



REF: APRUEBANSE NUEVAS POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN QUE SE INDICAN.

RESOLUCIÓN EXENTA N° 4604

SANTIAGO, 19 DIC 2019

VISTOS:

Lo dispuesto en los artículos 5º N°s 1, 12, y 13 del D.L. N° 2.465, de 1979; en los D.S. N°s 356, de 1980 y 307, de 2018, ambos del Ministerio de Justicia y Derechos Humanos; en los D.S. N°s 83 de 2005, 93 de 2006 y 14 de 2014 todos, del Ministerio Secretaría General de la Presidencia; en la Norma Chilena NCH-ISO 27001:2013; en la Ley N°20.285; en el D.F.L. N° 29, del Ministerio de Hacienda, que fija texto refundido, coordinado y sistematizado de la Ley N° 18.834, sobre Estatuto Administrativo; la Resolución Exenta N° 2269, de 9 de julio de 2019, de la Dirección Nacional del SENAME; el Memorandum N° 457, de 13 de diciembre de 2019, del Departamento de Planificación y Control de Gestión; en la Resoluciones N° 7 y 8, de 2019, de la Contraloría General de la República.

CONSIDERANDO:

- 1º. Que, el Servicio Nacional de Menores es el organismo del Estado que tiene por misión contribuir a proteger y promover los derechos de los niños, niñas y adolescentes que han sido vulnerados en el ejercicio de los mismos y a la inserción social de adolescentes que han infringido la ley penal.
- 2º. Que, en cumplimiento de sus funciones propias, el SENAME reconoce que la información es un recurso que, como el resto de los activos, tiene valor para la Institución, debiendo consecuentemente ser protegida. La pérdida parcial de información podría tener consecuencias graves para la gestión, debiendo implementarse mecanismos para garantizar la seguridad en el funcionamiento de equipos, datos y sistemas de soporte.
- 3º. Que, el Decreto Supremo N° 83, de 2004, del Ministerio Secretaría General de la Presidencia, aprobó Norma Técnica para los Órganos de la Administración del Estado sobre Seguridad y Confidencialidad de los Documentos Electrónicos. Asimismo, la Norma Chilena Oficial NCh-ISO 27001:2013, proporciona un marco de gestión de Seguridad de la Información utilizable en cualquier tipo de organización, pública o privada.
- 4º. Que, a través de la Resolución Exenta N° 2269, de 9 de julio de 2019, de la Dirección Nacional del SENAME, se designó al Encargado (Titular y Subrogante), de Seguridad de la Información, así como también a los integrantes (Titulares y Subrogantes) del Comité de Seguridad de la Información.
- 5º. Que, por Resolución Exenta N° 3026, de 7 de diciembre de 2017, de la Dirección Nacional del SENAME, se aprobaron las siguientes Políticas del Sistema de Gestión de Seguridad de la Información:
 - SGSI.PO.01 Política General del Sistema de Gestión de Seguridad de la Información
 - SGSI.PO.02 Política de Escritorios y Pantallas Limpias
 - SGSI.PO.03 Política de Gestión de Redes
 - SGSI.PO.05 Política de Respaldo y Recuperación de Información
 - SGSI.PO.09 Política de Acceso y Perímetro de Seguridad Física
 - SGSI.PO.10 Política de Dispositivos Móviles y Medios Removibles
 - SGSI.PO.11 Política Uso de Internet y Correo Electrónico
- 6º. Que, el acto administrativo singularizado en el considerando precedente fue modificado por la Resolución Exenta N° 3580, de 28 de noviembre de 2018, del SENAME, en el sentido de sustituir la General del Sistema de Gestión de Seguridad de la Información, e incorporar dos 2 nuevas políticas a dicho Sistema:
 - SGSI.PO.01 Política General del Sistema de Gestión de Seguridad de la Información
 - SGSI. PO.12 Política de Transferencia de Información y Acuerdos de Confidencialidad.

1985

- SGSI.PO.13 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas.

7º. Que, el Departamento de Planificación y Control de Gestión, a través de su Memorandum N° 457, de 13 de diciembre de 2019, solicitó proceder a la actualización del texto de las políticas existentes y la incorporación de tres nuevas Políticas al Sistema de Gestión de Seguridad de la Información, como se señala a continuación:

- SGSI.PO.01 Política General (Sustitución)
- SGSI.PO.02 Política de Escritorios y Pantallas Limpias (Sustitución)
- SGSI.PO.03 Política de Gestión de Redes (Sustitución)
- SGSI.PO.05 Política de Respaldo y Recuperación de Información (Sustitución)
- SGSI.PO.09 Política de Control de Acceso y Perímetro de Seguridad Física (Sustitución)
- SGSI.PO.10 Política de Dispositivos Móviles, Medios Removibles (Sustitución)
- SGSI.PO.11 Política de Uso de Internet y Correo Electrónico (Sustitución)
- SGSI.PO.12 Política de Transferencia de Información y Acuerdos de Confidencialidad (Sustitución)
- SGSI.PO.13 Política de Adquisición, Desarrollo y Mantenimiento de Sistemas (Sustitución)
- SGSI.PO.14 Política de Controles Criptográficos (Nueva)
- SGSI.PO.15 Política de Continuidad Operativa (Nueva)
- SGSI.PO.16 Política de Seguridad con Proveedores (Nueva)

RESUELVO:

1º APRUÉBANSE los textos de las Políticas del Sistema de Gestión de Seguridad de la Información, singularizadas en el considerando séptimo del presente acto administrativo, siendo su texto el siguiente:

I.

**POLÍTICA GENERAL
SISTEMA DE GESTIÓN DE
SEGURIDAD DE LA INFORMACIÓN
SGSI.PO.01**

1. INTRODUCCIÓN

El Servicio Nacional de Menores (SENAME) es un organismo gubernamental centralizado y dependiente del Ministerio de Justicia. Fue creado por el Decreto de Ley N° 2.465 del 10 de enero de 1979, que fija el texto de su Ley Orgánica, y fue publicado en el Diario Oficial el 16 de enero del mismo año.

El SENAME tiene como objetivos estratégicos institucionales:

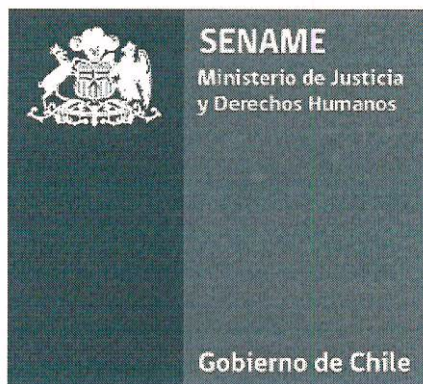
- Restituir y/o reparar los derechos vulnerados de los niños/as y adolescentes por medio de prestaciones de protección.
- Reinsertar socialmente a adolescentes imputados y/o condenados/as conforme a estándares definidos por la Ley 20.084.
- Promover los derechos y prevenir la vulneración de los mismos para niños/as y adolescentes.
- Supervisar la atención de los niños/as y adolescentes atendidos en la oferta del Servicio como a su vez el uso eficiente de los recursos, a fin de mejorar la calidad de las prestaciones dando cumplimiento a los estándares establecidos por el Servicio en concordancia con mandatos legales aprobados por el Estado de Chile.
- Actualizar continuamente la oferta dedicada a la atención de niños, niñas y adolescentes vulnerados/as en sus derechos y la rehabilitación de adolescentes que han infringido la ley, a fin de adecuarlas a las políticas nacionales e internacionales sobre la materia y mandatos legales aprobados por el Estado de Chile y en conformidad a estándares de calidad.

El SENAME reconoce que la información es un recurso que, como el resto de los activos, tiene valor para la Institución y, por consiguiente, debe ser debidamente protegida. La pérdida parcial de información podría tener consecuencias graves para la gestión y, por ende, se deben implementar las salvaguardas adecuadas para garantizar que los equipos, datos y los sistemas que los soportan, sean seguros.

Por esta razón, se establece esta Política del Sistema de Gestión de Seguridad de la Información, el cual tiene como objetivo proteger los activos de Información de una amplia

POLÍTICA USO DE INTERNET Y CORREO ELECTRÓNICO

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN



SGSI.PO.11

Información del Documento

REV 01	ELABORADO POR	REVISADO POR	APROBADO POR
Nombre	Hector Burgos Cañete Encargado Sistema de Gestión de Seguridad de la Información	Cristian Castillo Silva Jefe Departamento de Planificación y Control de Gestión	Susana Tonda Mitri Directora Nacional
Fecha	06/12/2019	10/12/2019	06/12/2019
Firma			

Control de Versiones

	Nombre	Fecha	Dpto.
Elaboró	Hector Burgos Cañete	06 DIC. 2019	Encargado Sistema de Gestión de Seguridad de la Información
Revisó	Cristian Castillo Silva	06 DIC. 2019	Jefe Departamento Planificación y Control de Gestión

Registro de Modificaciones (*)				
Revisión		Nombre /Dpto. Emisor	Descripción de la modificación / (Página o sección afectada)	Aprobó
Nº	Fecha			
00	13 OCT. 2017	DEPLAE	Emisión	DIRECCIÓN NACIONAL
01	06 DIC. 2019	DEPLAE	<ul style="list-style-type: none"> Se actualiza política (Sección 2) Se eliminan documentos relacionados al no pertenecer a estructura de políticas (Sección 2.1) Renombramiento de Unidad de Informática por Subdepartamento de Informática (Todo el Documento) Inclusión del uso de Firewall con control de navegación para el restringir acceso a páginas web restringidas. 	DIRECCIÓN NACIONAL

(*) La presente versión sustituye completamente a todas las precedentes, de manera que el último des listado será el único documento válido de todos los registrados.

TABLA DE CONTENIDOS

1. INTRODUCCIÓN	4
2. POLÍTICA	4
3. ALCANCE	7
4. OBJETIVOS	7
5. ROLES Y RESPONSABILIDADES	7
DIRECTOR(A) NACIONAL DE SENAME	7
SUBDEPARTAMENTO DE INFORMÁTICA.....	7
ADMINISTRADORES DE SISTEMAS	8
ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN	8
PERSONAL DEL PROCESO DE DESARROLLO DE LA OFERTA DEL SENAME.....	8
6. REVISIÓN, VALIDACIÓN Y DIFUSIÓN	9
7. CUMPLIMIENTO	9
8. SANCIONES.....	9
9. TÉRMINOS Y DEFINICIONES.....	9

1. INTRODUCCIÓN

La presente política se establece en el marco del Sistema de Gestión de Seguridad de la Información, con la finalidad de asegurar el correcto uso del servicio de internet y la plataforma de correo electrónico, garantizando la protección de los activos de información de SENAME, accesibles por parte de todos los funcionarios y personal externo del servicio y evitando accesos o descargas de sitios con contenido malicioso que podrían afectar la integridad de los activos de información.

2. POLÍTICA

El Servicio Nacional de Menores, implantará las medidas requeridas para el resguardo de la información manejada por sus funcionarios en el uso de internet y correo institucional como herramienta para el desempeño de las funciones, y es por ello que proporciona el acceso, protección y medios para su uso. Toda información transmitida por estos medios será tratada como información relacionada con SENAME y debe estar alineada a las normas enumeradas más abajo.

El uso personal ocasional o eventual del servicio de internet es permitido, en tanto no interfiera con la productividad del personal y no cause conflictos con la actividad de la Organización.

El personal que requiera el acceso a sitios restringidos, como parte de sus actividades laborales, deberá previamente justificar la necesidad y obtener la autorización de su respectiva jefatura. En caso que el acceso a un sitio en particular esté deshabilitado deberá solicitarlo la jefatura correspondiente.

Para controlar el acceso del personal a sitios restringidos en internet y la descarga de música, videos u otros medios se utilizará un Firewall con control de navegación.

Restricciones sobre el uso de Internet

A continuación, se listan los usos estrictamente prohibidos de Internet:

- Acceso a sitios Web relacionados con actividades de juego, apuestas, o actividades ilegales en general.
- Acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía.
- Acceso a todos los tipos de sitios de entretenimiento: música, juegos, videos, o cualesquiera otros sitios de entretenimientos on-line.
- Acceso a sitios Web de carácter discriminatorio, racista, o material potencialmente ofensivo incluyendo, bromas de mal gusto, prejuicios, menosprecio, o acoso explícito.
- Acceso a sitios de "hacking" o sitios reconocidos como inseguros, los cuales puedan poner en riesgo la integridad y confidencialidad de la información de SENAME.
- Descarga desde Internet de cualquier material (incluyendo software) protegido bajo leyes de derecho de propiedad, o archivos electrónicos para usos no relacionados con la actividad del servicio.
- Participación en cualquier actividad ilegal o criminal.
- Obtención de acceso no autorizado sobre otras computadoras pertenecientes a cualquier otra organización o entidad.

- Instalación y uso de programas de tipo “peer-to-peer” para el intercambio de archivos en Internet (Ej. Kazaa, Morpheus, Limewire, emule, etc.)
- Instalación y uso de programas de “Instant Messenger” (Ej. Hangouts, Yahoo, AOL, etc.)

Restricciones complementarias sobre el uso de Internet:

- No deje su navegador abierto cuando no esté utilizando Internet, cierre la sesión. De esta manera evitará consumo de ancho de banda innecesario.
- Se deberá cumplir con las leyes y regulaciones sobre transmisión de datos y derechos de autor.
- No duplicar software licenciado o con derechos de autor.
- La descarga o instalación de software solo será permitida si la misma está relacionada con el desarrollo de las funciones laborales y siempre que se cumplan las siguientes condiciones:
 - Deber ser autorizado previamente por su jefatura;
 - La autenticidad del software está debidamente comprobada;
 - Han sido investigadas y determinadas las condiciones para su uso (incluyendo tarifas de shareware), y estas condiciones han sido cumplidas;
 - Que el software se instale de acuerdo a las políticas de seguridad correspondientes;
 - El software fue examinado por una versión actualizada del antivirus estándar de la firma.
 - La instalación debe ser realizada por personal del Subdepartamento de Informática.
 - Cumplir rigurosamente las normas de conducta anteriormente mencionadas.

Uso de Correo Electrónico

La plataforma de correo es un activo de SENAME, suministrado a sus funcionarios para contribuir con su actividad laboral. La protección sobre los mensajes de acceso no autorizado se realizará con base al “Procedimiento de gestión de contraseñas” (SGSI.PR.17) y la “Política de Control de Acceso y Perímetro de Seguridad Física” (SGSI.PO.09).

Toda información transmitida por este medio será tratada como información relacionada con SENAME y debe estar alineada con las normas regulatorias vigentes.

Todo funcionario, independiente de su calidad jurídica o vinculado externamente a el Servicio Nacional de Menores, debe asegurar el correcto uso de la plataforma de correo velando por los siguientes aspectos:

Todo funcionario o externo debe tener presente:

- a) Usar su cuenta con fines laborales de acuerdo con su función.
- b) Usar un lenguaje apropiado en sus mensajes.
- c) No enviar ni contestar cadenas de correo o cualquier otro esquema de “pirámide” de mensajes.
- d) No usar su cuenta para fines comerciales.
- e) Los usuarios no deben acceder ni leer correo ajeno ni generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.

- f) Se prohíben las violaciones de los derechos de cualquier persona o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual. Entre otras actividades, se incluye la distribución o instalación de software sin la licencia legal proporcionada por SENAME.
- g) Se prohíbe el uso del correo electrónico con el fin de realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad hostil, sin importar el idioma, la periodicidad o tamaño del mensaje.
- h) Es obligación de los usuarios reportar al encargado de Seguridad en la Información, cualquier tipo de irregularidad o abuso de estos servicios, para evitar que esto le vuelva a suceder o que les ocurra a otros funcionarios.
- i) SENAME se reserva el derecho de monitorear las cuentas que presenten un comportamiento sospechoso para su seguridad, lo que no incluye acceso al contenido de los correos.

Consideraciones complementarias

- a) El correo electrónico es vulnerable a modificaciones y accesos no autorizados;
- b) Existen peligros asociados a la apertura de archivos adjuntos y/o a la ejecución de programas que se reciban vía correo electrónico;
- c) Es **prohibido** divulgar contraseñas de acceso al correo electrónico y la misma es de entera responsabilidad del usuario;
- d) No es conveniente almacenar contraseñas de acceso al correo electrónico en el mismo computador desde el cual se accede al correo electrónico;
- e) No es conveniente acceder al correo electrónico desde lugares de uso público (wifi pública, work café, etc.)

Para el cumplimiento de lo anteriormente expuesto, el Subdepartamento de Informática deberá:

- a) Instalar un antivirus que proteja el equipo frente a la posibilidad de obtener vía correo electrónico software malicioso;
- b) Proveer mecanismos, que, mediante el uso de técnicas de cifrado, permitan proteger la confidencialidad e integridad de los documentos electrónicos;
- c) Evitar el uso de cuentas de correo grupales;
- d) Verificar que todos los equipos informáticos y medios digitales que sean usados en el almacenamiento y/o procesamiento de documentos electrónicos, de ser posible, sean formateados previo a ser dados de baja.

Artículo 22.- En todos los organismos sujetos a la presente norma, deberán explicitarse y difundirse los siguientes antecedentes e información:

- a) Los contactos de apoyo ante dificultades técnicas u operacionales inesperadas de sistemas informáticos;
- b) Las exigencias relativas al cumplimiento con las licencias de software y la prohibición del uso de software no autorizado;
- c) 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.

3. ALCANCE

El alcance de la presente política será aplicable a los activos de información, activos físicos, activos de servicio de TI y activos humanos asociados al proceso de Desarrollo de la Oferta de líneas de acción establecidas en la ley N°20.032, realizados en la Dirección Nacional del Servicio Nacional de Menores, ubicada en Huérfanos 587, Santiago.

Se aplica a los funcionarios (planta, contrato, honorarios) de la Dirección Nacional del Servicio, proveedores y trabajadores externos, que pertenezcan al proceso de "Desarrollo de la Oferta", y los sistemas controlados serán los siguientes:

- Active Directory
- SENAINFO

4. OBJETIVOS

Apoyar las funciones de comunicación a los usuarios de SENAME.

Proporcionar los recursos para el acceso al servicio de Internet y/o correo institucional, sensibilizar y controlar su adecuado uso y acordar requisitos de seguridad de la información para mitigar riesgos asociados a su uso inadecuado.

Especificar los actos restringidos para los usuarios del servicio de Internet provisto por SENAME.

Cumplir con las disposiciones vigentes normadas en nuestro país, referentes a la protección de la información para el uso de internet.

5. ROLES Y RESPONSABILIDADES

DIRECTOR(A) NACIONAL DE SENAME

En su calidad de tal, tiene la responsabilidad de revisar y aprobar esta Política dentro de su área de competencia, debiendo procurar además que se asignen suficientes recursos humanos, materiales y financieros para implementarla. La alta dirección debe establecer claramente el enfoque de la Política en línea con los objetivos institucionales y demostrar su apoyo y su compromiso con la seguridad de la información, promoviendo la mejora continua a través de la emisión y actualización de esta Política de Uso de Internet y Correo Electrónico en la Institución y así asegurar que el SGSI logre sus resultados esperados.

SUBDEPARTAMENTO DE INFORMÁTICA

Mantener las condiciones de seguridad de acceso al servicio de internet y correo electrónico institucional.

Gestionar los accesos a los activos de información, privilegios de accesos y la gestión de contraseñas seguras.

Junto con lo anterior serán responsables de crear, administrar y eliminar las cuentas de usuarios y sus respectivas credenciales, en los momentos que corresponda, del sistema del cual es responsable.

Monitorear periódicamente los accesos a los activos de información.

ADMINISTRADORES DE SISTEMAS

Mantener las condiciones de seguridad de acceso a los activos de información que estén bajo su responsabilidad, resguardando que los proveedores sólo tengan ingreso a la información que requieran.

Gestionar los accesos a los activos de información, privilegios de accesos y la gestión de contraseñas seguras.

Junto con lo anterior serán responsables de crear, administrar y eliminar las cuentas de usuarios y sus respectivas credenciales, en los momentos que corresponda, del sistema del cual es responsable.

Monitorear periódicamente los accesos a los activos de información.

Visar en conjunto con el encargado de Seguridad de la Información y la jefatura del Subdepartamento de Informática, la Declaración de Aceptación de la Política General de Seguridad de la Información del Servicio Nacional de Menores.

Informar con anticipación a quien corresponda el vencimiento de plazos de acceso establecidos, con el fin de gestionar las solicitudes de prórrogas en caso de que fuere necesario, al igual que el término anticipado de contrato.

ENCARGADO DE SEGURIDAD DE LA INFORMACIÓN

Tendrá la responsabilidad de coordinar las actividades relacionadas a la gestión de la Política de Seguridad de la Información dentro del SENAME, a través de la ejecución de las siguientes funciones:

1. Coordinar las actividades del Comité de Seguridad de la Información.
2. Coordinar la debida respuesta y priorización al tratamiento de incidentes y riesgos vinculados a los activos de información de los procesos institucionales y sus objetivos de negocio.
3. Monitorear el avance general de la implementación de las estrategias de control y tratamiento de riesgos asociados a seguridad de la información y ciberseguridad.
4. Mantener coordinación con otros departamentos de la Institución para apoyar los objetivos de la seguridad de la información.
5. Mantener la aplicabilidad de este documento acorde a las prácticas operacionales del SENAME, por lo que es responsable de generar las modificaciones necesarias para que éste siempre actualizado. Junto con lo anterior, es responsable de gestionar la publicación y dar a conocer nuevas versiones del documento.

PERSONAL DEL PROCESO DE DESARROLLO DE LA OFERTA DEL SENAME

Tendrán la responsabilidad de cumplir con lo formalizado en este documento y así garantizar que los activos de información que se encuentren a su cargo estén protegidos contra el mal uso, robo, falta de disponibilidad o destrucción. Deberán trabajar en conjunto con los Directivos en todos los aspectos de la seguridad de la información, para garantizar que se implementen controles y procedimientos en forma adecuada y completa. Además, tendrán la responsabilidad de notificar incidentes de seguridad y potenciales debilidades que pudieran identificarse.

6. REVISIÓN, VALIDACIÓN Y DIFUSIÓN

El Comité de Seguridad de la Información de la Institución revisará una vez al año la presente Política, a efectos de mantenerla actualizada. Asimismo, efectuará toda modificación que sea necesaria en función de posibles cambios que puedan afectar su definición, como, por ejemplo, cambios tecnológicos, variación de los costos de los controles, impacto de los incidentes de seguridad, cambios legislativos, entre otros.

La responsabilidad de la validación y difusión de la Política de Uso de Internet y Correo Electrónico al interior del SENAME es del (la) Director(a) Nacional del Servicio. El Subdepartamento de Informática de SENAME, apoyarán la difusión de las políticas y procedimientos utilizando las herramientas y plataformas que estime conveniente para tal efecto.

El Subdepartamento de Informática o la Unidad de Comunicaciones del SENAME, apoyarán en la difusión de las políticas y procedimientos utilizando las herramientas y plataformas que estime conveniente para tal efecto.

Los funcionarios, proveedores de servicios y personal externo, tendrán acceso a esta Política en su última versión vía Intranet y Pagina Web del servicio, en formato digital.

7. CUMPLIMIENTO

La presente Política entra en vigencia una vez oficializada por el (la) Director(a) Nacional del SENAME. Las Jefaturas de los distintos departamentos pertenecientes al Proceso de Desarrollo de la Oferta serán responsables de difundirlas a su personal a cargo.

Para el caso del personal que se contrate con posterioridad a la fecha de publicación, se le deberá comunicar acerca de la existencia de la política, para conocimiento y acceso a la misma.

8. SANCIONES

Cualquier conflicto con las leyes y normativas asociadas a seguridad de la información debe ser informado inmediatamente al encargado de seguridad del SGSI.

El incumplimiento de la Política de Gestión de Redes podrá tener como resultado la aplicación de diversas sanciones en el ámbito administrativo, civil y/o penal, conforme a la magnitud y característica del aspecto no cumplido o vulnerado.

9. TÉRMINOS Y DEFINICIONES

- **Correo electrónico:** Servicio que permite el intercambio de mensajes a través de sistemas de comunicación electrónicos.
- **Internet:** Conjunto descentralizado de redes de comunicación interconectadas que utilizan la familia de protocolos TCP/IP.