Parte I.

Seguridad informática en las comisarías de familia.

La seguridad informática es esencial para garantizar que la información confidencial esté a salvo y que los servicios se brinden de manera segura y eficiente.

Por lo anterior, es importante que las comisarías de familia implementen estrategias que aseguren de manera práctica y eficaz la información que administran.

Conoce algunas estrategias para fortalecer la seguridad informática en las comisarías de familia:

Contraseñas seguras

Las contraseñas son la puerta de acceso a información sensible y privada que se manejan en las diversas plataformas tecnológicas. Elegir una contraseña segura es importante para mantener la información a salvo, al igual que cambiar las contraseñas regularmente, al menos cada tres meses.

Consejos para crear contraseñas seguras:

- Utilizar al menos 12 caracteres.
- Mezclar letras mayúsculas y minúsculas.
- Incluir números y caracteres especiales como: !, @, o #.
- Evitar el uso de información personal como nombres o fechas de nacimiento.
- No utilizar contraseñas obvias como "123456" o palabras sencillas.

Protección de datos sensibles

La protección de datos es esencial para garantizar la privacidad y seguridad de las personas que acuden a la comisaría de familia.

Cómo manejar y proteger información confidencial:

- Identificar y clasificar datos confidenciales, relatos, datos de víctimas, pruebas.
- Garantizar que esta información tenga acceso restringido.
- Limitar la información que se comparte interna y externamente solo a personal autorizado.

Evita el phishing

El phishing es una técnica que consiste en el envío de un correo electrónico por parte de un ciberdelincuente a un usuario, simulando ser una entidad legítima (red social, banco, institución pública, etc) solicitando información privada.

La conciencia y la vigilancia son claves para evitar el phishing y proteger la seguridad de la comisaría y su personal.

Cómo reconocer correos electrónicos y enlaces de phishing:

- Desconfiar de correos electrónicos no solicitados.
- Verificar la dirección de correo electrónico del remitente.
- No hacer clic en enlaces sospechosos, ni descargar archivos adjuntos no esperados.
- No compartir información confidencial a través de correos electrónicos no seguros.
- Generalmente son correos que realizan promesas difíciles de cumplir o amenazas por alguna acción que el usuario supuestamente ha cometido.

Consejos para no caer en estafas cibernéticas:

- Educar a todo el personal sobre cómo reconocer el phishing.
- Utilizar software de filtrado de correos electrónicos y antivirus.
- Reportar correos sospechosos a los administradores de la red.
- Mantener un registro de incidentes de phishing.