Ministerio del Interior y Seguridad Pública

Subsecretaría de Prevención del Delito

Subsecretaría de Prevención del Delito
Ministerio del Interior y Seguridad Pública
Gobierno de Chile

Política General de Seguridad de la Información

La información contenida en este documento es de propiedad de la Subsecretaría de Prevención del Delito, por lo tanto cualquier uso, reproducción, divulgación, distribución no autorizada ya sea parcial o total de su contenido está prohibida y podría ser sancionado.

Este documento es de origen electrónico, una vez impreso pasa a ser copia no controlada y podría estar obsoleto. Para ver la versión vigente debe dirigirse a http://dms.spd.gov.cl/sitios/seguridad

16255165

Contenido

1 INTRODUCCIÓN 3
2 OBJETIVO 3
3 ALCANCE 3
4 ACRÓNIMOS 3
5 DEFINICIONES 4
6 POLÍTICAS DE SEGURIDAD 6
6.1 Principio de Constitucionalidad y Legislación 6
6.2 Seguridad de la Información en la Institución 6
6.3 Implementación de Seguridad de la Información 6
6.4 Responsabilidad de las Personas 6
6.5 Organización de la Seguridad 6
6.6 Gestión de Activos de Información 7
6.7 Seguridad Ligada a las Personas 7
6.8 Seguridad Física y Ambiental 7
6.9 Seguridad en las Comunicaciones y Operaciones 7
6.10 Seguridad en el Acceso a la Información 8
6.11 Seguridad en la Adquisición, Desarrollo y Mantención de Sistemas de Información 8
6.12 Gestión de Incidentes de Seguridad 8
6.13 Gestión de la Continuidad de Negocio 8
6.14 Gestión del Cumplimiento Normativo 9
7 ROLES Y RESPONSABILIDADES 9
7.1 Subsecretario(a) de la Institución 9
7.2 Comité de Seguridad de la Información 9
7.3 Encargado(a) de Seguridad de la Información 9
7.4 Auditoría Interna 10
7.5 Funcionarios(as) y Terceros Relacionados 10
8 METODOLOGÍAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN 10
8.1 Metodología de Gestión de Seguridad 10
8.2 Metodología de Gestión de Riesgos 10
9 OBSERVANCIA DE POLÍTICAS, NORMATIVAS, ESTÁNDARES Y PROCEDIMIENTOS 10
9.1 Responsabilidad por Incumplimiento 10
10 DIFUSIÓN Y REVISIÓN 11
10.1 Difusión de la Política 11
10.2 Revisión de la Política 11
10.3 Revisión de Cumplimiento de la Política 11
11 CONTROL DOCUMENTAL 12
11.1 Control de Revisión 12
11.2 Control de Aprobación 12
11.3 Control de Cambios 13
11.4 Publicación y Difusión 14

1 INTRODUCCIÓN

La Subsecretaría de Prevención del Delito, que de acuerdo con lo previsto en la Ley N° 20.502, es el órgano de colaboración inmediata del Ministro del Interior y Seguridad Pública en todas aquellas materias relacionadas con la elaboración, coordinación, ejecución y evaluación de políticas públicas destinadas a prevenir la delincuencia, a rehabilitar y a reinsertar socialmente a los infractores de ley, sin perjuicio del ejercicio de las atribuciones que el Ministro le delegue, así como del cumplimiento de las tareas que aquél le encargue, considera relevante e imprescindible resguardar de manera adecuada y eficientemente la información que posee para el cumplimiento de sus objetivos.

En relación a esto, se declara la necesidad de gestionar la Política General de Seguridad de la Información de la Subsecretaría de Prevención del Delito, esto con la finalidad de identificar, evaluar y controlar los riesgos que pudieran afectar la confidencialidad, integridad y disponibilidad de la información de la Institución.

2 OBJETIVO

La Política General de Seguridad de la Información, tiene como objetivo establecer el lineamiento institucional de la Subsecretaría de Prevención del Delito referente a la responsabilidad, resguardo y gestión de riesgos de la información, como también entregar las directrices generales sobre el acceso, manipulación, procesamiento, transmisión, protección, almacenamiento o cualquier otro tratamiento que se realice sobre los activos de información de la Institución.

3 ALCANCE

Esta Política es aplicable a los principales activos de información que están relacionados a los productos declarados en la ficha de definiciones estratégicas de la Subsecretaría de Prevención del Delito para el período 2018 al 2022 considerando sus áreas, departamentos, programas de gobierno, personas, instalaciones, procesos internos, sistemas informáticos, infraestructura tecnológica, redes de comunicación, bases de datos, archivos y datos, documentos físicos, entre otros, como también es extensible a terceros que mantengan contratos de prestación de servicios con la Institución.

4 ACRÓNIMOS

S.G.S.I. : Sistema de Gestión de Seguridad de la Información.

S.S.P.D. : Subsecretario(a) de la Subsecretaría de Prevención del Delito.

I.S.O. : Organización Internacional de Estándares.

I.E.C. : Comisión Electrotécnica Internacional.

5 DEFINICIONES

Seguridad de la Información	:	Conjunto de procesos, metodologías, políticas, normativas, estándares, procedimientos, controles, software, hardware, y otros elementos necesarios para mantener la confidencialidad, integridad y disponibilidad de la información.
Activo de información	:	Recurso del sistema de información como personas, instalaciones, procesos, archivos digitales, documentos físicos, base de datos, intangibles e información en general, entre otros, necesario para que la Institución funcione correctamente y alcance los objetivos propuestos.
Tratamiento de información	:	Actividad de creación, digitación, transmisión, procesamiento, almacenamiento, modificación, eliminación, consulta, o cualquier otra acción que diga relación con manipulación de información.
Proceso	:	Conjunto de actividades o eventos que se realizan de manera estructurada o alternativa con el fin de cumplir un objetivo determinado.
Confidencialidad	:	Propiedad de la información que apunta a que el acceso a la información, sólo pueda ser realizado por personas, sistemas o entidades autorizadas para hacerlo.
Integridad	:	Propiedad de la información que apunta a mantener la exactitud y totalidad de la información, como también los métodos y mecanismos de tratamiento en general.
Disponibilidad	:	Propiedad de la información que apunta a que los usuarios autorizados, tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
Sistema de información	:	Uno o más computadores, software asociado, hardware y periféricos, terminales, procesos físicos, medios de transferencia, bases de datos, entre otros, que forman un todo autónomo capaz de realizar tratamiento de información.
Riesgo de información	:	Cualquier acción o situación que podría afectar las propiedades de la información y a su vez ocasionar resultados no esperados para la Institución.
Evento de seguridad	:	Ocurrencia anómala de un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información o a la falla de controles establecidos, pudiendo ser desconocida y que podría afectar la seguridad de niveles menores a moderados, tales como violaciones a la política, instalación no autorizada de software, accesos denegados a un servidor, etc. y en ningún caso afectando la continuidad operacional.

Incidente de seguridad	:	Materialización de algún riesgo significativo conocido o desconocido para la Institución, o también se entenderá como tal la sumatoria de eventos de seguridad relacionados que afecten de manera considerable al Organismo, tales como acciones que afecten de manera negativa la imagen Institucional; desastres naturales menores que inhabiliten temporalmente las instalaciones de procesamiento; fallas tecnológicas críticas que interrumpan temporalmente la continuidad de las operaciones, entre otros.

6 POLÍTICAS DE SEGURIDAD

6.1 Principio de Constitucionalidad y Legislación

La Política de Seguridad de la Información deberá mantener un lineamiento acorde a las directrices definidas por la Institución, siempre considerando el marco constitucional y legislativo vigente en nuestro país, particularmente lo referido a los derechos y libertades de las personas y otras leyes aplicables al campo de la información y la tecnología.

6.2 Seguridad de la Información en la Institución

Se declara que todo activo de información que sea propio a realizar su tratamiento por personas, sistemas o cualquier otra entidad al interior de la Subsecretaría de Prevención del Delito o por terceros, deberán implementar los mecanismos necesarios para resguardar la confidencialidad, integridad y disponibilidad de la información, permitiendo controlar los riesgos inherentes a los cuales por su naturaleza pueda verse expuesta.

6.3 Implementación de Seguridad de la Información

La implementación se llevará a cabo de manera continua a través de un proceso de mejora en la seguridad, el cual deberá considerar prioritariamente la información de mayor valor para la Institución, abarcando los programas de gobierno y productos estratégicos, y posteriormente extendiéndose a los procesos y áreas de soporte de la Subsecretaría de Prevención del Delito.

6.4 Responsabilidad de las Personas

Toda persona, ya sea funcionario(a) o personal externo a la Institución y que tenga acceso a información de esta, será responsable de mantener el resguardo adecuado de la seguridad de los datos, para lo cual se destinará la siguiente clasificación de tipos de usuarios(as):

- Propietario(a) de información: Persona responsable de una información en particular, como también de su valorización y clasificación.
- Administrador(a) de información: Persona encargada de resguardar la información y administrar las definiciones establecidas por el propietario de la información.
- Usuario(a) de información: Persona que solicita acceso para realizar tratamiento sobre la información resguardada por el Administrador de información.

6.5 Organización de la Seguridad

La Subsecretaría de Prevención del Delito mantendrá una adecuada organización relacionada a la seguridad de la información, para lo cual gestionará a través de un Comité de Seguridad de la Información y/o el Encargado(a) de Seguridad de la Información, normativas, estándares, procedimientos o cualquier otro mecanismo de control que ayuden a mejorar el S.G.S.I. de la Institución.

La facultad que mantiene tanto el Comité como el Encargado(a) de Seguridad de la Información para dictaminar marcos de trabajo de seguridad, contempla también la relación con entidades externas a la Institución y/o terceros que presten servicios de cualquier índole a la Subsecretaría de Prevención del Delito.

6.6 Gestión de Activos de Información

Para hacer más eficiente el proceso de implementación del S.G.S.I., la Institución desarrolla estrategias focalizadas de trabajo para optimizar el uso de los recursos de seguridad, por lo mismo se establecen métodos para la identificación, clasificación y valorización de los activos de información, considerando también la asignación de responsabilidades sobre su tratamiento, permitiendo mantener claramente identificación sobre los activos de información relevante para la Institución y mantener mecanismos acordes para el control de los riesgos de información.

6.7 Seguridad Ligada a las Personas

Debido a la importancia que tienen las personas en la Institución, se considera fundamental gestionar la seguridad de la información aplicada al ciclo de vida de las personas y mientras presten servicios para la organización, por lo mismo se incorporarán términos legales de confidencialidad y responsabilidades de seguridad en los contratos y descripciones de cargos, adicionalmente se desarrollarán planes orientados a incorporar la cultura de seguridad en los funcionarios(as) y en su quehacer laboral, en conjunto con otros mecanismos complementarios a este ámbito, permitiendo entregar un apoyo permanente a la gestión del cambio frente a temas de seguridad de la información en las personas.

6.8 Seguridad Física y Ambiental

Los activos de información físicos, tales como centros de atención o denuncia, oficinas administrativas, áreas de procesamiento de información, equipos tecnológicos y de soporte, información en medios físicos, entre otros, son base para el cumplimiento de los objetivos de la Institución, por lo mismo se mantendrán normativas, controles y otros mecanismos que resguarden la seguridad de las instalaciones y ambientes de trabajo, el acceso a las áreas, el manejo de los documentos, los mecanismos físicos para el tratamiento de la información, el hardware que da soporte a los procesos, entre muchos otros, permitiendo garantizar la protección de los activos de información frente a amenazas físicas, ambientales y naturales.

6.9 Seguridad en las Comunicaciones y Operaciones

Gran parte de la información que se manipula en la Institución se encuentra en formato digital, por lo mismo se considera de vital necesidad gestionar los riesgos asociados a las comunicaciones y operaciones relacionados a los activos de información, el definir responsabilidades y segregación de funciones, documentar las operaciones en el tratamiento de información, establecer criterios de calidad para la aceptación de los sistemas de información, administrar planes de respaldo, implementar mecanismos de monitoreo y supervisión, como también en el manejo de los soportes y la seguridad de la redes tecnológicas, permiten entregar un grado razonable en el resguardo de los activos de información y un cumplimiento adecuado de la política Institucional de seguridad.

La gestión de los servicios entregados por terceros, sobre la cual es requisito obligatorio la supervisión y revisión de los acuerdos de niveles de servicio establecidos, tanto en el ámbito de la calidad como en la seguridad en que son prestados, además de la gestión de cambios entre las partes y sobre todo en los acuerdos de confidencialidad y el intercambio de información con entidades externas a la Subsecretaría de Prevención del Delito, como también áreas internas de la institución, velando en todo momento por preservar la protección y el resguardo de la información.

6.10 Seguridad en el Acceso a la Información

La Institución considera fundamental controlar el acceso a los activos de información para mantener su confidencialidad principalmente, por tanto los archivos digitales, documentos electrónicos, bases de datos, software y aplicativos, entre otros, son componentes esenciales para lograr el cumplimiento de los objetivos de la Institución, por lo mismo y en relación a este principio es que los sistemas de información del organismo cuentan con medidas de control que son adecuadas para mantener el resguardo de la información, considerando normativas de acceso, gestionando cuentas de usuarios autorizados, estableciendo responsabilidades por parte de las personas, controlando el ingreso a las redes de comunicación y equipos computacionales, como también aplicando mecanismos de protección de acceso sobre las aplicaciones y la información de la Institución, tratando de evitar en todo momento que pueda verse afectada por el acceso o la manipulación no autorizada.

6.11 Seguridad en la Adquisición, Desarrollo y Mantención de Sistemas de Información

La Institución cuenta con sistemas de información que dan soporte a los procesos internos y programas estratégicos de la Subsecretaría de Prevención del Delito, con lo cual permite entregar una mayor calidad y seguridad en la ejecución de las actividades y optimizar el uso de los recursos informáticos, sin embargo la incorporación de nuevas tecnologías en la organización también incorpora riesgos que son propios de esta, por lo mismo la institución mantiene mecanismos que permitan controlar estos riesgos a través de normativas y estándares base de requerimientos de seguridad, metodologías y procesos formales para la construcción de sistemas, implementación de controles criptográficos, como también actividades de aseguramiento de software.

Por otra parte, los sistemas de información que se encuentran en producción cuentan con medidas de control que permitan resguardar adecuadamente los archivos de sistema y la información sobre la cual se realiza tratamiento, normativas y herramientas de gestión de cambios y de configuración, son acciones que ayudan al cumplimiento de esta política y en el logro de los objetivos de la Institución.

6.12 Gestión de Incidentes de Seguridad

La retroalimentación de parte de las personas y entidades es base para mejorar el control interno de la Institución, por lo mismo se desarrollan canales de comunicación para la notificación de eventos, debilidades y oportunidades de mejora en el S.G.S.I., como también se establecen equipos de respuesta frente a eventuales incidentes que puedan afectar la seguridad de la información, considerando el análisis y aprendizaje de los efectos generados por dichas situaciones e implementando mecanismos que permitan prevenir o detectar su ocurrencia, además de minimizar su impacto y/o probabilidad, apoyando la mejora continua del sistema de seguridad.

6.13 Gestión de la Continuidad de Negocio

Los productos estratégicos son la cadena de valor de la Subsecretaría de Prevención del Delito, por lo mismo se deben implementar los mecanismos necesarios para mantener su continuidad operacional frente a situaciones que pudieran afectar prioritariamente su disponibilidad, donde la infraestructura, la tecnología, los procesos, las personas y la información son la base fundamental sobre la cual se centran los planes de continuidad de negocio, los que a través de la gestión de riesgos, el análisis de impacto, el desarrollo de estrategias y los planes de contingencia y recuperación, permiten garantizar razonablemente la operación de los productos estratégicos de la Institución.

6.14 Gestión del Cumplimiento Normativo

El marco regulatorio, legislativo y constitucional de nuestro país representa los límites de aplicabilidad de esta política, como también obliga el cumplimiento de la normativa vigente relacionada a la información y la tecnología, leyes relacionadas a la propiedad intelectual, el manejo de datos personales, los documentos electrónicos y la firma digital, los delitos penales asociados a la tecnología y los sistemas de información, o sobre las comunicaciones y su privacidad, la política nacional de ciberseguridad, entre otras, así como también el marco normativo interno de seguridad de la información, son considerados relevantes para la Institución, por lo mismo se mantienen herramientas de auditoría en los sistemas de información y un adecuado control a través de entidades independientes y objetivas podrán monitorean y supervisan periódicamente su cumplimiento.

7 ROLES Y RESPONSABILIDADES

7.1 Subsecretario(a) de la Institución

Responsable de liderar la implantación y mejora continua del S.G.S.I., en donde sus funciones claves son de aprobar políticas y validar el proceso de gestión de Seguridad de la Información, como también de aprobar las estrategias y mecanismos de control para el tratamiento de riesgos, además de colocar a disposición los recursos necesarios para su ejecución.

7.2 Comité de Seguridad de la Información

Responsable de gestionar la Política de Seguridad de la Información, en donde sus funciones claves son de asegurar que las actividades sean ejecutadas en conformidad con la política de seguridad de la información, definir y aprobar la implementación de normas vinculados a la política de seguridad de la información, identificar y evaluar las acciones correctivas para dar solución a las observaciones de auditoría, aprobar las metodologías y procesos relacionados a la evaluación del riesgo y la seguridad de la información, identificar cambios significativos que pudieran generar riesgos en el procesamiento de la información, proponer soluciones y evaluar la idoneidad y coordinación en la implementación de los controles de seguridad de información, establecer medios para la concientización y capacitación del personal en temas de seguridad de la información, arbitrar conflictos en materia relacionada a la seguridad de la información, sus riesgos y soluciones, evaluar la información recibida de los incidentes de seguridad de la información, emitiendo recomendaciones para su prevención, detección y corrección, como también reportar a la Alta Dirección, respecto a oportunidades de mejora en el S.G.S.I., así como de los incidentes relevantes y su solución.

7.3 Encargado(a) de Seguridad de la Información

Responsable de asesorar al Jefe(a) de Servicio y coordinar actividades de gestión de seguridad relativas a la información, en donde sus funciones claves son de proponer políticas y normativa a la Alta Dirección y al Comité de Seguridad de la Información para su aprobación y velar por su correcta aplicación, coordinar la respuesta a incidentes de seguridad que afecten a los activos de información que dan soporte a los procesos institucionales, establecer puntos de enlace con encargados(as) de seguridad de otros organismos públicos y especialistas externos que le permitan estar al tanto de las tendencias en materia de seguridad de la información, gestionar la creación y/o aprobación de estándares y procedimientos documentados operativos de seguridad para el tratamiento de los activos de información, proponer al responsable por omisión de los documentos electrónicos de esta Subsecretaría conforme al artículo 14° del Decreto Supremo N° 83 de 2004 emitida por el Ministerio Secretaría General de la Presidencia, formular los planes de contingencia para asegurar la continuidad de las operaciones críticas de esta Subsecretaría, conforme al artículo 35 del Artículo primero del Decreto Supremo N° 83 de 2004 emitida por el

Ministerio Secretaría General de la Presidencia, monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos, como también mantener la coordinación con otras unidades del Servicio para apoyar los objetivos de seguridad.

7.4 Auditoría Interna

Otorgar aseguramiento a la Dirección sobre el cumplimiento de la Política de Seguridad de la Información, a través de las actividades de auditoría que se encuentren programadas o le sean encomendadas.

7.5 Funcionarios(as) y Terceros Relacionados

Responsable de dar cumplimiento a la Política de Seguridad de la Información y sus normativas, además del deber de informar sobre incidentes de seguridad o acciones que transgredan los objetivos declarados o que puedan afectar la confidencialidad, integridad y disponibilidad de la información de la Institución.

8 METODOLOGÍAS DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN

8.1 Metodología de Gestión de Seguridad

La Institución adoptará para todo efecto lo dictado en la norma estándar NCh ISO/IEC 27001 Of.2013 y NCh ISO/IEC 27002 Of.2013, sin embargo para ámbitos específicos y de contribuir de mejor manera a esta política, se considerarán otras normativas existentes relacionadas a las anteriores, constituyéndose en la base fundamental de todo el marco de gobernabilidad del Sistema de Gestión de Seguridad de la Información.

8.2 Metodología de Gestión de Riesgos

La Institución adopta la metodología establecida por la Dirección de Presupuestos o Red de expertos designada para la gestión de riesgos de la información y su tratamiento de control, la cual se encuentra documentada a través de la Guía Metodológica emitida por dichos Organismos, siendo consistente y alineada con lo establecido en las mejores prácticas de gestión de riesgo.

9 OBSERVANCIA DE POLÍTICAS, NORMATIVAS, ESTÁNDARES Y PROCEDIMIENTOS

9.1 Responsabilidad por Incumplimiento

Todo incumplimiento de las políticas, normativas, estándares y/o procedimientos de seguridad, esto bajo el marco de la normativa legal vigente y/o el Estatuto Administrativo según corresponda, por parte de cualquier servidor(a) que se desempeñe en la Institución será evaluado por el Comité de Seguridad de la Información quién deberá informar del hecho al S.S.P.D. para que determine de ser procedente la instrucción de un proceso disciplinario.

10 DIFUSIÓN Y REVISIÓN

10.1 Difusión de la Política

La difusión de esta política se realizará mediante correo electrónico a todo el personal de la Subsecretaría de Prevención del Delito y terceros relacionados contractualmente, además su versión digitalizada quedará a disposición en el sitio Web interno y externo de la Institución para facilitar su acceso y conocimiento.

10.2 Revisión de la Política

La revisión formal de esta política se realizará a lo menos cada 3 años desde la fecha de su publicación por el Comité de Seguridad de la Información, sin embargo bajo circunstancias que estimen conveniente, la política será revisada a intervalos menores según sea necesario para mantener una adecuado lineamiento con la misión y objetivos de la Institución.

10.3 Revisión de Cumplimiento de la Política

El Departamento de Auditoría Interna de la Institución tendrá la responsabilidad de llevar a cabo el aseguramiento de aspectos generales en relación al cumplimiento de esta política, el cual se desarrollará de manera anual como parte del programa de actividades de auditoría que sean realizadas en las diferentes áreas del Organismo.

11 CONTROL DOCUMENTAL

11.1 Control de Revisión

Nombre	Cargo	Actividad	Firma
Ariel Severino Fuentes	Encargado de Seguridad de la Información.	Creación del documento	
Dominique Díaz Rohde	Encargada PMG Seguridad de la Información.	Revisión del documento	
Mauricio Toro Rojas	Jefe Departamento Gestión de Personas.	Revisión del documento	
Alejandro Yuretic de la Cuadra	Jefe Departamento de Informática.	Revisión del documento	
Juan Salazar Lorca	Jefe Departamento de Administración.	Revisión del documento	
Juan Francisco García Mac-Vicar	Jefe División de Administración, Finanzas y Personas.	Revisión del documento	

11.2 Control de Aprobación

Nombre	Cargo	Fecha	Firma
Katherine Martorell Awad	Subsecretaria de Prevención del Delito.	17-01-18	

11.3 Control de Cambios

Versión	Cambio	Fecha	Aprobador
1.0	Aprobación y difusión del documento.	02.08.2012	Cristobal Lira Ibáñez
2.0	Incorporación de términos legales y responsabilidad en el punto 6.7 Seguridad Ligada a las Personas. Revocación de reportar monitoreo en el punto 7.2 al Comité de Seguridad de la Información. Adecuación de nuevas funciones en el rol 7.3 Encargado(a) de Seguridad de la Información. Modificación en el punto 5 de definición de incidente de seguridad e incorporación de evento de seguridad. Modificación en las políticas 6.12 de Gestión de Incidentes de Seguridad. Se incorpora el punto 10.3 que hace referencia a la revisión del cumplimiento de la política.	02.09.2013	Cristóbal Lira Ibáñez
3.0	Se modifica alcance para ser ajustado a las definiciones estratégicas establecidas en la ficha A1. Se elimina de la política el atributo de legalidad de la información, ajustando propiedades a lo establecido por la Dirección de Presupuesto. Se modifica la metodología ISO/IEC 27.001:2009 que apoya el sistema de gestión por su nueva versión ISO/IEC 27.001:2013.	25.08.2015	Antonio Frey Valdés
4.0	Se incorpora como parte de la política de cumplimiento normativo los aspectos de ciberseguridad en el punto 6.14. Se adecúa documento para dar cumplimiento a los aspectos de equidad de género.	03.05.2018	Katherine Martorell Awad

11.4 Publicación y Difusión

Listado de Distribución
• Intranet de la Subsecretaría de Prevención del Delito. • Correo electrónico a todos(as) los(as) usuarios(as) del servicio.