CONECTA INTERNET

Seguridad de la red

Código P-01 · Edición 1.0 · 06/10/2026

1. Objeto y alcance

Establecer lineamientos para proteger la confidencialidad, integridad y disponibilidad de los servicios de acceso a internet por fibra óptica y radioenlace. Aplica al personal, contratistas y terceros con acceso a los activos de red que la empresa defina. El responsable técnico debe documentar y revisar los controles aplicables a la operación.

2. Riesgos que deben comunicarse al usuario

Entre los riesgos se encuentran el robo de contraseñas, la suplantación de páginas o personas, el software malicioso, el acceso no autorizado al Wi-Fi, las vulnerabilidades de equipos, la exposición de información y los ataques que afectan la disponibilidad. Ningún servicio de acceso elimina por sí mismo todos los riesgos de los dispositivos, las aplicaciones o los contenidos de terceros.

3. Acceso y administración de equipos

Se debe mantener un inventario de activos y responsables; usar cuentas individuales; restringir la administración a personal autorizado; asignar solo los permisos necesarios; deshabilitar accesos que ya no se requieren; y proteger los canales de administración. Las contraseñas no deben compartirse por canales públicos. El uso de autenticación multifactor se evaluará en los sistemas que la admitan.

4. Mantenimiento y protección técnica

El plan técnico deberá incluir la evaluación de actualizaciones, cambios controlados, respaldo de configuraciones, segmentación y reglas de acceso adecuadas a la arquitectura real. Se definirán mecanismos para detectar anomalías y mitigar tráfico dañino. La aplicación de controles debe respetar la confidencialidad de las comunicaciones y no autoriza inspección indiscriminada de contenidos.

5. Gestión de incidentes

La ruta de atención comprende: recibir el reporte; registrar fecha, contacto y afectación; valorar severidad; asignar responsable; contener el incidente; recuperar el servicio; comunicar avances pertinentes; y documentar cierre y mejoras. La empresa debe determinar sus tiempos de atención, responsables y mecanismos de escalamiento. Se conservarán únicamente las evidencias necesarias y se notificarán los incidentes a las autoridades o titulares cuando exista obligación aplicable.

6. Recomendaciones al usuario

Utiliza contraseñas únicas y robustas, actualiza tus dispositivos, activa mecanismos de protección y verifica los enlaces antes de abrirlos. Mantén el router en un lugar seguro; utiliza cifrado Wi-Fi compatible con tu equipo; no compartas claves de administración; y desconfía de solicitudes de códigos o credenciales. No restablezcas a fábrica ni manipules instalaciones del proveedor sin orientación técnica.

7. Reporte seguro

Para reportar una falla indica el nombre del titular, un contacto, la dirección del servicio y una descripción con fecha aproximada. No envíes contraseñas, códigos de autenticación, datos bancarios completos ni contenidos ilegales. El reporte técnico no sustituye la denuncia ante autoridad cuando existan hechos que puedan constituir delito.

8. Seguimiento y actualización

El área técnica debe mantener la documentación de los controles, registrar las actuaciones frente a incidentes y revisar estos lineamientos cuando cambien la infraestructura, los riesgos o las obligaciones aplicables. Las solicitudes de soporte se reciben a través de los canales indicados en este documento.

Canales de atención

Correo: conectainternetsas@gmail.com. Dirección: Calle 2 #5-19, Tena, Cundinamarca. Soporte y ventas (teléfono y WhatsApp): 322 357 2801. Área de facturación (teléfono y WhatsApp): 313 464 4205.

Fuentes de consulta

Resolución CRC 5050 de 2016, texto compilado. Revisar notas de vigencia y transición aplicables a servicios fijos.
https://normograma.crcom.gov.co/crc/compilacion/docs/resolucion_crc_5050_2016.htm