



Comunicaciones sin limites

# GUIA DE SEGURIDAD EN LA RED

# SEGURIDAD EN LA RED

- La seguridad de la red se refiere a todas las medidas y precauciones que se toman para proteger la información y los datos que se transmiten a través de una red. Su importancia radica en varios aspectos;

## 1 INTEGRIDAD Y CONFIDENCIALIDAD

**INTEGRIDAD** : Garantiza que los datos no sean alterados de manera no autorizada. esto significa proteger la integridad de los registros de llamadas, datos de clientes y configuraciones de red.

**CONFIDENCIALIDAD**: Asegura que solo las personas autorizadas tengan acceso a la información sensible. En telecomunicaciones, esto incluye datos de facturación, contratos y detalles de servicios.

## 2 PREVENCIÓN DE CIBERATAQUES

- Las empresas de telecomunicaciones son objetivos atractivos para ciberdelincuentes. La seguridad de la red busca evitar ataques como el robo de datos, el secuestro de cuentas o el acceso no autorizado a infraestructuras críticas.
- Medidas como firewalls, sistemas de detección de intrusiones y actualizaciones regulares son esenciales para prevenir amenazas.

## 3 CONTROL DE ACCESO

- Las redes de telecomunicaciones manejan grandes volúmenes de datos. Es crucial controlar quiénes pueden acceder a qué recursos.
- Autenticación sólida y políticas de acceso garantizan que solo los empleados autorizados y los sistemas confiables tengan acceso.



# SEGURIDAD EN LA RED

En la seguridad en la red existen diversas vulnerabilidades y amenazas que pueden afectar la seguridad de sus sistemas y datos.



## 1 VULNERABILIDADES

- **Errores de Configuración:** Configuraciones incorrectas o descuidadas pueden dejar puertas abiertas para los atacantes. Por ejemplo, si un cortafuegos no está correctamente configurado, podría permitir el acceso no autorizado.
- **Software Desactualizado:** No mantener actualizados los sistemas operativos, aplicaciones y software de seguridad puede exponer a la empresa a vulnerabilidades conocidas. Los ciberdelincuentes buscan explotar estas debilidades.
- **Fallas en el Diseño:** Algunos sistemas pueden tener defectos de diseño que los hacen susceptibles a ataques. Identificar y corregir estas fallas es esencial.

## 2 AMENAZAS

- **Malware:** Los programas maliciosos (como virus, troyanos y ransomware) son una amenaza constante. Pueden robar datos, dañar sistemas o bloquear el acceso a archivos.
- **Ataques de Denegación de Servicio (DDoS):** Los atacantes inundan los servidores con tráfico falso, sobrecargándolos y dejando los servicios inaccesibles para los usuarios legítimos.
- **Ingeniería Social:** Los ciberdelincuentes engañan a empleados para obtener información confidencial o acceso a sistemas. Esto puede incluir phishing, pretexting o suplantación de identidad.
- **Fugas de Datos Internas:** Los empleados pueden filtrar información sensible de manera intencional o accidental. La protección contra estas amenazas internas es crucial.

# SEGURIDAD EN LA RED

## ¿ COMO FUNCIONA EL FRAUDE EN LA RED?

### 1 Phishing y Suplantación de Identidad

- **Phishing:** Los estafadores envían correos electrónicos falsos haciéndose pasar por entidades confiables (como bancos o empresas) para obtener información personal o financiera. Por ejemplo, te llega un correo que dice ser de tu banco y te pide que ingreses tus datos en un enlace falso.
- **Suplantación de Identidad:** Aquí, los atacantes se hacen pasar por alguien que conoces (amigos, familiares o colegas) para obtener información o dinero. Puede ocurrir en redes sociales o incluso por teléfono.

### 3 Malware y Ransomware

- El malware (software malicioso) se instala en tu dispositivo sin tu conocimiento. Puede robar información o dañar tus archivos.
- El ransomware cifra tus archivos y exige un rescate para desbloquearlos.

### 2 Ingeniería Social

- Los ciberdelincuentes manipulan a las personas para que revelen información confidencial. Pueden hacerlo mediante llamadas telefónicas (vishing), mensajes de texto (smishing) o incluso en persona.
- Por ejemplo, alguien podría llamarte haciéndose pasar por un empleado de tu banco y pedirte que confirmes tus datos.

### 4 Ofertas Falsas o Premios Engañosos

- Recibes un mensaje que dice que ganaste un premio o que tienes una oferta increíble. Sin embargo, para "reclamarlo", debes proporcionar información personal o pagar una tarifa.
- Estas ofertas suenan tentadoras, pero en realidad son trampas para obtener tus datos o dinero.



## ¿ COMO PREVENIR EL FRAUDE EN LA RED?

- **Educación:** Aprende a reconocer señales de fraude. No hagas clic en enlaces sospechosos ni compartas información personal sin verificar.
- **Verificación:** Antes de proporcionar datos o dinero, verifica la autenticidad de la fuente. Llama al número oficial de la entidad o visita su sitio web directamente.
- **Actualización y Seguridad:** Mantén tus dispositivos y software actualizados. Usa herramientas de seguridad, como antivirus y firewalls.
- **Contraseñas Fuertes:** Utiliza contraseñas únicas y cambia regularmente. No uses la misma contraseña para todo.
- **Sentido Común:** Si algo parece demasiado bueno para ser verdad, probablemente lo sea. Desconfía de ofertas sorprendentes o correos inesperados.

# INTERNET SANO

## BENEFICIOS DEL INTERNET

- **Acceso a la Información:** Internet nos brinda acceso a una cantidad inmensa de conocimiento en forma de artículos, videos, tutoriales y más.
- **Aprendizaje en Grupo:** Plataformas educativas y colaborativas permiten el aprendizaje conjunto.
- **Comunicación Global:** Facilita la conexión con amigos, familiares y personas de diferentes culturas.
- **Desarrollo de Habilidades:** Juegos y videojuegos pueden mejorar habilidades cognitivas y psicomotoras.



## PROBLEMAS ASOCIADOS AL USO INADECUADO DEL INTERNET



- **Uso Abusivo:** El exceso de tiempo en línea puede afectar la salud física y mental de los niños y adolescentes.
- **Uso Delictivo:** El acoso en línea (ciberbullying), el sexting y el grooming son riesgos importantes.
- **Noticias Falsas:** La desinformación se propaga rápidamente en Internet.

## COMO PROMOVER UN INTERNET SANO

- **Educación:** Conciencia sobre los riesgos y cómo protegerse.
- **Verificación de Fuentes:** Antes de crear o compartir información, verifica su autenticidad.
- **Privacidad:** Protege tus datos personales y configura opciones de privacidad en redes sociales.
- **Uso Responsable:** Limita el tiempo en línea y equilibra con actividades fuera de la pantalla.



# INTERNET SANO

## Estrategia para proteger la identidad de niños y jóvenes en la red



Con el fin de preservar el respeto y la dignidad de los niños y jóvenes, Vive emplea e informa los alcances de la Ley 679 del 3 de agosto del 2001, expedida por el Congreso de la República, con el fin de prevenir y contrarrestar la explotación, pornografía y turismo sexual de menores de edad.

Realizada en el desarrollo del Artículo 44 de la Constitución, pretende dictar medidas preventivas y sanciones para quienes exploten y/o abusen sexualmente de los menores de edad.

Internet Sano, es una campaña del Ministerio de Comunicaciones, la cual busca proteger la identidad y dignidad de niños y Jóvenes en la red. De esta manera ayudamos a prevenir, bloquear, combatir y denunciar la explotación, alojamiento, uso, publicitación, difusión de imágenes, textos, documentos, archivos audiovisuales y cualquier uso indebido de redes de telecomunicaciones, destinados a publicar material pornográfico o alusivo a actividades sexuales de menores de edad.

En TIC confío, es el programa del Ministerio de Tecnologías de la Información y las Comunicaciones que promueve el desarrollo de las habilidades digitales para enfrentar con seguridad los riesgos asociados al uso de internet y las TIC. Así mismo, impulsa el uso y la apropiación de internet como la oportunidad para generar una huella digital positiva en el entorno digital.

### Medios para denunciar

-> Ministerio de Comunicaciones

línea nacional:

☎ 01800 09 12667

@ <http://www.mintic.gov.co/>

✉ [minticresponde@mintic.gov.co](mailto:minticresponde@mintic.gov.co)

-> Instituto Colombiano de Bienestar Familiar:

☎ 01 8000 91 8080

@ <http://www.icbf.gov.co>

✉ [notificaciones.judiciales@icbf.gov.co](mailto:notificaciones.judiciales@icbf.gov.co)

-> Policía Nacional:

☎ 01800 09 10600

@ <https://policia.gov.co>

✉ [lineadirecta@policia.gov.co](mailto:lineadirecta@policia.gov.co)



Comunicaciones sin límites

# SEGURIDAD EN LA RED

Para la empresa C&C VISION SAS es de vital importancia proteger los datos, garantiza la continuidad del servicio y mantiene la confianza de los clientes, por eso implementamos en nuestro sistema medidas de prevención para el bloqueo de paginas que afecta en buen uso de la red.

## Referencias.

Para mayor informacion consultar los siguientes sitios

- <https://www.ibm.com/es-es/topics/network-security>
- <https://www.ciberriesgos.com/fraudes-en-la-red/>
- <https://www.deltaprotect.com/blog/seguridad-de-la-red>
- <https://foundation.mozilla.org/es/internet-health/>
- <https://lopddirecta.es/que-es-la-seguridad-de-la-red/>
- <https://www.deltaprotect.com/blog/seguridad-de-la-red>
- <https://blog.getsilt.com/estrategias-prevencion-fraude-digital/>
- <https://mintic.gov.co/portal/inicio/Sala-de-prensa/Noticias/720:Internet-Sano-una-estrategia-para-proteger-la-identidad-de-ninos-y-jovenes-en-la-red>