
digilogics

# SEGURIDAD DE LAS COMUNICACIONES POL-09

## 1. Objetivo

Establecer las directrices para garantizar la protección de la información en las redes e infraestructura de apoyo para el procesamiento de información de la organización.

## 2. Alcance

Es de aplicación para toda las redes e infraestructura de la organización.

## 3. Términos y Definiciones

**ATSI**: Administrador técnico de seguridad de la información

## 4. Política

### A.8.20 Controles de red

- El administrador técnico de seguridad de la información debe asegurarse de que se cumpla con los siguientes puntos dentro de la organización:

  - Todos los dispositivos de comunicación deben tener configuradas contraseñas para acceder a las funciones de operación y administración.
  - Se deben restringir las actividades y funciones que puedan realizar los operadores y los administradores sobre las plataformas de cómputo y comunicaciones de acuerdo a su perfil.
  - El acceso a las funciones de operación y administración de los dispositivos de comunicación se debe realizar exclusivamente a través de una consola específica o de terminales restringidas.
  - Los servicios de File Transfer Protocol (FTP) en los equipos de comunicación se deben habilitar de acuerdo a los perfiles de usuario documentando los mismos. De igual manera, se deben deshabilitar todos los servicios o protocolos que no sean requeridos.

### A.8.21 Seguridad en los servicios de red

- Se debe implementar mecanismos que limiten el acceso a los recursos existentes en la red de datos (Firewall) y voz (Conmutador).
- Se debe monitorear y proteger los servicios de red en contra de accesos no autorizados para lo cual debe cumplir con los siguientes puntos:

  - Identificar y documentar las redes y servicios de red utilizados por usuarios.
  - Definir procedimientos de autorización para determinar qué usuarios pueden acceder las redes y los servicios de red.
  - Los privilegios de acceso otorgados a los usuarios sólo deben incluir aquellos que están explícitamente autorizados a utilizar.
  - Se debe identificar, implementar y mantener los mecanismos y procedimientos de monitoreo de servicios de red que permitan identificar como mínimo a nivel usuario o grupo de usuarios:

    a) Accesos a los servicios de red.

b) Intentos de acceso no autorizados.
c) Cambio de privilegios especiales no autorizados.

- El administrador técnico de seguridad de la información debe controlar los accesos permitidos a los sistemas de administración y monitoreo, y vigilar estrechamente las actividades relacionadas, almacenándolas en bitácoras.

### A.8.22 Segregación de redes

- El ATSI debe limitar a usuarios el acceso a los servicios de Internet de acuerdo a los propósitos exclusivamente autorizados por la organización.
- El ATSI debe revisar y monitorear el uso de los servicios, equipos, información enviada o recibida, intentos de ataques y vulnerabilidades de los sistemas utilizados, a fin de reducir los riesgos derivados del uso de Internet.
- La organización deberá contar con 3 segmentos de red: el primero designado a las operaciones inalámbricas (Wi-Fi), el segundo segmento estará dedicado exclusivamente a los servicios administrativos de la empresa y el tercer segmento a los servicios operativos.
- El ATSI debe crear y mantener los procesos y mecanismos que permitan la autorización y control de usuarios con derecho de uso y acceso a Internet.
- El acceso a los servicios de Internet debe realizarse exclusivamente a través de los equipos y medios de comunicación expresamente autorizados.
- Todos los usuarios que utilicen el servicio de Internet pertenecientes a la organización, deben hacerlo de manera responsable.
- Queda prohibido conectarse a redes inalámbricas no administradas por la organización dentro de las instalaciones.
- La separación de redes está establecida en el documento **mapa de red.**

### A.8.23 Filtrado web

- La dirección general se reserva el derecho de bloquear el acceso a ciertos sitios de web que no estén relacionadas con funciones propias de la organización.

- Para el acceso a la aplicación de videos “YouTube” está restringido a sólo material relacionado con el perfil del usuario.
- Otras aplicaciones de streaming de video se encuentran restringidos.
- El acceso a las aplicaciones de streaming musicales no están restringidos, pero sólo podrán ser escuchados por medio de auriculares.
- El acceso a redes sociales como Facebook, Instagram, Twitter, Snapchat, TikTok, Tinder, Bumble, y similares, es acceso restringido.
- Las descargas de servicios en la nube que permitan el intercambio de archivos libre, se encuentran prohibidos.
- Queda estrictamente prohibido el ingreso a páginas pornográficas.
- No es permitido la descarga de archivos de páginas no seguras.
- Para el uso de aplicaciones específicas o acceso temporal a páginas de internet, se requiere la autorización del ATSI.
- Queda explícitamente prohibido el uso de internet para las siguientes actividades:

  - Descargar software ilegal o para uso personal.
  - Descargar música y/o videos de manera ilegal.
  - Realizar “streaming” desde las instalaciones de la organización.
  - Utilizar software P2P.
  - Subir información confidencial y/o reservada en repositorios no certificados con protocolos y controles de seguridad.