



POLÍTICAS DE SEGURIDAD EN LA RED

Guía de Elementos, Conceptos y Recomendaciones para una Conectividad Segura

1. ELEMENTOS DE SEGURIDAD

La red mundial Internet y sus elementos asociados son mecanismos ágiles que proveen una amplia gama de posibilidades de comunicación, interacción y entretenimiento, tales como multimedia, foros, chats, correo electrónico, comunidades y bibliotecas virtuales que pueden ser accedidos por todo tipo de público. Sin embargo, estos elementos deben contener mecanismos que protejan y reduzcan los riesgos de seguridad alojados, distribuidos o potenciados a través del propio servicio de Internet.

MEGANET TELECOMUNICACIONES S.A.S. busca fortalecer la relación con sus Usuarios desde una comunicación asertiva, sana y orientada a proporcionar las herramientas y consejos prácticos necesarios para la protección adecuada de sus equipos de cómputo y los servicios asociados a la red. Por esta razón, ponemos a disposición de todos nuestros clientes y de la comunidad en general, conceptos teórico-prácticos y buenas prácticas que pueden evitar o reducir los riesgos a los que se está expuesto al interactuar en el ecosistema digital.

2. CONCEPTOS GENERALES DE SEGURIDAD

Para comprender la gestión de seguridad de la información, se definen los siguientes conceptos clave:

Confidencialidad

Garantiza que la información y los datos solo puedan ser conocidos y accedidos por individuos y sistemas autorizados.

Integridad

Asegura que la información no sea alterada, borrada, duplicada o reordenada de forma maliciosa durante su transmisión o almacenamiento.

Disponibilidad

Asegura que la información y los servicios de red puedan ser accedidos y recuperados por

Seguridad de la Información

Conjunto de directrices orientadas a resguardar la confidencialidad, integridad y

los usuarios autorizados en el momento
requerido.

disponibilidad, manteniendo la continuidad
del servicio.

**POLÍTICA SEGURIDAD EN LA RED****Activo de Información**

Recursos físicos (servidores, PCs, routers) o lógicos (datos, bases de datos, políticas, licencias) que poseen valor para el usuario o la empresa.

Vulnerabilidad

Debilidad o fallo de seguridad presente en un sistema operativo, software, firmware o configuración de red.

Amenaza

Cualquier circunstancia o evento con potencial de causar daño a un activo de información mediante un ataque o intrusión.

Riesgo

Probabilidad de que una amenaza aproveche una vulnerabilidad del sistema causando un impacto negativo en la operación o seguridad.

3. ELEMENTOS DE PROTECCIÓN DE RED

- **Firewall (Cortafuegos):** Filtra el tráfico de paquetes (entrantes y salientes) de una red basada en reglas y directivas preestablecidas, bloqueando accesos no autorizados.
- **Antivirus:** Software diseñado para detectar, contener y neutralizar malware, incluyendo virus, troyanos, gusanos (worms), spyware, rootkits y adwares.
- **Antispam:** Filtro especializado para servidores de correo electrónico que identifica y aísla mensajes publicitarios, fraudulentos o masivos no solicitados.
- **Criptografía:** Proceso de codificación de la información utilizando claves secretas para que solo los destinatarios autorizados puedan descifrar y leer los datos.

4. AMENAZAS Y FRAUDES COMUNES EN INTERNET

- **Ingeniería Social:** Técnicas de manipulación psicológica aplicadas por atacantes para que los usuarios revelen claves o ejecuten acciones inseguras de forma voluntaria.
- **Malware (Código Malicioso):** Programas de software espía, virus o secuestradores de datos diseñados para infiltrarse en dispositivos sin el consentimiento del usuario.
- **Phishing (Suplantación de Identidad):** Sitios web fraudulentos o correos falsos estructurados para imitar la apariencia de entidades oficiales (bancos, proveedores) y así robar datos bancarios o

contraseñas.

- **Vishing:** Fraude de suplantación de identidad realizado a través de llamadas de voz IP.
- **Smishing:** Mensajes de texto (SMS) fraudulentos enviados con enlaces trampa a dispositivos móviles.

¿Cómo detectar Sitios de Phishing?

Preste atención a la barra de direcciones (URL). Los estafadores suelen usar variaciones engañosas en el dominio como: `www.miBanco-seguro.com` o subdominios maliciosos como `www.miBanco.com.servidor-externo.com`. Ingrese siempre digitando la dirección oficial directamente en el navegador y nunca haga clic en enlaces enviados por correo o mensajería instantánea.



5. CONSEJOS Y TIPS DE SEGURIDAD PARA EL USUARIO

- **Seguridad de Contraseñas:** Utilice contraseñas robustas con una extensión mínima de 10 caracteres, combinando mayúsculas, minúsculas, números y caracteres especiales. Cámbielas cada 30 o 45 días.
- **Uso Seguro de Correo Electrónico:** Nunca publique su dirección de correo en portales públicos no confiables. Si recibe notificaciones de restablecimiento de contraseña no solicitadas, desestímelas e ingrese al portal oficial de forma independiente.
- **Actualización de Software:** Mantenga al día el sistema operativo (Windows, Android, macOS), los navegadores web (Chrome, Firefox) y las aplicaciones de seguridad para asegurar la corrección de fallas críticas.
- **Seguridad en Wi-Fi:** Asegúrese de que su enrutador doméstico esté configurado con cifrado WPA2 o WPA3 y con una contraseña de red personalizada y robusta.

6. MEDIDAS DE SEGURIDAD DE MEGANET TELECOMUNICACIONES S.A.S.

Para garantizar la protección de la infraestructura y el tráfico de internet, MEGANET TELECOMUNICACIONES S.A.S. implementa los siguientes controles técnicos perimetrales:

- **Firewall Perimetral:** Filtros a nivel de infraestructura para repeler ataques de denegación de servicio (DDoS) e intrusiones externas.
- **Filtros DNS y Bloqueo Legal (Ley 679 de 2001):** Bloqueo automatizado de URLs y dominios que contengan o difundan material de explotación infantil o contenidos fraudulentos señalados por las autoridades del orden nacional.
- **Neutralidad de Red:** MEGANET TELECOMUNICACIONES S.A.S. da estricto cumplimiento a las directrices de neutralidad en la red y las políticas del Ministerio de las TIC. Exceptuando los bloqueos regulatorios legales obligatorios, la empresa no restringe, limita ni bloquea la libre navegación de sus usuarios ni altera el acceso a contenidos digitales legítimos en internet.

Reportar Delitos Informáticos y Enlaces Sospechosos:

Manténgase informado y reporte cualquier intento de fraude digital a través de los portales gubernamentales de Colombia:

- **Línea de Denuncia MinTIC y Red PaPaz:** www.teprotejo.org
- **CAI Virtual de la Policía Nacional:** caivirtual.policia.gov.co / lineadirecta@policia.gov.co

- **Líneas Gratuitas de Atención:** Fiscalía General (122) / Policía Nacional (Línea 123)