requieren un procesamiento para convertirse en información.
- **Disponibilidad:** Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
- **Documento electrónico:** constituyen un activo para la entidad que los genera y obtiene. La información que contienen es resultado de una acción determinada y sustenta la toma de decisiones por parte de quien la administra y accede a ella.
- **Documento público:** aquellos documentos que no son ni reservados ni secretos y cuyo conocimiento no está circunscrito.
- **Documento reservado:** aquellos documentos cuyo conocimiento está circunscrito al ámbito de la respectiva unidad del órgano a que sean remitidos, en virtud de una ley o de una norma administrativa dictada en conformidad a ella, que les confiere tal carácter.
- **Documento secreto:** 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.
- **Falsificación informática:** El que indebidamente introduzca, altere, dañe o suprima datos informáticos con la intención de que sean tomados como auténticos o utilizados para generar documentos auténticos.
- **Firma Electrónica:** Cualquier sonido, símbolo o proceso electrónico, que permite al receptor de un documento electrónico identificar al menos formalmente a su autor.
- **Firma Electrónica Avanzada:** aquella firma certificada por un prestador acreditado, que ha sido creada usando medios que el titular mantiene bajo su exclusivo control, de manera que se vincule únicamente al mismo y a los datos a los que se refiere, permitiendo la detección posterior de cualquier modificación, verificando la identidad del titular e impidiendo que desconozca la integridad del documento y su autoría.
- **Fraude informático:** El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático.
- **Identificador Temporal:** Es aquel que se asigna a un usuario(a) la primera vez que accede a un sistema o equipo, y que debe ser cambiado por éste en su primer acceso.
- **Integridad:** Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente.
- **Interceptación ilícita:** El que indebidamente intercepte, interrumpa o interfiera, por medios técnicos, la transmisión no pública de información en un sistema informático o entre dos o más de aquellos.
- **Hardware:** Referido a las partes tangibles, de un sistema informático, sus componentes eléctricos, electrónicos, electromecánicos y mecánicos.

- **Plan de recuperación de desastres:** Se entiende por plan de contingencia el conjunto de procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información.
- **Prestadores de servicios:** Toda entidad pública o privada que ofrezca a los usuarios de sus servicios la posibilidad de comunicar a través de un sistema informático y cualquier otra entidad que procese o almacene datos informáticos para dicho servicio de comunicación o para los usuarios del mismo.
- **Receptación de datos informáticos:** El que conociendo su origen o no pudiendo menos que conocerlo comercialice, transfiera o almacene con el mismo objeto u otro fin ilícito, a cualquier título, los datos informáticos.
- **Recurso:** Activo o medio que utiliza la tecnología para cumplir su propósito. Estos pueden ser tangibles como computadores, servidores, impresoras, etc, o bien, intangibles como sistemas computacionales, aplicaciones móviles, casillas de correo electrónico, entre otros.
- **Repositorio:** Estructura tecnológica donde son almacenados los documentos electrónicos.
- **Riesgo TI:** Referido al continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Está asociado con el uso, propiedad, operación, involucramiento, influencia y adopción de TI dentro del municipio.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad, y disponibilidad de la información.
- **Seguridad perimetral:** La seguridad perimetral es un concepto emergente asume la integración de elementos y sistemas, tanto electrónicos como mecánicos, para la protección de perímetros físicos, detección de tentativas de intrusos en instalaciones especialmente sensibles.
- **Servicio TI:** Conjunto de actividades que busca responder a las necesidades de los funcionarios/as - ciudadanos/as por medio de un cambio de condición en los activos, potenciando su valor y mitigando sus posibles riesgos. Adicionalmente considera elementos de hardware, software y comunicaciones entre ambos.
- **Sistema computacional:** Referido a software de desarrollo propio o contratado.
- **Software:** Corresponde a un programa o conjunto de programas computacionales, así como datos, procedimientos y pautas que permiten realizar distintas tareas dentro de un sistema.
- **Transformación Digital:** Implica que el ciclo completo de los procedimientos administrativos se realice por medios electrónicos, con el consiguiente aumento significativo en la eficiencia de los servicios; una mayor certeza, seguridad y velocidad en su entrega a las personas; a la vez de una mayor transparencia de los procesos y actuaciones del Estado en relación con éstas.

I. MUNICIPALIDAD DE SANTO DOMINGO
SECRETARIO MUNICIPAL

Municipalidad de Santo Domingo
Plaza del Cabildo S/N. (35) 220006 10
www.santodomingo.cl

- **Uso responsable:** Cumplimiento por parte de los funcionarios(as) de las normas legales, políticas, reglamentos, procesos, procedimientos y buenas prácticas que propicien el resguardo de información y uso eficiente de los recursos tecnológicos.
- **Usuario(a):** Corresponde a funcionarios y funcionarias municipales, cualquiera sea su jerarquía, escalafón o estamento. Asimismo, a aquellos prestadores de servicios contratados a honorarios, a proveedores externos y terceros que sean autorizados a utilizar los recursos tecnológicos y sistemas de información del municipio

I. SOBRE LOS RIESGOS TI

a) GESTIÓN DE RIESGOS TI:

El Departamento de Informática y Gobierno Electrónico mantendrá actualizada anualmente una matriz de riegos que contenga la ponderación de cada uno de estos y su medición correspondiente.

La matriz de riesgos deberá ser almacenada en dispositivos o unidades de almacenamiento en línea que propicien un acceso inmediato.

La pertinencia de los ítems susceptibles a riesgos deberá ser evaluada anualmente por el Departamento de Informática y Gobierno Electrónico, considerando su seguimiento y adopción de medidas relevantes cuando existan cambios que impliquen un efecto negativo en la municipalidad.

b) INFORMACIÓN RIESGOS TI:

El Departamento de Informática y Gobierno Electrónico mantendrá informados a todos los funcionarios y funcionarias municipales sobre materias de riesgos TI, según sea relevante para el desempeño de su trabajo considerando como mínimo:

- Los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos;
- Las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado;
- Las buenas prácticas para protegerse de los riesgos asociados a la obtención de archivos y software a través de las redes de telecomunicaciones, o por otros medios, indicando qué medidas de protección se deberán aplicar.

Asimismo, el Departamento de Informática y Gobierno Electrónico deberá informar sobre aquellas materias relativas a los siguientes aspectos del ambiente externo:

- Consumo de alimentos, bebidas y tabaco en las cercanías de sistemas informáticos.
- Condiciones climatológicas y ambientales que pueden afectar sistemas informáticos o entornos cercanos.

- Promoción de una práctica de escritorio limpio.

Una vez detectada la problemática, el funcionario encargado de redes deberá actualizar las configuraciones de seguridad de acuerdo a los lineamientos establecidos por la jefatura y será enviada una notificación a la unidad(es) municipal(es) comprometidas indicando el problema y su resolución.

En cuyos casos donde la corrección y/o mitigación de un riesgo TI requiera de un licenciamiento, hardware o software adicional esta deberá ser canalizada inmediatamente junto al informe técnico que sustente la Solicitud de Compra.

c) **USO INDEBIDO TI:**

El Departamento de Informática y Gobierno Electrónico efectuará semanalmente un monitoreo continuo sobre el tráfico de datos, acceso a sitios web, licenciamiento y sistemas computacionales que puedan significar un alto consumo o sean un riesgo TI que impacte en la gestión municipal.

Los usuarios(as) tendrán prohibido cualquier intento de configuración de la red municipal, esta labor estará gestionada únicamente por el Departamento de Informática y Gobierno Electrónico. Asimismo, quedará totalmente prohibido interrumpir, interceptar las comunicaciones de la red municipal, acceder a recursos e información a los cuales no hayan sido autorizados y ejecutar software o herramientas que vulneren o comprometan la seguridad de la red municipal, de los sistemas computacionales o de los datos gestionados por la municipalidad.

El Departamento de Informática y Gobierno Electrónico restringirá el acceso a la red municipal a todo equipo tecnológico que no respete las políticas de ciberseguridad o lo indicado en el presente reglamento. Una vez ocurrido el hecho, el funcionario(a) municipal, y su jefatura directa, serán notificados respecto de la medida implementada junto con las medidas de resguardo que deberán considerar a futuro.

Aquellos funcionarios/as, trabajadores o prestadores de servicios que incurran en dos oportunidades en la misma falta, serán restringidos sus accesos y serán notificados junto al Administrador Municipal. Frente a una tercera oportunidad, los accesos serán restringidos totalmente hasta la resolución por parte del Alcalde.

d) **LEGALIDAD DE LOS ACTOS**

Las responsabilidades de seguridad aplicables al personal deberán ser explicitadas en la etapa de selección e incluirse expresamente en los decretos o resoluciones de nombramiento o en las contrataciones respectivas.

En cuyos casos sobre el uso indebido de la red municipal, uso indebido de los datos, uso indebido de recursos compartidos, accesos de máxima amenaza o que puedan exponer a la institución frente a la violación de leyes y normas legales. El Departamento de Informática y Gobierno Electrónico entregará los antecedentes

I. MUNICIPALIDAD
SECRETARIO MUNICIPAL
SANTO DOMINGO
Municipalidad de Santo Domingo
Plaza del Cabildo S/N, (35) 220 06 10
www.santodomingo.cl

para la debida investigación por parte de la Dirección de Control, Dirección de Asesoría Jurídica, Administración Municipal y Alcalde, según corresponda.

Previa orden judicial o requerimiento del Ministerio Público, la I. Municipalidad de Santo Domingo proporcionará la información requerida que dé cuenta de actos ilícitos por parte de los usuarios(as) correspondientes.

e) CLASIFICACIÓN, CONTROL Y ETIQUETADO DE BIENES

Los documentos electrónicos y sistemas informáticos deberán clasificarse y etiquetarse para indicar la necesidad, prioridad y grado de protección. La clasificación de un sistema informático corresponderá a la clasificación más estricta aplicable al documento electrónico que almacene o procese de acuerdo con los lineamientos normativos vigentes.

Asimismo, el Departamento de Informático y Gobierno Electrónico por cada sistema informático, tendrá asignado un responsable quien velará por su debida clasificación y etiquetado.

Se deberá proponer quién será responsable por omisión, sea asignando tal responsabilidad al usuario que lo crea, sea atribuyéndosela al responsable por el sistema informático que lo generó, u otra modalidad.

La I. Municipalidad de Santo Domingo deberá garantizar un adecuado manejo de la información a través de metodologías de trabajo que definan la clasificación de los activos de la información considerando:

- Los responsables de los activos de información que tengan bajo su responsabilidad deberán clasificar como "Confidencial", "Uso interno" o "Público" según sea la importancia respecto de la seguridad del activo para la municipalidad.
- Todo activo de información que no sea clasificado deberá considerarse como de "Uso Interno", de manera que reciba los niveles de protección acordes a esta clasificación.
- Los activos deberán recibir la clasificación apropiada de manera que las medidas de protección sean aplicadas y correspondan a las necesidades del municipio.
- Por cada uno de los niveles de clasificación establecidos serán definidas las medidas de protección específicas que serán aplicadas por todo el municipio.

Todo usuario/a de los activos de información deberá respetar los siguientes lineamientos:

- No podrán divulgar archivos o datos clasificados como "Confidencial" o de "Uso Interno" de la I. Municipalidad de Santo Domingo ni de sus usuarios/as externos/as, salvo expresa autorización del responsable de la información, quien será responsable de la divulgación. Está prohibido que los

usuarios/as extraigan información fuera de las dependencias municipales si no han sido específicamente autorizados.

- Para transmitir a terceros la información "Confidencial" o de "Uso Interno" el usuario/a deberá solicitar la autorización al responsable de la información correspondiente. La entrega de la información será realizada suscribiendo acuerdos de confidencialidad con el tercero y aplicando controles específicos que se definan, y en los casos que la Ley lo determine.

La salida desde un sistema de un documento electrónico que está clasificado como reservado o secreto, según reglamento particular que lo rija, deberá tener una etiqueta apropiada de clasificación en la salida. Para estos efectos, deberá considerarse, entre otros, los informes impresos, pantallas de computador, medios magnéticos (cintas, discos, CDs, cassettes), mensajes electrónicos y transferencia de archivos

II. SOBRE LA RED Y DOMINIO MUNICIPAL

a) ACCESO A RED Y SERVICIOS:

El Departamento de Informática y Gobierno Electrónico gestionará y controlará las credenciales de acceso a la red y servicios municipales para todos los funcionarios y funcionarias municipales que lo requieran según la naturaleza de su cargo, sin perjuicio de aquellos usuarios externos que cuenten con la debida autorización de su jefatura directa.

Para otorgar acceso a la red y sus servicios cada responsable de la Unidad Municipal deberá enviar un correo electrónico indicando el nombre de la persona que requiere acceso, área de desempeño, sistemas a los que desea acceder, privilegios sobre los datos a gestionar y periodo de vigencia de la cuenta de acceso.

Los usuarios(as) contarán con un acceso controlado a la red de datos municipal que les permitirá trabajar con recursos compartidos como carpetas, aplicativos, impresoras, sistemas computacionales, unidades compartidas, servicio de internet, entre otros.

Las cuentas de acceso y sus credenciales corresponderán a un conjunto de caracteres integrados por números, letras o símbolos, cuyo objetivo es impedir el acceso no autorizado al equipo computacional, equipo de almacenamiento, correo electrónico, sistema computacional, entre otros.

Las credenciales de acceso serán individuales, intransferibles, secretas y entregadas vía electrónica únicamente al usuario(a) en cuestión a través de un identificador temporal. Será responsabilidad de cada usuario(a) acusar recibo y mantener los resguardos de sus contraseñas para el acceso a la red, sistemas computacionales, correo electrónico, entre otros, siendo de uso personal e intransferible. El Departamento de Informática y Gobierno Electrónico no será responsable del mal uso de ellas.

I. MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

Para una adecuada gestión de contraseñas los usuarios(as) deberán considerar las siguientes medidas de seguridad y buenas prácticas:

- No crear contraseñas que puedas ser adivinadas, tales como nombres, fechas específicas, lugares, números telefónicos, número de rut, nombre de su dirección municipal, entre otros.
- No utilizar la misma contraseña para todos sus accesos.
- No compartir las contraseñas.
- No registrar contraseñas en su puesto de trabajo o papel.
- No incluir contraseñas en cualquier proceso de inicio de sesión automatizado, por ejemplo, almacenado en una macro
- Evitar el uso de contraseñas antiguas o anteriores que pudieron ser expuestas.
- Evitar almacenar sus contraseñas en el navegador de internet.
- Cambiar contraseñas iniciales entregadas para iniciar sesión por primera vez.
- Realizar el cambio de contraseña cada 3 meses o antes.
- Cambiar las contraseñas cada vez que sospeche o tenga indicios de un posible compromiso de estas.
- Elegir contraseñas que tengan una longitud mínima de ocho caracteres, considerando signos especiales y letras en mayúscula y minúscula.
- Cerrar sesión de todo sistema computacional u equipo donde haya ingresado sus credenciales de acceso.

Para reducir el riesgo de acceso no autorizado a documentos electrónicos o sistemas informáticos, deberán ser promovidas buenas prácticas, como las de pantalla limpia. En particular, se incentivará a los usuarios o configurar los sistemas de manera que se dé cumplimiento a los siguientes estándares:

- Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que éstas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con protector de pantalla con una contraseña protegida.
- Cerrar las sesiones de los computadores principales cuando la sesión finaliza, lo que no significa, necesariamente, apagar el terminal o los equipos.
- Asegurar los terminales o equipos frente al uso no autorizado, mediante una contraseña de traba o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.

Los usuarios(as) no deberán intentar acceder a sistemas computacionales o equipos TI a los que no han sido expresamente autorizados. Esta acción supondrá intento de acceso malicioso o suplantación de identidad, por lo que el Departamento de Informática y Gobierno Electrónico tomará las acciones pertinentes auditando los procesos involucrados e informando a las autoridades municipales.

En cuyos casos donde un usuario(a) presuma que la contraseña de su cuenta esté comprometida deberá informar inmediatamente al Departamento de Informática y Gobierno Electrónico para recibir asesoría y coordinar su restauración.

El Departamento de Informática y Gobierno Electrónico podrá gestionar cambios periódicos de contraseñas obligatorios y será responsable de la implementación y administración de cualquier otro medio de autenticación que el municipio incorpore.

El Departamento de Informática y Gobierno Electrónico realizará un monitoreo mensual respecto a las credenciales de acceso otorgadas con el fin de mantener un registro actualizado. Sin perjuicio de aquellos funcionarios(as), trabajadores(as) y prestadores de servicios que ya no tengan una relación contractual con el municipio, los cuales serán respaldados y dados de baja previa notificación por parte de la Jefatura directa, Dirección de Recursos Humanos, Dirección Educación Municipal, Dirección Salud Municipal, Administración Municipal o Alcalde.

b) **PERFIL DE ACCESO A RED Y SERVICIOS:**

El Departamento de Informática y Gobierno Electrónico gestionará mecanismos de seguridad y control que establezcan perfiles de acceso a los diversos recursos municipales de acuerdo con la naturaleza del cargo.

Asimismo, serán entregadas recomendaciones y buenas prácticas para mantener seguridad en las credenciales de acceso y uso de los servicios municipales.

Toda instalación de software recaerá exclusivamente en el Departamento de Informática y Gobierno Electrónico, quien previamente analizará la pertinencia, licenciamiento, condiciones de seguridad y su impacto respectivo.

c) **ACCESO A SERVIDORES Y EQUIPOS ESPECIALIZADOS:**

El Departamento de Informática y Gobierno Electrónico restringirá el acceso, ya sea local o remoto, a las instalaciones de servidores o equipos especializados municipales sin previa autorización del Departamento de Informática y Gobierno Electrónico cuyo fin es minimizar el acceso innecesario a las áreas de trabajo y disminuir las posibilidades de amenazas de humo y fuego, humedad y agua, inestabilidad en el suministro eléctrico, hurto y robo.

Todo ingreso de visitas al perímetro de seguridad deberá ser autorizado por escrito, quedando constancia del propósito y duración de ella. Cada persona autorizada al momento de ingresar deberá registrar en la bitácora correspondiente su nombre, fecha de ingreso, hora de ingreso y descripción de las acciones realizadas. Los controles físicos de entrada en el perímetro de seguridad deberán utilizar el carné de identidad como identificación válida en el caso de los chilenos, y el pasaporte en el caso de los extranjeros.

Los visitantes serán acompañados en todo momento por alguna persona autorizada de la organización hasta que abandonen el recinto.

I. MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

Municipalidad de Santo Domingo
Avda. O'Higgins N. (35) 220 06 10
www.santodomingo.cl

d) **GESTIÓN CREDENCIALES RED Y SERVICIOS:**

La I. Municipalidad de Santo Domingo evitará el acceso no autorizado en la red y servicios mediante la implementación de mecanismos de seguridad confiables y oportunos para la institución.

El Departamento de Informática y Gobierno Electrónico permitirá únicamente el acceso a los servidores, servicios de almacenamiento y motores de bases de datos municipales solo a aplicaciones, sistemas computacionales, servicios de consulta API, estaciones de trabajo que sean identificables a través de métodos localizables como dirección IP (Internet Protocol).

El Departamento de Informática y Gobierno Electrónico tendrá la responsabilidad de mantener un registro electrónico que contenga las estaciones de trabajo y servicios identificados que tienen acceso a servidores, servicios de almacenamiento y motores de bases de datos.

El Departamento de Informática y Gobierno Electrónico realizará anualmente la actualización de las credenciales de acceso a los servidores, servicios de almacenamiento y motores de bases de datos municipales.

En cuyos casos de cese de funciones de un usuario(a), el Departamento de Informática y Gobierno Electrónico suspenderá la cuenta asociada. Por motivos de seguridad, la suspensión de la cuenta podrá ser efectuada previo a la tramitación del cese.

e) **ACTIVOS TI EN LA RED MUNICIPAL:**

El Departamento de Informática y Gobierno Electrónico restringirá el acceso a la red institucional, ya sea local o remoto, para todo equipamiento tecnológico que no sea de propiedad o esté bajo la administración municipal.

Sin perjuicio de aquellos casos de fuerza mayor, el Departamento de Informática y Gobierno Electrónico otorgará permisos para acceder a la red municipal únicamente con privilegios de navegación a internet.

Preferentemente, la conexión a la red municipal será a través de la infraestructura cableada para aquellos equipos computacionales de escritorio, mientras que será inalámbrica para los equipos computacionales portátiles como notebook, laptop. Los dispositivos móviles como smartphones y tabletas no tendrán acceso a la red municipal, salvo excepciones debidamente justificadas.

El Departamento de Informática y Gobierno Electrónico deberá mantener redes de área local virtuales (*vlan*) crear redes lógicas independientes dentro de la misma red física municipal. Las VLAN serán divididas de acuerdo con las unidades municipales y la naturaleza de sus funciones, diferenciando acceso a servidores, bases de datos, unidades externas de almacenamiento, etc.

Quedará totalmente prohibido utilizar en la red municipal equipamiento TI que no cuente con el debido licenciamiento en software de ciberseguridad y que ofrezca estándares mínimos frente a amenazas tecnológicas.

Cada usuario(a) tendrá la responsabilidad de conectar su equipo computacional a la red municipal en forma periódica, a lo menos cada 15 días corridos para los efectos de actualizar el software y servicios de uso general como antivirus, sistema operativo y políticas de dominio.

f) **PROTECCIÓN DE ACTIVOS TI:**

El Departamento de Informática y Gobierno Electrónico mantendrá mecanismos de control y seguridad para el acceso a los equipos tecnológicos de acuerdo con los perfiles de acceso definidos. Asimismo, será responsable de administrar la seguridad en la red de datos municipal a través de la mantención del cortafuego y de otros dispositivos de enrutamiento y filtrado de tráfico.

Asimismo, en cada equipo computacional deberá ser instalado un antivirus o agente que proteja frente a la posibilidad de amenazas a la seguridad TI.

En todo caso y sin perjuicio de los controles dispuestos para la protección TI, los funcionarios y funcionarias municipales deberán procurar mantener sus equipos con el resguardo adecuado para evitar accesos no autorizados que pongan en riesgo su información almacenada en el equipo y/o sistema computacional.

Para el trabajo diario deberán ser utilizados únicamente los sistemas de información autorizados y designados, de acuerdo con el perfil y/o rol de usuario otorgado.

El usuario(a) tendrá la responsabilidad de priorizar el almacenamiento de la información en el equipo municipal utilizado y su acceso a los sistemas computacionales, evitando ser guardadas en medios extraíbles o susceptibles a pérdidas y fallas como discos compactos, unidad flash, tarjeta de memoria, pendrives, discos duros externos, entre otros.

Cada usuario(a) deberá abstenerse de ingresar, almacenar y/o manipular archivos que pudieran tratar contenido ilegal, pornográfico, injurioso, amenazador, ofensivo, obsceno, racista o sexista y en general todos aquellos que sean ajenos a las funciones que les correspondan. Asimismo, cada usuario(a) deberá tener especial precaución de abrir comunicaciones cuya procedencia sea desconocida, sospechosa o que pueda contener programas o archivos maliciosos. Una vez identificado deberá ser comunicado inmediatamente al Departamento de Informática y Gobierno Electrónico.

Será responsabilidad de cada usuario(a) mantener a buen recaudo los equipos, aplicaciones y sistemas computacionales que manejan información reservada y/o sensible.

I. MUNICIPALIDAD
SECRETARIO MUNICIPAL
SANTO DOMINGO
Municipalidad de Santo Domingo
Plaza del Cabildo S/N, (35) 220 06 10
www.santodomingo.cl

Cada usuario(a) será responsable de respaldar la información, archivos y datos institucionales residentes en los equipos computacionales a su cargo. El Departamento de Informática y Gobierno Electrónico colaborará y asesorará en el respaldo previo requerimiento por parte del usuario(a).

Con el objetivo de asegurar la información, archivos y datos institucionales críticos que no se encuentran en los sistemas computacionales, el Departamento de Informática y Gobierno Electrónico dispondrá unidades de almacenamiento en red para cada dirección municipal que posibilitarán el trabajo colaborativo y una ágil recuperación frente a ataques que atenten a estos.

La I. Municipalidad de Santo Domingo suministrará los recursos pertinentes para que los equipos computacionales en los que se almacenen documentos electrónicos y sistemas informáticos que los procesen, tengan un adecuado suministro de energía eléctrica, incluyendo no sólo el flujo de energía suministrado, sino también la "tierra eléctrica" de las instalaciones.

g) PROTECCIÓN DE SERVICIOS WEB Y CORREO ELECTRÓNICO:

El Departamento de Informática y Gobierno Electrónico utilizará estándares de correo electrónico para evitar, en lo posible, el spoofing y la suplantación de identidad (phishing) en los servicios de correo electrónico institucionales. Estos estándares, deberán ayudar a que los mensajes enviados desde el municipio no sean catalogados como spam.

Frente a esto, serán utilizados estos estándares de correo:

- SPF: especificar los servidores y los dominios que están autorizados para enviar correo en nombre de la municipalidad.
- DKIM: añadir una firma digital a todos los mensajes enviados, que permita a los servidores que los reciben verificar que realmente proceden de la I. Municipalidad de Santo Domingo.
- DMARC: indicar a los servidores que receptores qué deben hacer con los mensajes que se envían desde la municipalidad y que no superan las comprobaciones de SPF o DKIM anteriores.

Mientras que los servicios web deberán considerar como requerimiento mínimo:

- SSL (Secure Sockets Layer (Capa de sockets seguros)): Todos los servicios o desarrollos propios, contratados o adquiridos mediante otros servicios públicos y que se encuentren bajo administración municipal, deberán agregar certificados SSL a sus sitios web para proteger las transacciones en línea y mantener la privacidad y seguridad de la información del cliente.
- TLS (Transport Layer Security (Seguridad en capas de transporte): Permite aumentar la seguridad con la interoperabilidad de las transmisiones de datos encriptados de diferentes aplicaciones como HTTP, pasando a ser HTTPS.

El Departamento de Informática y Gobierno Electrónico administrará los servidores de alojamiento web que soportan el hosting correspondiente. Mientras que, según corresponda, podrá ser otorgado un usuario perfilado que permita realizar toda la configuración y edición de un sitio web, con diferentes niveles de posibilidades de acuerdo a la naturaleza de sus funciones.

h) **PROTECCIÓN DE DATOS:**

Toda información almacenada en bases de datos, producto de la explotación de los sistemas computacionales para la gestión municipal, los servicios digitales y plataformas institucionales, será considerado como activo de valor estratégico para la municipalidad. Por lo tanto, la I. Municipalidad de Santo Domingo velará por el correcto uso, considerando las precauciones de seguridad y lineamientos normativos vigentes.

Los equipos computacionales, las aplicaciones y sistemas computacionales manejan información que en algunos casos es reservada y/o sensible, por lo que será responsabilidad del usuario(a) que tiene autorización para accederla, mantener un nivel de seguridad adecuado para su resguardo.

El Departamento de Informática y Gobierno Electrónico será responsable del respaldo de datos de los sistemas computacionales almacenados en servidores físicos, unidades de almacenamiento en red (*NAS*) y servicios digitales alojados en el dominio santodomingo.cl, incluyendo subdominios de este.

El Departamento de Informática y Gobierno Electrónico efectuará respaldos de las bases de datos que residen en servidores físicos. Estos respaldos deberán ser programados para ejecutarse considerando como mínimo lo siguiente:

- Cada respaldo deberá ser realizado en horarios fuera de atención de público, salvo excepciones de fuerza mayor.
- Compresión de las copias de respaldo para resguardar el espacio en discos de almacenamiento.
- Cada copia de respaldo deberá ser almacenada dentro del servidor y clonado en servicios externos a la red municipal para asegurar su disponibilidad a través de la metodología 3-2-1.
- Las copias de respaldo serán retenidas considerando un periodo máximo de 2 meses en servidor físico, 2 años en unidad externas de almacenamiento en red y 4 años en unidades de respaldo en nube.

Con el fin de mantener los datos seguros y protegidos contra la pérdida, corrupción y robo de datos, la I. Municipalidad de Santo Domingo deberá tener una Copia de Seguridad de datos que residen en servidores según la siguiente estrategia:

- Método de Backup o Respaldo Combinado de la Base de Datos: Será realizada con una periodicidad diaria el respaldo completo de toda la base de datos de los servidores administrados por el municipio. Mientras que durante los días y horarios laborales será efectuado un respaldo diferencial

I. MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

Municipalidad de Santo Domingo
Plaza de [illegible] Santo Domingo (35) 220 06 10
www.santodomingo.cl

conteniendo sólo copia lo que ha cambiado desde el último backup completo.

- Almacenamiento de Backup o Respaldo: Deberán ser mantenidas al menos tres (3) copias de las bases de datos relevantes. Las copias serán almacenadas en al menos 2 soportes distintos, y al menos una de las copias de respaldo será dispuesta en una ubicación ajena al municipio. El plazo de retención de los respaldos almacenados en el servidor físico será de dos meses, mientras que serán de cinco años para los soportes de ubicación remota.
- Método de Backup o Respaldo de Servidores Web: Existirá una copia semanal completa del (los) servidor(es) web, la cual será almacenada en una unidad de almacenamiento masivo y otra copia dispuesta en una ubicación ajena al municipio.
- Método de Backup o Respaldo de los Servidores Físicos: Mensualmente deberá ser realizada una copia de seguridad del (los) servidor(es) físico(s) administrados por el municipio. Serán almacenadas en una unidad de almacenamiento masivo y otra copia dispuesta en una ubicación ajena al municipio.

i) AUDITORIAS E INVESTIGACIONES:

Toda solicitud de acceso de este tipo deberá ser canalizado al Departamento de Informática y Gobierno Electrónico quien utilizará estándares de seguridad para la autorización de acceso a un sistema informático para auditorías e investigaciones que toda índole mediando la autorización expresa del titular del mismo.

Las credenciales de acceso tendrán un tiempo máximo de vigencia de acuerdo al cronograma establecido para la actividad en cuestión. La ampliación o renovación de estos plazos deberá ser fundada e informada por escrito a los interesados.

j) PROTECCIÓN FRENTE A ACCESOS NO AUTORIZADOS:

Todo usuario(a) deberá dar cumplimiento a los siguientes estándares que permitirán minimizar accesos no autorizados a la red o servicios autorizados:

- Cerrar las sesiones activas en el computador cuando se finaliza la labor, a menos que éstas se puedan asegurar mediante un sistema apropiado de control de acceso, por ejemplo, con protector de pantalla con una contraseña protegida;
- Cerrar las sesiones de los computadores principales cuando la sesión finaliza, lo que no significa, necesariamente, apagar el terminal o los equipos, y
- Asegurar los terminales o equipos frente al uso no autorizado, mediante una contraseña de traba o de un control equivalente, por ejemplo, una contraseña de acceso cuando no se use.

k) RESTITUCIÓN CREDENCIALES RED Y SERVICIOS:

La I. Municipalidad de Santo Domingo a través del Departamento de Informática y Gobierno Electrónico restituirá las credenciales de acceso a la red y servicios municipales, previo requerimiento formal y escrito por parte del director o jefatura de la unidad municipal correspondiente.

l) **MANTENIMIENTO SERVIDORES Y EQUIPOS DE ALTO RENDIMIENTO:**

La I. Municipalidad de Santo Domingo asignará los recursos correspondientes para proteger físicamente los equipos frente a las amenazas de riesgos del ambiente externo, pérdida o daño, incluyendo las instalaciones de apoyo tales como el suministro eléctrico y la infraestructura de cables.

La ubicación del equipamiento municipal deberá minimizar el acceso innecesario a las áreas de trabajo y disminuir las posibilidades de amenazas de humo y fuego, humedad y agua, inestabilidad en el suministro eléctrico, hurto y robo.

Los equipos servidores, cortafuegos, switch y todos aquellos de alto rendimiento deberán estar actualizados según las recomendaciones del fabricante o proveedor de los sistemas de seguridad. Bajo ningún caso serán permitidas las acumulaciones de estas puesto que podrían involucrar brechas de vulnerabilidad y exposición para el municipio. Dichas actualizaciones deberán realizarse preferentemente fuera de horarios de atención de público.

m) **MANTENIMIENTO INFRAESTRUCTURA RED:**

La I. Municipalidad de Santo Domingo asignará los recursos correspondientes para mantener en óptimas condiciones los componentes activos de la red (dispositivos inalámbricos, cableado, módem, router, etc.).

III. SOBRE EL SOFTWARE UTILIZADO

a) **AUTORIZACIÓN DE SOFTWARE:**

La I. Municipalidad de Santo Domingo a través del Departamento de Informática y Gobierno Electrónico, prohibirá la utilización de software que infrinja la normativa vigente o la ley de propiedad intelectual. La instalación de sistemas computacionales, software, ejecutables, hojas de cálculo, script o cualquier otro sin el correspondiente licenciamiento que autoriza su uso, comprometerá únicamente la responsabilidad del usuario(a) a cargo del activo TI.

Los usuarios(as) deberán considerar los siguientes alcances:

- Software, sistema, ejecutable o similares no autorizados: Con el fin de prevenir infracciones a la normativa vigente y la prevención de programas maliciosos que propicien riesgos o amenacen la red y datos municipales, los usuarios(as) no podrán instalar o ejecutar aplicativos que no estén autorizados previamente por el Departamento de Informática y Gobierno Electrónico.

I. MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

Municipalidad de Santo Domingo
Plaza del Canelo 01 (35) 220006 10
www.santodomingo.cl

- P2P o intercambio de archivos: Estará prohibida su utilización puesto que representan un riesgo de seguridad, proveen copias ilegales de material protegido y consumen gran ancho de banda de la red municipal. Lo anterior deviene en una interrupción del servicio de internet, telefonía, dispositivos de seguridad, entre otros, perjudicando el desempeño de los servicios y de las funciones de la municipalidad.

- Otros archivos de fuentes desconocidas: Estará prohibida la descarga de material que no pueda asegurar su confiabilidad como libros electrónicos (e-books), archivos de audio, archivos de video, archivos de imágenes o similares.

- Software, sistema, ejecutable o similares de código abierto: La instalación de estos deberá ser solicitada al Departamento de Informática y Gobierno Electrónico, quien analizará el licenciamiento y seguridad que presenten. Dicho requerimiento podrá ser denegada atendiendo a los riesgos señalados y regirá de la misma forma para controladores asociados a dispositivos externos como lectores/grabadores de CD/DVD, escáner, impresoras, cámaras, unidades de almacenamiento, entre otros.

- Sistemas o sitios web utilizados bajo convenio: La utilización de estos recursos serán otorgados únicamente a los señalados en el convenio o contrato suscrito entre ambas partes. Además, serán aplicadas las medidas de seguridad correspondientes, incluyendo direccionamiento IP público para cada uno de estos según amerite.

IV. SOBRE EL RESPALDO DE DATOS

a) RESPALDOS DATOS EN SISTEMAS DE INFORMACIÓN:

La I. Municipalidad de Santo Domingo a través del Departamento de Informática y Gobierno Electrónico, mantendrá diariamente copias de seguridad de las bases de datos y archivos alojados en los servidores municipales.

b) RESPALDOS DATOS EN ACTIVOS DE USO PERSONAL:

La I. Municipalidad de Santo Domingo considerará responsabilidad de cada funcionario y funcionaria sobre la información alojada en los equipos computacionales, los cuales deberán mantener un nivel de seguridad adecuado para su resguardo. El conjunto de datos deberá ser procesado a través de los sistemas informáticos, aplicaciones y/o unidades compartidas habilitadas para tales casos.

c) RESPALDOS DATOS EN CORREO ELECTRÓNICO:

La I. Municipalidad de Santo Domingo considerará responsabilidad de cada funcionario o funcionaria la pérdida de datos o archivos de su correo institucional a causa del uso indebido por parte de este.

d) **RESTAURACIÓN RESPALDOS:**

La I. Municipalidad de Santo Domingo pondrá a disposición de las unidades municipales requirentes toda copia de seguridad de su competencia para la continuidad de los servicios y/o auditorías.

V. SOBRE LA RECUPERACIÓN FRENTE A UN ATAQUE INFORMÁTICO

Al momento de ser detectado un incidente grave, ataque o fuga de información, el Departamento de Informática y Gobierno Electrónico deberá notificar inmediatamente al Administrador Municipal sobre las posibles consecuencias de ello.

Sin perjuicio de ello, deberán ser registradas las incidencias o brechas detectadas en el Documento de Seguridad que será desarrollado y actualizado conteniendo:

- El tipo de incidencia, ataque o fuga detectada.
- El momento en que se ha producido o detectado.
- La persona que realiza la notificación.
- La persona o personas a quien se realiza la notificación.
- Los efectos que derivan de la incidencia.
- Las medidas correctoras que se han aplicado.

Dicho documento será utilizado para la presentación de una denuncia ante las autoridades competentes, permitiendo recoger todas las pruebas que faciliten una posterior investigación.

El Departamento de Informática y Gobierno Electrónico llevará a cabo un plan organizado de recuperación que permitirá restablecer copias de seguridad, backups, sistemas computacionales y servicios correspondientes, con el fin de aproximarlo a un estado anterior al incidente.

Las configuraciones de respaldo para los sistemas individuales deberán ser probadas con regularidad, a lo menos cada 2 años, para asegurar que ellas satisfacen la continuidad operacional del municipio.

En cuyos casos donde fuere necesaria la reconstitución de un expediente o piezas de éste se reemplazará en todo o parte por una copia fiel, que se obtendrá de quien la tuviere, si no se dispusiere de ella directamente.

Si no existiere copia fiel los actos se dictarán nuevamente, para lo cual la I. Municipalidad de Santo Domingo reunirá los antecedentes que le permitan fundamentar su preexistencia y contenido, y las actuaciones se repetirán con las formalidades previstas para cada caso según dicta la normativa legal vigente.

VI. SOBRE LAS COMUNICACIONES FRENTE A UN ATAQUE INFORMÁTICO

I. MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

Municipalidad de Santo Domingo
Plaza del Ca... 2020 0... 10
www.sa...do...

La I. Municipalidad de Santo Domingo notificará a los interesados toda violación de la seguridad que afecte a sus datos personales. No será requerida la notificación cuando:

- Sean implementadas las medidas de seguridad apropiadas como la encriptación.
- Si se han adoptado medidas que impiden que el riesgo pueda ser materializado.
- Si la comunicación corresponde a un esfuerzo desproporcionado.

En caso contrario, el municipio deberá incluir en su notificación lo siguiente:

- Las posibles consecuencias de la violación de la seguridad de sus datos personales.
- Una descripción clara y sencilla de las medidas adoptadas por el municipio, o bien, las propuestas que permiten mitigar la violación de la seguridad de los datos personales y sus posibles efectos.
- Correo electrónico de contacto en el que pueda obtenerse mayor información o para dar respuesta a las susceptibles dudas que puedan surgir.

La I. Municipalidad de Santo Domingo podrá notificar a los funcionarios(as) municipales sobre la violación de seguridad detectada para que sean tomadas las medidas de resguardo frente a posibles afectaciones de su gestión diaria. Adicionalmente, propiciará la localización de puntos utilizados por los terceros para acceder a los datos municipales.

Asimismo, la I. Municipalidad de Santo Domingo podrá tomar contacto con medios de comunicación o terceros que hayan publicado la información sustraída: anunciando que se trata de una información confidencial que ha sido sustraída de manera ilícita, solicitando su retiro a la mayor brevedad posible y requiriendo su colaboración para la posible detección e identificación de los atacantes.

VII. SOBRE EL ENCARGADO DE SEGURIDAD

El Departamento de Informática y Gobierno Electrónico actuará como unidad asesora correspondiente en las materias relativas a seguridad de los documentos electrónicos según lo señalado en la normativa legal.

Las funciones específicas que desempeñe internamente el encargado de seguridad serán establecidas en la resolución que lo designe. En todo caso, deberá tener, a lo menos, las siguientes funciones:

- Tener a su cargo el desarrollo inicial de las políticas de seguridad al interior del municipio y el control de su implementación, y velar por su correcta aplicación.
- Coordinar la respuesta a incidentes computacionales.

- Establecer puntos de enlace con encargados de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias, normas y métodos de seguridad pertinentes.

VIII. DIFUSIÓN Y ACTUALIZACIÓN DEL REGLAMENTO

Será responsabilidad de todos los funcionarios y funcionarias conocer y cumplir con los presentes lineamientos institucionales.

Una vez aprobados por resolución municipal se presumirá conocida por todo el municipio y no podrá ser objeto de alegatos por desconocimiento de ellas, sin perjuicio de la comunicación mediante correo electrónico u otro medio pertinente para conocimiento general.

2. **DÉJESE** sin efecto el Decreto Alcaldicio N° 141 de fecha 29.01.2019, siendo éste un documento estratégico que incorpora herramientas y recomendaciones actualizadas para la gestión municipal.

3. El reglamento y su implementación comenzará a regir a contar de la fecha de publicación de la presente resolución municipal.

Anótese, comuníquese, regístrese y archívese.

I. MUNICIPALIDAD SECRETARIO MUNICIPAL SANTO DOMINGO

RENZZO ROJAS TRONCOSO
SECRETARIO MUNICIPAL

ILUSTRE MUNICIPALIDAD ALCALDE SANTO DOMINGO

DINO LOTITO FLORES
ALCALDE

DRC/LRV/jva
DISTRIBUCIÓN DIGITAL: Administración Municipal, Juzgado de Policía Local, Dirección de Obras Municipales, Dirección de Desarrollo Comunitario, Dirección de Asesoría Jurídica, Dirección de Seguridad Pública, Dirección de Gestión de Riesgos de Desastres, Secretaría Comunal de Planificación, Dirección de Recursos Humanos, Dirección de Tránsito y Transporte Público, Dirección de Medio Ambiente, Aseo y Ornato, Dirección de Gestión Territorial, Dirección de Administración y Finanzas, Dirección de Control Interno, Dirección de Operaciones y Apoyo Logístico, Secretaría Municipal y Archivo Municipal.
INT-DEC-2542-MUNI-2022

Thiare Rubio Gonzalez
Firmado digitalmente por Thiare Rubio Gonzalez
Fecha: 2022.12.23 16:45:46 -03'00'