

## Políticas de Seguridad en la Red y Protección al Usuario

Gane Móvil establece esta política para mitigar riesgos en la red que soporta, enfocándose en la protección de datos de usuarios y transacciones en el contexto de servicios móviles en Colombia. Se prioriza la confidencialidad, integridad y disponibilidad, responsabilizando al usuario en el manejo seguro de su equipo terminal.

### Riesgos Principales Identificados:

Los principales riesgos incluyen fuga de información por uso de redes públicas, software malintencionado, pérdida o robo de dispositivos, y fraudes en transacciones vía redes no seguras. Gane Móvil no realiza respaldos de datos de clientes, por lo que el usuario debe gestionarlos independientemente, evitando infracciones legales como piratería o spam. Eventos de fuerza mayor pueden causar indisponibilidad, sin responsabilidad del operador.

### Recomendaciones Generales de Seguridad:

- Habilite contraseñas en equipos móviles y bloqueo automático tras inactividad.
- Instale solo Apps de fuentes confiables, mantenga actualizado su software, y use antivirus compatible.
- Configure Bluetooth oculto con contraseña, realice respaldos periódicos y cifre datos sensibles.
- Reporte robo o pérdida a autoridades y proveedor; evite enlaces o archivos sospechosos en email/SMS.
- No realice transacciones en redes públicas sin seguridad mínima.

### Seguridad Específica para el Portal Web:

El Sitio Web de Gane Movil no es transaccional, protegete contra phishing, donde estafadores suplantan identidad para robar credenciales vía email o SMS. Para malware, instale antivirus confiable, mantenga software actualizado, use contraseñas seguras y firewall activo, y escanee dispositivos externos.

### Monitoreo y Cumplimiento:

Gane Móvil monitorea la red con firewalls y logs, realiza actualizaciones periódicas y pruebas OWASP para vulnerabilidades web.

## Política de Seguridad en la Red para la App de Gane Móvil:

Gane Móvil adapta esta política de seguridad en la red para su aplicación móvil, protegiendo datos de usuarios y transacciones en servicios móviles, cumpliendo normativas colombianas como Ley 1581 de 2012 y Decreto 1377 de 2013. La App opera sobre redes seguras, enfatizando responsabilidad del usuario en el manejo de su dispositivo terminal para mitigar riesgos inherentes al medio móvil.

## Riesgos Principales en la App:

Riesgos clave incluyen fugas por redes públicas, malware en dispositivos, robo o pérdida de equipos, y fraudes en transacciones App vía redes no seguras. Indisponibilidad por fuerza mayor exonera al operador de responsabilidad.

## Recomendaciones Generales de Seguridad:

- Active contraseñas y bloqueo automático en dispositivos para la App.
- Instale Apps solo de fuentes confiables, actualice su App regularmente, use antivirus.
- Configure Bluetooth oculto con PIN, respalde datos periódicamente y cifre información sensible en el dispositivo.
- Reporte pérdidas a autoridades y Gane Móvil; evite enlaces sospechosos en SMS/emails relacionados con la App.
- Realice transacciones en la app solo en redes seguras privadas.

## Seguridad Específica para la App:

La App Gane previene phishing, donde estafas buscan credenciales vía SMS/emails falsos. Use contraseñas de  $\geq 8$  caracteres (mayúsculas, minúsculas, números, símbolos), cámbielas cada 3 meses, evitando nombres, fechas o IDs.

## Monitoreo y Cumplimiento en la App:

Gane Móvil monitorea redes de la app con firewalls, logs y actualizaciones OWASP para vulnerabilidades móviles. Revisión anual por gerencia alinea con riesgos MVNO; notifica Superintendencia de Industria y Comercio en brechas de datos.