Ministerio de Vivienda y Urbanismo

Gobierno de Chile

DEJA SIN EFECTO RESOLUCIÓN EXENTA N°2.097, (V. y U.), DE 2019, Y APRUEBA LA POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN PARA EL MINISTERIO DE VIVIENDA Y URBANISMO, SUS SERVICIOS DE VIVIENDA Y URBANIZACIÓN, EL PARQUE METROPOLITANO DE SANTIAGO Y LA SUBSECRETARÍA DE VIVIENDA Y URBANISMO (NIVEL CENTRAL Y SUS SECRETARIAS REGIONALES MINISTERIALES).

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA
08 SEP 2023
RESOLUCIÓN TRAMITADA

SANTIAGO, 08 SEP 2023
HOY SE RESOLVIO LO QUE SIGUE

RESOLUCIÓN EXENTA N° 1508

VISTOS: Lo dispuesto en el D.L N°1305 de 1975 que reestructura y regionaliza el Ministerio de Vivienda y Urbanismo; en el D.S N°83, de 2005, de MINSEGPRES, que aprueba norma técnica para los órganos de la administración del Estado sobre la seguridad y confidencialidad de los documentos electrónicos; D.S N°181, de 2012, del Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la ley 19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; la Norma ISO 27001, sobre Sistema de Gestión de Seguridad de la Información - requisitos; la Política Nacional de Ciberseguridad de Abril de 2017; el Instructivo Presidencial N°8 de 2018 que imparte instrucciones en materia de Ciberseguridad; la Resolución Exenta N°2.097 (V. y U.), de 2019, que aprueba la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo; la Resolución N°1.238, (V. y U.), de 2023 que actualiza la estructura funcional para el Sistema de Seguridad de la Información y Ciberseguridad; el Decreto N°273 de 2022, del Ministerio del Interior que establece la obligación de reportar incidentes de ciberseguridad; y la Resolución N°7, de 2019, de la Contraloría General de la República, que fija normas sobre exención del trámite de toma de razón; y

CONSIDERANDO:

a) Que se han dictado una serie de normas en materias de Seguridad de la Información entre las que se encuentra el Decreto Supremo N°83, de 2005, del Ministerio Secretaría General de la Presidencia, que aprueba norma técnica para los órganos de la administración del Estado sobre seguridad y confidencialidad de los documentos electrónicos; D.S N°181, de 2002, de Ministerio de Economía, Fomento y Turismo, que aprueba reglamento de la Ley N°19.799 sobre documentos electrónicos, firma electrónica y la certificación de dicha firma; la Norma ISO 27001 que proporciona un marco de gestión de Seguridad de la Información utilizable por cualquier tipo de organización, pública o privada; la Política Nacional de Ciberseguridad de Abril de 2017 y el Instructivo Presidencial N°8 de 2018 que imparte instrucciones en materia de Ciberseguridad.

b) La necesidad evaluada, como resultado de la revisión efectuada por parte del Comité de Seguridad de la Información, de reestructurar y ajustar contenidos en la Política General de Seguridad de la Información versión 08, aprobada mediante Resolución Exenta N°2.097, (V. y U.), de 2019.

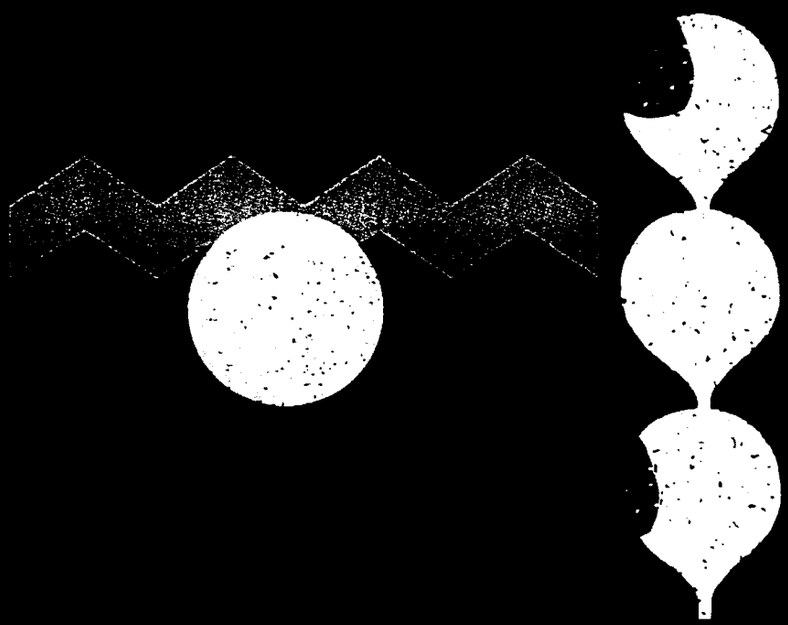
RESOLUCIÓN:

I. Se deja sin efecto, a partir de la total tramitación del presente acto administrativo, la Resolución Exenta N°2.097 (V. y U.) de 2019.

II. Apruébase la Política General de Seguridad de la Información para el Ministerio de Vivienda y Urbanismo, versión 09, para ser implementada en todos los Servicios de Vivienda y Urbanización, en el Parque Metropolitano de Santiago, y en la Subsecretaría de Vivienda y Urbanismo (Nivel Central y todas sus Secretarías Regionales Ministeriales de Vivienda y Urbanismo), la que se detalla a continuación:

Política General de Seguridad de La Información

Ministerio de Vivienda y Urbanismo
Versión 09



Ministerio de Vivienda y Urbanismo

Gobierno de Chile

CONTENIDO

Nota: En el contenido del documento se identifican los cambios respecto a la versión anterior en negrita y cursiva

0. GLOSARIO

Activo de Información	***Información que tiene valor para la institución y por lo tanto se debe proteger, puede tener*** *formato físico, electrónico o verbal, ser equipos o aplicativos, o incluso las personas cuyo conocimiento sirve para los propósitos de la Institución.*
Confidencialidad	***Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados***
Disponibilidad	Propiedad de la información ***de estar accesible y utilizable cuando lo requiera una entidad autorizada***
Documento de Aplicabilidad	Declaración documentada que describe los controles que son relevantes para el Sistema de Gestión de la Seguridad de la Información, en adelante, SGSI, de la organización y aplicables al mismo, así como el rol de cada institución del Ministerio de Vivienda y Urbanismo -en lo sucesivo, MINVU, en la implementación de los controles de la norma ISO 27001.
Incidente de Seguridad de la Información	***Suceso único o serie de sucesos de seguridad de la información inesperados o no deseados que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.***
Información	Toda comunicación o representación de conocimiento como datos, en cualquier forma, tales como formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea digital, en papel, audiovisual u otro.
Integridad	Propiedad de mantener la información con exactitud y completitud.
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información.
Sistema de Gestión de Seguridad de la Información (SGSI)	La parte del sistema de gestión general, basada en un enfoque de riesgo organizacional, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información. Este incluye la estructura organizativa, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los procedimientos, los procesos y los recursos.

1. DECLARACIÓN INSTITUCIONAL

El Ministerio de Vivienda y Urbanismo -MINVU- ha decidido establecer, implementar, mantener y mejorar continuamente un Sistema de Seguridad de la Información -en adelante el SSI-, siendo éste un "compromiso en el fomento y desarrollo de una cultura de seguridad, basado en preservar los principios de confidencialidad, integridad y disponibilidad de la información, en beneficio de ***la ciudadanía*** y partes interesadas para alcanzar los objetivos institucionales, contribuyendo al ***desafío de avanzar hacia una Política Habitacional y Urbana que recupere el Rol del Estado en el fortalecimiento del Derecho a la Ciudad y a una Vivienda Digna y Adecuada, con enfoque territorial y perspectiva de género, poniendo énfasis en la ejecución del Plan de Emergencia Habitacional, el Mejoramiento de Viviendas y Entornos para vivir en Comunidad, la Construcción de Ciudades Justas para el encuentro ciudadano, la recuperación de suelo e inmuebles para las familias y la Modernización de la Gestión***".

Por tal motivo ***la información es un activo esencial para que el MINVU avance al cumplimiento de su misión ministerial, entendiendo*** por activo de información todos aquellos elementos que hacen posible o sustentan los procesos ***operacionales***, como las personas que utilizan la información; los equipos, sistemas e infraestructura que soporta la información; y la información propiamente tal en cualquiera de sus múltiples formatos, incluyendo soporte papel y digital.

Para el desarrollo del SSI, la presente política general, las políticas específicas, procedimientos y otros documentos relacionados, se ajustan a los requerimientos normativos vigentes en seguridad de la información, además de considerar los aspectos pertinentes del marco normativo del MINVU[1].

2. OBJETIVO

El objetivo de este documento es:

- Establecer los lineamientos institucionales y entregar orientación en la implementación del Sistema de Seguridad de la Información del MINVU.
- Definir los objetivos y principios para guiar las actividades relacionadas con la seguridad de la información, ***con el fin de contar con información precisa, completa, y disponible de manera oportuna y así permitir el logro de los objetivos institucionales, la eficiencia de los procesos y el cumplimiento de la legislación***.

2.1 Objetivos de la Seguridad de la Información

El Sistema de Seguridad de la Información del MINVU se alinea y permite soportar los objetivos estratégicos ministeriales definidos en la Ficha de Definiciones Estratégicas A0[2]. ***La institución establece los siguientes*** objetivos de la gestión de seguridad de la información:

- ***Asegurar el cumplimiento de los requisitos normativos, estatutarios, reglamentarios y***

[1] Disponible en www.minvu.cl, enlace "Marco Normativo".

[2] Los objetivos estratégicos ministeriales se encuentran disponibles en la Ficha de Definiciones Estratégicas (Formulario A0) publicado en la Intranet del MINVU.

contractuales, que estén orientados hacia la seguridad de la información.

- *Establecer los niveles de acceso apropiados a la información, brindando y asegurando la confidencialidad, integridad y disponibilidad que requiera cada sistema, proceso, actividad crítica y usuario.*
- *Apoyar al modelo de gestión de continuidad de negocio, a través de acciones tendientes a gestionar los incidentes y a revertir y resolver contingencias que se detecten.*
- *Establecer un marco de Gestión de Riesgo Cibernético para cada sistema, proceso, actividad crítica, que permita alcanzar los objetivos estratégicos.*

Para lo anterior, en el marco del SSI, se establecen ***mediante la implementación de un conjunto de controles aplicables, seleccionados a través de un proceso de gestión de riesgos y la formalización de políticas, procesos, procedimientos para proteger los activos de información en consistencia con los principios establecidos en el punto 5 de esta política.***

3. ÁMBITO DE APLICACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y DEL SSI - ALCANCE

La presente política es aplicable a ***todos*** los procesos[3] ***vinculados a los objetivos ministeriales y productos estratégicos*** del MINVU.

Asimismo, esta política es aplicable a funcionarios de planta, contrata y honorarios, en adelante también "el personal", que forman parte del Ministerio de Vivienda y Urbanismo, o se relacionan con esta Secretaría de Estado, esto es, la Subsecretaría de Vivienda y Urbanismo (Nivel Central y sus SEREMI), todos los SERVIU y el Parque Metropolitano de Santiago, así como también a asesores, consultores, practicantes y personas naturales o jurídicas ***indistintamente de la modalidad de trabajo que realice, ya sea "presencial", "a distancia", "teletrabajo" u otra, en las condiciones que establezca la legislación vigente.***

Para el desarrollo del SSI, se consideran los requisitos de la norma ISO 27001, así como los requisitos regulatorios y legales aplicables identificados en el documento Catastro Normativa MINVU.

Para dar cumplimiento a los requisitos, el MINVU establecerá un conjunto de normas, directrices, procedimientos, instructivos y herramientas de seguridad que permitirán mitigar los riesgos que pudiesen afectar la protección de los activos de información. Esta documentación estará disponible para todo el personal del MINVU en la intranet institucional.

Esta Política genera el marco ministerial de Seguridad de la Información; sin embargo, cada Servicio puede definir las políticas específicas que considere necesarias y que sean de aplicación local; estos documentos no pueden contener elementos que contravengan la presente política, aplicándose además esta última en todos los aspectos no regulados por aquellas.

Existen algunos controles que son abordados en forma transversal, que producto de la dependencia Tecnológica de SERVIU y ***Parquemet*** con la Subsecretaría de V. y U. se tratan desde Nivel Central. Para orientar al respecto el MINVU cuenta con un "Documento de Aplicabilidad", publicado en la Intranet, en el cual se identifican los controles de la norma ISO 27001, su aplicabilidad institucional y el rol de la Subsecretaría, los SERVIU y el ***Parquemet*** en su implementación.

[3] Los procesos se encuentran definidos en el Mapa de Procesos Ministerial.

4. ROLES Y RESPONSABILIDADES

Los roles y responsabilidades para el SSI son definidos por cada Servicio, en cuanto al contenido específico de su composición y funciones, mediante la formalización de un acto administrativo que considera al menos:

- **Encargado/a de Seguridad de la Información**: cuyo rol asesora a la jefatura de cada Servicio en materias relativas a Seguridad de la Información y Ciberseguridad, coordinar las acciones tendientes a cumplir y apoyar los objetivos de seguridad de la información y lidera la identificación de amenazas o riesgos en la seguridad de la información o de sus instalaciones.
- **Comité de Seguridad de la Información** o Comité de similar denominación: formado por un equipo multidisciplinario de alto nivel en cada Servicio que tiene injerencia en las decisiones estratégicas relativas a la seguridad de la información, así como también en la supervisión y monitoreo del SSI.

Cabe destacar que los usuarios, funcionarios de planta, contrata y honorarios que forman parte del Ministerio de Vivienda y Urbanismo, así como también asesores, consultores, practicantes y personas naturales o jurídicas que prestan servicios para el MINVU, son responsables de cumplir las políticas de seguridad de la información del MINVU, asegurar la confidencialidad, disponibilidad e integridad de la información que tienen a su cargo y reportar oportunamente los incidentes de seguridad de la información que detecten en el desarrollo de sus funciones.

5. PRINCIPIOS PARA EL RESGUARDO DE LOS ACTIVOS DE INFORMACIÓN

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

A continuación, se describe cómo el MINVU aborda los principios básicos de Seguridad de la Información:

5.1 De la confidencialidad de los activos de información

El MINVU se compromete a preservar la confidencialidad de la información institucional, estableciendo lineamientos, prácticas de seguridad y mecanismos para clasificar y reconocer la información de carácter confidencial en la gestión interna, que deba ser protegida ante filtración o divulgación no autorizada. Esta clasificación es de carácter interna y diferente de la tipificación del carácter reservado de la información, la cual se encuentra a cargo del equipo de Transparencia en cada Servicio, quienes resguardan el principio de transparencia de la función pública[4] recogido en la Ley N°20.285 sobre Acceso a la Información Pública.

Por lo anterior, y dada la condición pública de la información elaborada con presupuesto de la nación y que obra en poder de los Órganos de la Administración del Estado, es importante señalar que su resguardo no implica desconocimiento ni obstaculización del derecho de toda persona a solicitar y recibir información, en la forma y condiciones que establece la Ley N°20.285.

Además, el resguardo de la información involucra la obligación de las personas que trabajan en el tratamiento de datos personales o que tengan acceso a estos, de guardar secreto sobre los mismos, según lo dispone la Ley N°19.628 de Protección de Datos de Carácter Personal.

De este modo, cada Servicio se compromete a implementar los controles necesarios para garantizar que, tanto la información física como la digital, sea accesible sólo por aquellos usuarios autorizados de acuerdo a la legislación vigente, revisando periódicamente estos lineamientos.

[4] Artículo 5 de la Ley 20.285, que establece el carácter público de la información de los órganos de la Administración del Estado.

5.2 De la integridad de los activos de información

El MINVU establece lineamientos, prácticas de seguridad y mecanismos que resguardan la integridad de los activos de información contenida en cualquier espacio, equipo, sistema o infraestructura, en todos los formatos posibles, salvaguardando además la mayor completitud, coherencia, consistencia y actualización de sistemas y procesos.

5.3 De la disponibilidad de los activos de información

El MINVU asegura la disponibilidad de los activos de información ministerial, incluyendo la disponibilidad de equipos, sistemas e infraestructura que la contengan o la provean en los niveles y tiempos requeridos, tanto a escala interna como externa, estableciendo lineamientos, prácticas de seguridad y mecanismos que prevengan cualquier acción que elimine o exponga la información relevante y que mantengan la continuidad del flujo de información.

6. GESTIÓN DOCUMENTAL DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

6.1 Generación de una política y otros documentos

Las políticas de seguridad de la información se elaboran en base a un formato tipo establecido para dicho propósito publicado en la columna Trabajo Colaborativo SSI en la Intranet institucional. Asimismo, para la implementación operativa de algunas políticas específicas de seguridad, se elaboran procedimientos u otros instrumentos que se alinean con los parámetros establecidos de documentación en cada Servicio.

6.2 Aprobación de una política y otros documentos

La política general y las políticas específicas de seguridad son aprobadas a través de resolución del Jefe de Servicio, facultad que no puede ser delegada.

Otros documentos como normativas, procedimientos e instructivos son aprobados a través de un acto administrativo (Resolución) del Jefe de Servicio, o por aquellos funcionarios en quienes haya sido delegada dicha atribución, dependiendo de los lineamientos y prácticas de seguridad particulares o transversales definidos en cada Servicio, conforme a su estructura y requerimientos de seguridad.

6.3 Difusión de una política y otros documentos

Las versiones vigentes de la presente política y aquella documentación vinculada al Sistema de Seguridad de Información se publica de acuerdo a lo establecido por cada Servicio, asegurando que el contenido de la documentación sea accesible y comprensible para todo ***el personal del MINVU***.

La difusión de la presente política, las políticas específicas de seguridad, los procedimientos y otros documentos, se efectúa a través de los canales de difusión establecidos, pudiendo utilizarse publicación en la Intranet institucional y/o Minvuletín y/o Correo electrónico y/o Afiches y/o volantes, u otro medio que la institución considere pertinente.

Adicionalmente, tanto la política general como las políticas específicas de seguridad de la información se encuentran publicadas en la página web institucional disponible para consulta de personal o terceras partes que prestan servicios para el MINVU y para la ciudadanía en general.

6.4 Revisión de la política

La presente política será revisada al menos una vez al año o cuando el/la Encargado/a de Seguridad de la Información y Ciberseguridad de uno o más Servicios lo requiera, para asegurar su continuidad e idoneidad, considerando los ***resultados de revisiones y auditorías realizadas, y*** los cambios que puedan producirse, tales como:

- ***Nuevas definiciones estratégicas, cambios en la institución y/o enfoques a la gestión de seguridad.***
- ***Incorporación y/o modificaciones relevantes de procesos o actividades críticas de la institución.***
- ***Cambios significativos al soporte tecnológico.***
- ***Cambios significativos en los niveles de riesgo a que se expone la información.***
- ***Modificación y/o creación de leyes o reglamentos que afecten la institución.***
- ***Recomendaciones realizadas por autoridades pertinentes.***
- ***Tendencias relacionadas con amenazas y vulnerabilidades.***

Asimismo, cada Servicio evaluará el cumplimiento de la presente política general, a lo menos cada tres años, mediante auditorías internas, externas y/o revisiones independientes.

7. SANCIONES APLICABLES

El incumplimiento o violación a esta política, conlleva, en el caso de funcionarios del MINVU, la aplicación de alguna de las medidas disciplinarias previstas en el Estatuto Administrativo (censura, multa, suspensión o destitución), previa sustanciación del respectivo proceso disciplinario y en la medida que se acredite en el marco del mismo, responsabilidad administrativa por incumplimiento o violación de esta política; o el término anticipado del contrato por incumplimiento de las obligaciones que el mismo contempla, cuando se trate de personas que no tengan responsabilidad administrativa o empresas que se encuentren dentro del alcance de la presente política. Lo anterior, sin perjuicio de las responsabilidades civiles y penales que se deriven de tales infracciones.

8. CONTROL DE VERSIONES

Versión	Fecha Aprobación	Motivo de la revisión	Autor(es)
07	Octubre 2018	Revisión anual, considera ajuste en la aprobación de documentos por observación formulada por Contraloría General de la República. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Marcela Jara/ Encargada Sección Gestión de Procesos DIFIN.
08	Julio 2019	Revisión anual, considera ajuste en la aprobación de documentos y algunas especificaciones por recomendación de Red de Expertos. Se identifican los cambios en negrita y cursiva.	Leonardo Cavieres/ Encargado Seguridad Informática DINFO; Claudio Paredes/ Jefe de Ingeniería y Explotación de Sistemas DINFO; Ivonne Valdivia / Profesional Depto. Estudios DIVAD; Marcela Jara/ Analista Dpto. de Planificación y Control de Gestión DIFIN; M. Paula Melis Otonel/ Contralora Interna SERVIU Araucanía.
09	Julio 2023	***Revisión anual. Se identifican los cambios en negrita y cursiva.***	Ivonne Valdivia / DIVAD; Marcela Jara/ DIFIN; Tomás Yanquez/DIFIN; Leonardo Cavieres/ DINFO; Claudio Paredes/ DINFO; Erick Atenas/ DINFO; M. Paula Melis Otonel/ Contralora Interna SERVIU Araucanía; Alexis Cornejo Marín/ Unidad de Informática SERVIU Atacama; Marcelo López Otárola/ Depto. Programación Física y Control SERVIU Biobío.

Revisión:	Gabriela Elgueta Poblete/ Subsecretaria de Vivienda y Urbanismo. Vania Navarro Morales/ Encargada de Seguridad de la Información y Ciberseguridad, Jefa División de Finanzas Eduardo Gonzalez Yañez/Encargado Técnico de Seguridad Informática y Ciberseguridad, Jefe División Informática Comité de Seguridad de la Información Subsecretaría de V. y U. Encargados/as de Seguridad de la Información de SERVIU y Parque Metropolitano.
Aprobación:	Carlos Montes Cisternas / Ministro de Vivienda y Urbanismo.

III. Establécese la obligación de los/as Encargados/as de Seguridad de la Información y Ciberseguridad de la Subsecretaría de V. y U., los SERVIU y el Parque Metropolitano de Santiago de efectuar la difusión de la política fijada por este instrumento a todos los equipos de trabajo, así como realizar todas las acciones tendientes a su implementación y velar por su estricto cumplimiento.

IV. Se deja constancia que la presente Resolución no irroga gastos para el presupuesto de este Ministerio, ni para los Servicios que se relacionan con el Gobierno por su intermedio.

ANÓTESE, COMUNÍQUESE, CÚMPLASE Y ARCHÍVESE.

MINISTERIO DE VIVIENDA Y URBANISMO
MARCELA RIVAS CERDA
Jefa
DIVISIÓN JURÍDICA

Ministerio de Vivienda y Urbanismo
Gabinete del Ministro

CARLOS MONTES CISTERNAS
MINISTRO DE VIVIENDA Y URBANISMO

MINISTERIO DE VIVIENDA Y URBANISMO
SUBSECRETARIA

GEP/CGBM/MRC/MJGB/EGY/VNM/MJC

DISTRIBUCIÓN:

- Gabinete Ministro V. y U.
- Gabinete Subsecretaria V. y U.
- SEREMI (16)
- Directores/as SERVIU (16)
- Director/a PARQUEMET
- Divisiones Nivel Central (7)
- Auditoría Interna Ministerial
- Contraloría Interna Ministerial
- Comisión Asesora para la Reducción de Riesgos de Desastres y Reconstrucción
- Sistema Integrado de Atención a la Ciudadanía (SIAC)
- Depto. Comunicaciones
- Centro de Estudios de Ciudad y Territorio (CECYT)
- Equipo de Estudios Económicos y de Procesos-DIFIN
- Sección Partes y Archivos

LO QUE TRANSCRIBO PARA SU CONOCIMIENTO

GABRIELA ELGUETA POBLETE
SUBSECRETARIA DE VIVIENDA Y URBANISMO