

# Información a usuarios sobre la seguridad de la red

---

**Código:** POL-SEG-03

**Versión:** 1.0

**Año:** 2026

**Empresa:** netpaís

---

## 1. Objetivo

Establecer los lineamientos para informar a los usuarios sobre los riesgos asociados a la seguridad del servicio de acceso a Internet, así como las medidas que deben adoptar para proteger sus dispositivos, información y conexión.

---

## 2. Alcance

Aplica a todos los usuarios del servicio de acceso a Internet, tanto residenciales como empresariales, incluyendo el acceso mediante redes **Wifi** en dispositivos móviles, computadores y otros equipos conectados.

---


## 3. Riesgos Asociados a la Seguridad de la Red

El uso del servicio de Internet puede estar expuesto a diversos riesgos, especialmente cuando se accede a través de redes inalámbricas (Wifi), entre ellos:

- Malware (virus, troyanos, ransomware)
- Phishing (suplantación de identidad)
- Intercepción de datos en conexiones inalámbricas inseguras
- Robo de información personal o financiera
- Ataques informáticos (DDoS, intrusiones, etc.)

Estos riesgos pueden comprometer la confidencialidad, integridad y disponibilidad de la información del usuario.

---



## 4. Responsabilidad del Usuario

El usuario debe adoptar buenas prácticas de seguridad, especialmente en conexiones WiFi, tales como:

- Cambiar periódicamente la contraseña del WiFi
- Utilizar claves seguras
- No compartir el acceso a la red con personas no autorizadas
- Mantener actualizados los dispositivos móviles y computadores
- Instalar antivirus y mantenerlo actualizado
- No acceder a enlaces o sitios web sospechosos

---

## 5. Medidas Implementadas por la Empresa

Se implementan mecanismos de seguridad orientados a proteger la red y el servicio, tales como:

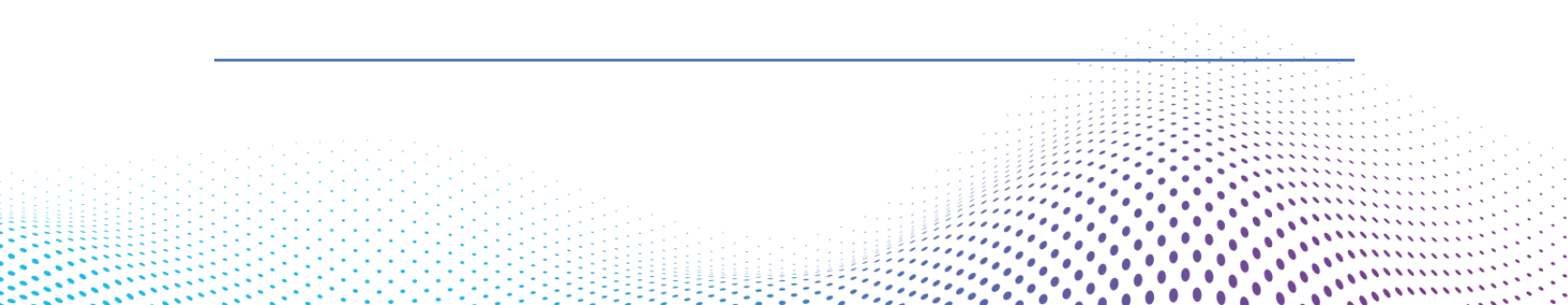
- Monitoreo continuo del tráfico de red
- Gestión y control de acceso a la red
- Implementación de políticas de seguridad (firewall, filtrado y control de tráfico)
- Detección y mitigación de amenazas e incidentes
- Segmentación de red para mayor seguridad
- Actualización periódica de configuraciones y firmware

Estas medidas permiten fortalecer la seguridad del servicio; sin embargo, la protección integral también depende de las buenas prácticas adoptadas por los usuarios, especialmente en el uso de redes WiFi.

---

## 6. Canales de Información al Usuario

La información relacionada con seguridad se pone a disposición a través de:

- Canales de atención al cliente
  - Soporte técnico
  - Comunicaciones informativas
  - Medios digitales oficiales
- 
- 

## 7. Marco Normativo

La presente política se desarrolla conforme a la regulación vigente en Colombia en materia de protección de usuarios de servicios de comunicaciones, expedida por la **Comisión de Regulación de Comunicaciones (CRC)**.

---

## 8. Revisión y Actualización

Este documento será revisado periódicamente o cuando se presenten cambios regulatorios o tecnológicos que impacten la seguridad del servicio.

