NAVEGACIÓN SEGURA

Lo que necesita saber para evitar amenazas en la red.

Tipos de amenazas en la red

Para SEAN COMUNICACIONES SAS la seguridad en la red es muy importante, por tal razón en este documento encontrará información para una navegación segura:

Malware

Es un término general utilizado para referirse a distintas formas de software hostil, intrusivo o molesto. El software malintencionado o malware es creado por hackers para perturbar operaciones de una computadora, obtener información confidencial o acceder a sistemas informáticos privados.
Incluye virus informáticos, gusanos, troyanos, spyware, adware, la mayoría de rootkits y otros programas malintencionados.

Spyware

El spyware es un software malintencionado que se instala en computadoras para obtener información sin el conocimiento del usuario. Puede ser difícil de detectar y, en algunos casos, como los keyloggers, se usa para controlar a los usuarios. También puede obtener datos personales, interferir en el sistema y afectar su rendimiento.

Spam

Consiste en el uso de sistemas de mensajes electrónicos para enviar de forma indiscriminada un gran número de mensajes no solicitados. El término también se aplica a spam en mensajería instantánea, motores de búsqueda, blogs, wikis, redes sociales, SMS, foros, etc.

Phishing

Es un intento de obtener información personal, como usuarios, contraseñas y datos bancarios, suplantando una entidad de confianza mediante correos o mensajes que redirigen a páginas fraudulentas. Esta técnica aprovecha vulnerabilidades de seguridad y se combate con legislación, formación y mejoras tecnológicas.

Pharming

Ataque que redirecciona el tráfico de un sitio web hacia una página fraudulenta. Es la combinación de “phishing” y “farming”. Su objetivo es obtener datos usados para robo de identidad. Es especialmente grave para empresas de comercio y banca electrónica.

RECOMENDACIONES DE SEGURIDAD

Material de Abuso Sexual Infantil (MASI)
Evite alojar, publicar o transmitir cualquier contenido que involucre actividades sexuales con menores de edad, según la Ley 679 de 2001, el Decreto 1524 de 2002 y demás normas aplicables.

Control de virus y códigos maliciosos

- Mantenga antivirus actualizado y ejecútelo periódicamente.
- Use anti-spyware y bloqueadores de ventanas emergentes.
- Evite páginas no confiables o instalar software de dudosa procedencia.
- Aplique actualizaciones del sistema operativo y navegadores.
- Deshabilite pop-up, Java, ActiveX o autoejecución si no los requiere.
- Utilice un firewall personal para reducir riesgos.

Correo electrónico

- No publique su correo en sitios no confiables.
- No preste su cuenta.
- No divulgue información personal o sensible por correo.
- No responda advertencias bancarias recibidas por correo.
- No responda formularios HTML incrustados.
- Si ingresó su clave en un sitio no confiable, cámbiela de inmediato.

Control de Spam y Hoax

- No haga clic en enlaces de correos sospechosos.
- Escriba la URL manualmente en el navegador.
- Verifique certificados SSL en sitios que dicen ser seguros.
- No reenvíe cadenas de correos.

Control de Ingeniería Social

- No divulgue información confidencial propia o de terceros.
- No converse con desconocidos sobre temas laborales o personales.
- Use los canales adecuados para divulgar información.

Control de phishing y modalidades

- No responda correos, llamadas o mensajes sobre advertencias bancarias.
- Verifique el certificado SSL.
- Confirme la validez del mensaje con la entidad correspondiente.

Robo de contraseñas

- Cambie sus contraseñas cada 30 días.
- Use contraseñas fuertes, mínimo de 10 caracteres con números y símbolos.
- No envíe contraseñas por correo ni medios sin cifrado.

MECANISMOS DE SEGURIDAD

Contamos con sistemas de autenticación y autorización para controlar el acceso a los servicios de la red. Disponemos de protecciones como:

Firewall
Primera línea de protección perimetral ante riesgos.

Antivirus
Protege estaciones de trabajo y servidores internos.

Antispam
Reduce correos no solicitados y congestión de buzones.

Filtrado de URL
Bloquea contenido MASI mediante servidores especializados.
Se sugiere instalar sistemas parentales.

Seguridad en el CPE
Los dispositivos del cliente cuentan con autenticación y autorización para una conexión más segura.

GARANTÍA DE SEGURIDAD DE LA RED E INTEGRIDAD DEL SERVICIO

Mantenemos monitoreo constante de los elementos técnicos para detectar eventos o anomalías mediante:

- Estado de los equipos.
- Logs de actividades.
- Comportamiento de tráfico en la red.
- Informes de Firewall.
- Backups protegidos.
- Comités de evaluación de seguridad.

MODELOS DE SEGURIDAD ADAPTADOS A LA RED (UIT)

1. Autenticación

Basada en UIT X.805 y X.811. Modelo descentralizado para evitar riesgos masivos.

2. Control de Acceso

Según UIT X.810 y X.812, aplicando medidas físicas y lógicas.

3. Registros de Auditoría

Conservamos logs de acceso y actividad en CORE y ACCESO.

4. Confidencialidad de Datos

Protegida mediante cifrado y controles de acceso.

5. Privacidad

La información de usuarios no se divulga sin autorización.

6. Integridad de Datos

Actualizaciones y mitigación de vulnerabilidades.

7. Disponibilidad

Infraestructura redundante y sistemas de respaldo.

MEDIDAS DE SEGURIDAD PARA GARANTIZAR CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

Implementamos autenticación, protección, cifrado y monitoreo continuo, además de controles de acceso y sistemas de detección.

Tratamiento de incidentes en seguridad
Realizamos análisis forense para recuperar información y rastrear eventos.

Mecanismos para garantizar confidencialidad, integridad y disponibilidad
Cumplimos regulaciones para manejar información del usuario y prevenir fraudes.

---

3. Prácticas de gestión de tráfico: NEUTRALIDAD EN LA RED

SEAN COMUNICACIONES SAS:

1. No bloquea contenidos sin consentimiento del usuario, salvo obligaciones legales (contenido MASI).
2. Implementa medidas de gestión de tráfico razonables y no discriminatorias.
3. No limita el acceso ni prioriza servicios, contenidos o protocolos específicos.