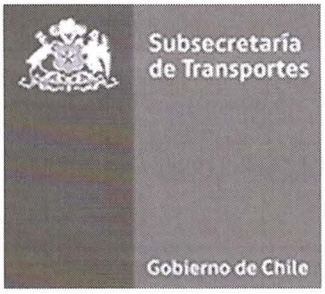
POLÍTICA DE SEGURIDAD EN LAS TELECOMUNICACIONES

Pol-SSI-13 v1.0



SUBSECRETARÍA DE TRANSPORTES

Diciembre 2017

	Nombre	Cargo	Firma	Fecha
Aprobado por	Matías Schöll	Presidente Comité Seguridad de la Información		27/12/2017
Revisado por Comité de Seguridad de la Información (Quorum mínimo 4 integrantes)	Carola Jorquera	Gabinete Subsecretario		27/12/2017
	Karen Caiceo	Encargada Unidad de Gestión de Procesos		27/12/17
	Mireille Caldichoury	Coordinación de Personas		27/12/17
	Juan Gregorio Flores	Departamento de Contabilidad, Presupuesto y Tesorería		
	Patricio Santidrian	División Legal		27/12/17
	Patricio Echenique	Encargado Unidad de Planificación y Control de Gestión		27/12/2017
	Jaime Gonzalez	Encargado Unidad TIC		27/12/2017
Elaborado por	Roy Mac Kenney	Encargado de Seguridad de la Información		27/12/2017

TABLA DE CONTENIDO

Nota de equidad de género:

El uso de un lenguaje que no discrimine ni marque diferencias entre hombres y mujeres ha sido una preocupación en la elaboración de este documento. Sin embargo, y con el fin de evitar la sobrecarga gráfica que supondría utilizar en español o/a para marcar la existencia de ambos sexos, se ha optado por utilizar el masculino genérico, en el entendido de que todas las menciones en tal género representan siempre a todos/as, hombre y mujeres, abarcando claramente ambos sexos.

1. DECLARACIÓN INSTITUCIONAL

La Subsecretaría de Transportes se compromete a mantener políticas y otras normativas en el ámbito de la seguridad de la información, con el fin de asegurar que sus procesos brinden servicios a la comunidad y tengan la debida continuidad operacional que se requiere.

Este documento presenta los lineamientos de seguridad necesarios en la protección de la información que se comunica por redes de datos y la protección de su infraestructura de soporte.

2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos generales de la Política de Seguridad en las Telecomunicaciones, son:

- Cumplir con la Norma Chilena Oficial NCh-ISO 27001:2013.
- Cumplir con la Política General de Seguridad de la Información.
- Definir los métodos de acceso y control a redes y a servicios de red.
- Mantener la integridad y disponibilidad del procesamiento de información y de los servicios de red.
- Asegurar la protección de la información de las redes y protección de la infraestructura tecnológica
- Regular el uso del servicio de Correo Electrónico y de Transferencia de Información

3. CONTEXTO O ÁMBITO DE APLICACIÓN

La Política de Seguridad en las Telecomunicaciones se aplica a todo el personal de la Subsecretaría de Transportes y sus Programas dependientes sean de planta, contrata o a honorarios, y externos que presten servicios a ella, e involucra a las visitas y a todos sus instalaciones, recursos y activos de información.

En cuanto a las temáticas de protección abordadas, el ámbito de aplicación de esta política corresponde al (a los) Dominio(s) de Seguridad de la Información y Controles de Seguridad respectivos, detallados a continuación:

Dominios y Controles de Seguridad relacionados	
A.13	Dominio: Seguridad de las Comunicaciones
A.13.01.01	Controles de red
A.13.01.02	Seguridad de los servicios de red
A.13.01.03	Separación en las redes
A.13.02.01	Políticas y procedimientos de transferencia de información
A.13.02.02	Acuerdos sobre transferencia de información
A.13.02.03	Mensajería electrónica
A.13.02.04	Acuerdos de confidencialidad o no divulgación

En cuanto al ámbito institucional de aplicación de esta política, corresponde a los siguientes objetivos y productos estratégicos del formulario A1 relacionados con procesos críticos que corresponden al alcance declarado del Sistema de Seguridad de la Información de SUBSECRETARÍA DE TRANSPORTE:

Objetivo, Producto estratégico y Proceso crítico en ámbito de aplicación		
Objetivo Estratégico SUBSECRETARÍA DE TRANSPORTE	Producto Estratégico A1	Proceso crítico protegido
(1) Disminuir fallecidos por accidentes de tránsito. (2) Desarrollar planes y estudios que permiten definir políticas y normativas en los temas relevantes a transporte de carga.	(1) Regulación que rige el transporte	Políticas y normas que rigen el transporte.
(3) Mejorar las condiciones para la operación e integración del Transporte Público a través de infraestructura prioritaria, con foco inicial en la mejora de los tiempos de viaje. (4) Diseñar sistemas de transportes que respondan a las principales necesidades multimodales de las personas, priorizando los modos más eficientes y sustentables y mejorando la convivencia de usuarios de los distintos modos. (6) Velar por la accesibilidad, calidad, seguridad e impacto ambiental que entregan los servicios de transporte terrestre y otros modos.	(5) Subsidios e iniciativas de inversión para la operación y fortalecimiento de los Servicios de Transporte Público.	Transporte Público Regional.

4. ROLES Y RESPONSABILIDADES

- **El Comité de Seguridad de la Información (CSI)**, en concordancia con la resolución que aprueba este comité, se identifican las siguientes funciones relacionadas con esta temática:
  - Supervisar la implementación de la presente política.

- **El Encargado de Seguridad de la Información (ESI)**
  - Es responsable de la elaboración de la presente política, de su actualización y velar por el cumplimiento de sus disposiciones.
  - Además, aprobará o rechazará las solicitudes de permisos especiales de acceso a los servicios de red.

- **El Encargado de la Unidad de TIC**
  - Es responsable de autorizar, gestionar y controlar las implementaciones de la presente política.
  - Es responsable de la implementación de la configuración, monitoreo y controles correspondientes a las redes y los servicios de red de la Subsecretaría de Transportes.
  - Además, aprobará o rechazará las solicitudes de permisos especiales de acceso a los servicios de red, previa revisión con el Encargado de Seguridad de la Información (ESI)

- **El Encargado de Infraestructura Tecnológica**
  - Es responsable de mantener actualizados todos los instructivos o procedimientos que le competen de la presente política. De igual manera, debe realizar la implementación de los siguientes aspectos:

- Mantener activo todos los registros (LOGS) que las políticas, procedimientos e instructivos indican.
- Mantener respaldo e integridad de los registros activos.
- Resguardar que los registros no sobrepasen los límites de almacenamiento definidos.
- Antes de eliminar cualquier registro, este debe ser respaldado.

- **El Encargado de Servicios de la Unidad de TIC**
  - Responsable de revisar si las solicitudes de nuevos permisos se acogen a los procedimientos vigentes, en cuyo caso, ejecutará la solicitud, de lo contrario, lo escalará al Encargado de la Unidad de TIC.

5. MARCO NORMATIVO

El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior https://www.csirt.gob.cl/decretos.html.

- Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad:
  - Decreto Supremo N° 1299, de 2004, del Ministerio del Interior.
  - Decreto Supremo N° 5996, de 1999, del Ministerio de Interior.
  - Decreto Supremo N°1, de 2015, del Ministerio Secretaría General de la Presidencia.
  - Decreto Supremo N°83, de 2004, del Ministerio Secretaría General de la Presidencia.
  - Decreto Supremo N°93, de 2006, el Ministerio Secretaría General de la Presidencia.

- Leyes relacionadas
  - Ley N°20.285/2008 Ley sobre acceso a la información pública
  - Ley N°17.336/2004 Ley sobre propiedad intelectual
  - Ley N°19.927/2004 Ley modifica códigos penales en materia de delitos sobre pornografía infantil
  - Ley N°19.880/2003 Ley que establece bases de los procedimientos administrativos que rigen los actos de los órganos de la administración del Estado
  - Ley N°19.799/2002 Ley sobre documentos electrónicos, firma electrónica y servicios de certificación de dicha firma
  - Ley N°19.628/1999 Ley sobre protección de la vida privada
  - Ley N°19.223/1993 Ley sobre figuras penales relativas a la informática

6. MATERIAS QUE ABORDA

La presente política aborda lineamientos de Seguridad en las Telecomunicaciones, en tópicos de:

- Autorización para permitir acceder a redes y servicios de red
- Controles de seguridad a la red y a los servicios de red

- Segmentación de redes
- Seguridad en los perímetros de la red
- Regulaciones para el Correo Electrónico
- Acuerdos sobre transferencia de información
- Mensajería electrónica
- Acuerdos de confidencialidad o no divulgación

7. LINEAMIENTOS DE SEGURIDAD EN LA OPERACIÓN Y ADMINISTRACIÓN DE SISTEMAS

7.1 Autorización para permitir acceder a redes y servicios de red

- Todos los computadores de la Subsecretaría de Transportes se deben configurar para acceder a los servicios de red.
- Todos los funcionarios tienen sus cuentas de red debidamente configuradas para acceder a los distintos servicios de red, de acuerdo a su perfil (cargo), el que es informado por Coordinación de Personas al momento de ingreso de un nuevo funcionario.
- Las solicitudes de permisos especiales o adicionales para utilizar redes o servicios de red deben ser aprobados por la jefatura directa de cada funcionario a través de correo electrónico a la Mesa de Ayuda, la cual revisará si se acoge a los procedimientos o instructivos vigentes, de lo contrario, escalará la solicitud al Encargado de la Unidad de TIC, el que, junto al Encargado de Seguridad de la Información, determinaran si la solicitud no vulnera la Política de Seguridad de la Subsecretaría, sopesando los criterios de facilidad de operación y protección de la información.
- Todos los permisos de red y servicios de red deben ser concordantes con la Política de Control de Acceso Lógico.
- El Encargado de Seguridad de la Información debe custodiar las credenciales de acceso de todos los Activos de Información de la Subsecretaría.

7.2 Controles de seguridad a la red y a los servicios de red

- Las conexiones de red y servicios de red de la Subsecretaría de Transportes deben estar configuradas para registrar todas las actividades que se realizan, manteniendo estos registros respaldados y disponibles.
- Los datos que se registran de los usuarios que utilizan redes o servicios de red de la Institución deben ser los siguientes:
  - Dirección IP origen
  - Nombre del dispositivo origen
  - Puertos utilizados
  - Dirección IP destino
  - URL destino
  - Tráfico de red
- Para minimizar las fallas y dar respuesta oportuna a incidentes, se debe monitorear los servicios de red de la Subsecretaría, alertando a los responsables de manera automática.

- Para utilizar servicios de red, todos los usuarios deben iniciar sesión en Active Directory o deben estar autenticados en el Portal Captivo (http://172.25.1.24:8090).
- Para usuarios que requieren acceso remoto, se aceptarán conexiones VPN que cumplan los requisitos del Instructivo de Seguridad para Acceso a Través de Redes y Acceso Remoto.
- Todos los usuarios que utilicen servicios de red desde dispositivos móviles deben cumplir con la Política de uso de medios tecnológicos.
- En el caso de existir redes inalámbricas (WIFI), esta debe cumplir con al menos las siguientes configuraciones:
  a) Debe emitir al menos dos nombres de acceso, una para los usuarios de la Subsecretaria y otra para visitas
  b) Permisos restringidos para las visitas o proveedores externos que soliciten conectarse a la red institucional. Esta conexión debe ser temporal y no debe otorgarse por más de 8 horas.
- Los usuarios con computadores personales que deseen utilizar servicios de red en la Subsecretaria de Transportes, deben ajustarse a los requisitos de la Política de Uso de Medios Tecnológicos y trabajo remoto, y deben mantener la configuración hasta el retiro del equipo de las dependencias de las redes de la Institución.
- Queda prohibido que los usuarios accedan a redes o a servicios de redes no permitidos, sin la autorización correspondiente.
- El servicio de red de acceso a internet debe ser restringido con un sistema de filtro de contenidos.
- Los usuarios tienen prohibición de conectar algún dispositivo que permita compartir acceso a redes o a servicios de red, tales como Router, Switch, o equivalente. De ser necesario, se debe solicitar vía correo electrónico a la mesa de ayuda de la Unidad de TIC la instalación y configuración.
- Todo servicio de red que consuma ancho de banda excesivo (transferencia de videos, o archivos de gran tamaño) será restringido, salvo a usuarios que lo requieran para el cumplimiento de sus funciones, en cuyo caso, la jefatura del usuario debe solicitar por correo electrónico a la mesa de ayuda el acceso a un servicio en particular.

7.3 Segmentación de redes

- Las redes de comunicación de la Institución, emplean el protocolo de red IP versión 4, estas deben estar adecuadamente segmentadas, o particionadas, para permitir el establecimiento de puntos de convergencia de los tráficos, los cuales facilitan el control de los datos en tránsito. De esta forma es posible restringir ciertos tipos de tráficos, así como asegurar otros.
- Para ello, se deberá establecer como mínimo los perímetros siguientes:
  - DMZ: Esta zona de seguridad deberá estar protegida mediante un firewall y tendrá como función contener a todos aquellos servidores que exponen información a las redes públicas.
  - Internet: Esta zona de seguridad se delimita por la interconexión con los enlaces de comunicación que permiten el acceso a las redes públicas, como lo es Internet. Debe estar resguardada por un firewall, el cual puede compartir la función de DMZ. Este punto establece la frontera entre lo público y lo privado.

- Producción: Este perímetro está destinado a contener aquellos servidores de distintos ámbitos (repositorios, intranet, bases de datos, etc.) que soportan los servicios de procesamiento de información. Estos servidores y/o servicios no pueden estar expuestos a las redes públicas en forma directa, solo a nivel interno. La exposición deberá realizarse mediante otro servidor de ambiente DMZ, por ejemplo, mediante arquitecturas de modelo de 3 capas. Debe estar delimitado mediante firewall.
- Interno: Este perímetro lo componen todas las estaciones de trabajo de los usuarios y aquellos elementos que les prestan servicios complementarios, como impresión, control de acceso, redes inalámbricas, etc. Los usuarios deben estar segregados de acuerdo con el organigrama de la Institución. Esta segregación deberá estar también reflejada en la estructura jerárquica del Active Directory y deberá ser coherente. Los distintos segmentos no podrán comunicarse entre sí, y no podrán exponer servicios de ningún tipo, con excepción del que aloja a las impresoras. Debe contar con un firewall para efectos de delimitaciones y control.
- Desarrollo, pruebas y certificación: Corresponde al perímetro destinado al proceso de construcción de sistemas previo al paso a los entornos de producción o de DMZ. Debe estar delimitado por controles duros de red, como firewall o equivalente y sólo debe ser accesible para quienes tengan relación con los sistemas en alguna de las etapas de construcción. No puede ser expuesto a Internet, no puede alojar sistemas en fase de explotación o producción. Si en alguna situación se requiere exponer un sistema, se podrá realizar una excepción, la que deberá tener asociada una duración máxima limitada y documentada.

Estos perímetros podrán estar implementados en equipos compartidos, con excepción del que delimita el entorno público y la(s) DMZ(s), que debe ser controlado por un firewall independiente.

Esta segmentación debe estar asociadas cada una a una Vlan o dominio de broadcast diferente, incluidos las distintas segmentaciones de redes de usuarios.

7.4 Seguridad en los perímetros de la red.

La Subsecretaría de Transporte debe contar con equipos del tipo Firewall propios o de terceros que al menos tengan las siguientes funcionalidades:

- Establecer reglas de filtro y navegación para los usuarios internos (LAN)
- Permitir configurar publicaciones de servicios internos hacia internet (DMZ) en forma segura.
- Filtro de correo (Antispam), bloqueo de mensajes no deseados en tiempo real.
- Filtro de Navegación, restricción de accesos WEB de usuarios, de acuerdo al contenido de los sitios, protección contra sitios maliciosos.
- Filtro antivirus, revisión de tráfico WEB y email de protección perimetral contra spyware, virus y otros.
- Servicio de conectividad remota segura a través de VPN.
- Sistema de prevención de intrusos (IPS), que posibilite en tiempo real, identificar, detectar y/o bloquear ataques o actividades sospechosas sobre la red de la Subsecretaría, complementando los dispositivos de seguridad del firewall.

- Integración con Active Directory, para controlar y agrupar por tipo los diferentes niveles de acceso a Internet por parte de los usuarios.

Por otra parte, el Área de Infraestructura, deberá gestionar, a través de recursos propios o de terceros, las siguientes tareas en orden de mantener la Seguridad Perimetral en permanente operación:

- Resumen de incidentes y requerimientos en un mes (Informes mensuales).
- Principales eventos de seguridad detectados, criticidad, origen de los mismos y recomendaciones.
- Análisis de upgrades y parches para la plataforma administrada.
- Monitoreo y Reportes de Uptime general de componentes.
- Registro de Conexiones denegadas.
- Registro y Reportes de Bloqueo de sitios Web no autorizados.
- Registro y Reportes de sitios Web más visitados.
- Registro y Reportes de Ranking de los usuarios con mayor actividad en el acceso bajo supervisión.
- Registro y Reportes de Eventos ocurridos en el firewall y en el acceso bajo supervisión durante el período.

7.5 Acuerdos de Servicios de Red

- Entre la documentación que el Área de Infraestructura debe generar y mantener permanentemente actualizado en la respectiva carpeta de red de la Unidad de TIC es la lista de los Servicios de Red, incluyendo en esta, los mecanismos de seguridad empleados para otorgar el servicio en forma segura, los niveles de servicio y reportes que sean solicitados a través de contratos o bien solicitados por la Subsecretaria, tales como reportes comprometidos en los CDC (Convenios de Desempeño Colectivo) o PMG (Programa de Mejoramiento de Gestión).
- Además, cada servicio debe contar para efectos de su documentación, un Diagrama que identifique todos los componentes de Hardware, Software y Networking, sus respectivos nombres de red y su numeración IP.

7.6 Regulaciones para el Correo Electrónico

- Sólo el personal interno, o externo que sea formalmente autorizado puede hacer uso del sistema de correo electrónico.
- Se permite el uso de casillas de correos personales, previa solicitud a la mesa de ayuda de la Unidad de TIC
- Se puede dar uso personal a este servicio, siempre que no interfiera con las actividades formales de la Institución, que no se sostengan actividades comerciales personales y que no comprometa a la institución.
- La creación de casillas de correo se regirá por un instructivo específico.
- Toda casilla debe estar asociada o a una persona, sistema o servidor específico.

- Se permiten listas de distribución solo para la recepción de correos.
- Sólo se permite el uso del software cliente de correo electrónico establecido como estándar para el servicio de correo electrónico institucional.
- Habrá una forma estándar y limitado de espacio de almacenamiento para cada usuario de correo. Las excepciones serán autorizadas por el Encargado de la Unidad de TIC.
- Se debe utilizar el estándar institucional de pie de firma para los correos.
- Se debe habilitar respuesta automatizada sólo para períodos de ausencia autorizadas por el servicio.
- En caso que la comunicación lo amerite, por su contenido o por el cargo de los participantes, el correo electrónico debiese generarse firmado digitalmente y/o cifrado.
- Es responsabilidad del usuario revisar y eliminar mensajes de correo detectados como SPAM por la plataforma central de seguridad del correo electrónico y avisar a la mesa de ayuda de la Unidad de TIC.

7.7 Regulación de Seguridad para Mensajería y Transferencia de Información

- Deben existir controles formales para la transferencia de información en las redes de datos de la institución con el fin de evitar actos no autorizados como intercepción, copia, modificación, ruteo incorrecto y destrucción.
- Deben existir mecanismos de protección de dichas comunicaciones:
  - Sistemas antivirus y antimalware para correo electrónico.
  - Uso de cifrado para transacciones que lo ameriten.
- Se debe informar al personal para evitar responsabilidades del usuario que comprometan al Servicio, por difamación, acoso, imitación, spam, u otros actos reñidos con la moral, buenas costumbres o legalidad.
- Se debe integrar a los lineamientos de uso aceptable de las instalaciones y tecnologías de comunicación.

7.8 Acuerdos de Confidencialidad o no Divulgación

Se deben considerar los siguientes elementos para identificar los requisitos de confidencialidad o para los acuerdos de no divulgación en el intercambio de información:

- Individualización de las partes.
- Identificar y definir claramente la información que se protegerá.
- Establecer la duración de los acuerdos, incluidos los casos donde es posible que sea necesario mantener la confidencialidad de manera extendida.
- Acciones necesarias al terminar un acuerdo.
- Responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada.
- Propiedad de la información, secretos legales o administrativos y propiedad intelectual y cómo esto se relaciona con la protección de información confidencial.
- El uso permitido de la información confidencial y los derechos del firmante para utilizar dicha información

- Derechos para auditar y monitorear actividades que involucran información confidencial.
- Notificar e informar la divulgación no autorizada o la fuga de información confidencial.
- Condiciones para la información que se va a regresar o destruir al término del acuerdo.
- Medidas esperadas que se tomarán en caso de un incumplimiento del acuerdo.

8. PERIODO DE REVISIÓN

La Subsecretaría debe establecer una revisión independiente la cual asegure la idoneidad, adecuación y efectividad continua del enfoque para administrar la seguridad de la información. Dicha revisión la deberían realizar personas independientes del área bajo revisión o una organización externa que se especialice. Los resultados de la revisión independiente se deberían registrar e informar a la dirección que inició esta revisión y mantener estos registros.

Esta política debe ser revisadas cada 3 años como máximo, para mantener al día su vigencia.

9. EVALUACIÓN DE CUMPLIMIENTO

La revisión del cumplimiento de esta Política se efectuará anualmente por el Encargado de Seguridad de la Información. Adicionalmente, según lo requiera un caso particular, podría requerirse una revisión de cumplimiento por Auditoría ministerial, auditoría interna, jefaturas de cada Unidad o el Comité de Seguridad de la Información, atendiendo necesidades de cambios, para garantizar su idoneidad, adecuación y efectividad.

10. EXCEPCIONES AL CUMPLIMIENTO DE ESTA POLÍTICA

Frente a casos especiales, el Comité de Seguridad de la Información podrá establecer condiciones puntuales de excepción en el cumplimiento de las directrices de esta Política de Seguridad de la Información, siempre que no infrinja la legislación vigente ni afecte directrices de otras Políticas. Toda excepción debe ser documentada y se le debe efectuar seguimiento, generando un proceso de revisión de la misma, para determinar si amerita una nueva directriz particular o un cambio en otra ya existente.

11. MECANISMO DE DIFUSIÓN

La Subsecretaría de Transportes difundirá ésta y todas las políticas de seguridad mediante un conjunto de actividades planificadas, que tienen como objetivo dar a conocer y sensibilizar a los funcionarios internos y externos, que realicen trabajos para la institución, a través de la publicación en secciones destinadas a la Seguridad de la Información en sitios web internos de la institución, difusión mediante correo electrónico, y como parte de los procesos de inducción del personal nuevo y de los contratos acordados con terceros. Frente a un cambio se notificará por el correo institucional al personal relacionado.

12. GLOSARIO DE TÉRMINOS, DEFINICIONES Y SIGLAS

El completo glosario de términos y siglas utilizados en los documentos del Sistema de Gestión de Seguridad de la Información de la Subsecretaría de Transporte, se encuentran integrados en el Estándar de Seguridad "Glosario Términos de SSI-MTT", ubicado en la sección "Políticas de Seguridad de la Información" de la intranet institucional.

Las siguientes son definiciones necesarias para la comprensión de la presente política:

- **Active Directory:** Servicio de Directorios de Microsoft. Sirve para la administración de usuarios, grupos y otros elementos de red. También administra las credenciales de los usuarios, los permisos de usuario y grupos y sus atributos.

- **Ancho de banda:** Corresponde a los datos utilizados o consumidos en una red que se expresan en bit/s (bits por segundo) o comúnmente kbps (kilobits por segundos). Esta medida es utilizada para calcular la velocidad de transferencia de información a través de una red.

- **Antispam:** El antispam es un método para prevenir el correo basura o correo no deseado.

- **Conexión VPN:** Red privada virtual (en inglés Virtual Private Network) permite realizar una conexión segura extendiendo una red hacia otra a través de Internet.

- **Cuenta de Red:** Son las credenciales con las que los usuarios se identifican en la red.

- **Dirección IP:** Numero único e irrepetible que identifica un equipo conectado a una red (computador, impresora, dispositivo móvil o equivalentes).

- **Filtro de Contenidos:** Se refiere a un programa diseñado para controlar qué contenido se permite mostrar, especialmente para restringir el acceso a ciertos materiales de la Web.

- **IP:** IP significa "Internet Protocol" y es un número que identifica un dispositivo en una red (un computador, una impresora, un router, etc...). Estos dispositivos al formar parte de una red serán identificados mediante un número IP único en esa red.

- **Networking:** Se le llama Networking a los elementos de red, sus conexiones e interconexiones, sus identificaciones, su topología y protocolos de comunicación.

- **Nombre del dispositivo origen:** Dispositivo que origina una conexión de red hacia otra.

- **Portal Captivo:** Es un programa de una red informática que controla el trafico HTTP y fuerza a los usuarios a que inicien sesión para poder navegar en internet.

- **Puerto utilizado:** Corresponde a una interfaz para comunicarse con un programa a través de una red. Un puerto suele estar numerado para de esta forma poder identificar la aplicación que lo usa.

- **Router:** Corresponde a un dispositivo que proporciona conectividad enviando datos de una red a otra.

- **Spyware:** El spyware o programa espía es un malware que recopila información de un computador y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario del computador.

- **Switch:** Es un dispositivo que tiene como función interconectar dos o más redes.
- **Tráfico de red:** Transmisión y recepción de datos transmitidos en una red.
- **URL:** Dirección web que localiza un servicio de red (en inglés Uniform Resource Locator).

13. HISTORIAL Y CONTROL DE VERSIONES

N° de Versión	Fecha de Aprobación	Resumen de las Modificaciones	Páginas Modificadas	Autor
0	07/2016	Elaboración inicial. Lineamientos a controles NCh-ISO 27001:2013	0	07/07/2016
1	10/2017	Actualización de formato y contenidos según requerimientos PG-SSi 2017.	Todas	RM