El planteamiento cuantitativo del problema, según Roberto Hernández Sampieri, implica estructurar formalmente la idea de investigación y definir claramente el problema a investigar. Este proceso incluye varios elementos clave:

**Objetivos de investigación**: Deben ser claros y alcanzables, sirviendo como guía durante todo el estudio.

**Preguntas de investigación**: Formuladas de manera precisa para orientar la investigación.

**Justificación del estudio:** Explicación de la importancia y los beneficios de realizar la investigación.

**Viabilidad de la investigación**: Evaluación de los recursos y el tiempo necesarios para llevar a cabo el estudio.

**Evaluación de deficiencias en el conocimiento**: Identificación de las lagunas en el conocimiento actual sobre el tema.

Estos elementos ayudan a asegurar que el problema de investigación esté bien definido y que la investigación sea viable y relevante.

—-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Tema hipotético: “El impacto del uso de redes sociales en el rendimiento académico de los estudiantes universitarios”.

1. **Objetivos de investigación**:
   * Determinar la relación entre el tiempo dedicado a las redes sociales y el rendimiento académico de los estudiantes universitarios.
   * Identificar las redes sociales más utilizadas por los estudiantes y su influencia en sus hábitos de estudio.
2. **Preguntas de investigación**:
   * ¿Existe una correlación significativa entre el tiempo de uso de redes sociales y el rendimiento académico?
   * ¿Qué redes sociales son las más utilizadas por los estudiantes universitarios?
   * ¿Cómo afecta el uso de redes sociales a los hábitos de estudio de los estudiantes?
3. **Justificación del estudio**:
   * Este estudio es importante porque el uso de redes sociales ha aumentado significativamente entre los jóvenes, y es crucial entender cómo esto puede estar afectando su rendimiento académico. Los resultados podrían ayudar a desarrollar estrategias para mejorar los hábitos de estudio y el rendimiento académico.
4. **Viabilidad de la investigación**:
   * La investigación es viable ya que se puede realizar mediante encuestas y análisis de datos académicos. Se cuenta con el apoyo de la universidad para acceder a los estudiantes y sus registros académicos, y se dispone de los recursos necesarios para llevar a cabo el estudio.
5. **Evaluación de deficiencias en el conocimiento**:
   * Aunque existen estudios sobre el uso de redes sociales y el rendimiento académico, hay una falta de investigaciones específicas que analicen cómo diferentes redes sociales afectan de manera distinta a los hábitos de estudio y el rendimiento académico de los estudiantes universitarios en esta región.

Ciberseguridad en Redes Sociales

La ciberseguridad en redes sociales se refiere a las medidas adoptadas para proteger a los usuarios de ciberamenazas como el phishing, el malware y el robo de identidad en las plataformas de redes sociales. Estas medidas incluyen:

Uso de contraseñas fuertes y únicas

Autenticación en dos pasos (2FA)

Protección de la cuenta con sistemas biométricos y reconocimiento facial

Vigilancia constante de las actividades en la cuenta y notificación de posibles incidentes

Implementación de políticas de seguridad claras para los empleados y usuarios

Monitoreo y respuesta rápida a posibles incidentes de seguridad

La ciberseguridad en redes sociales es esencial para garantizar que la presencia en línea siga siendo segura y que la información personal esté protegida. De lo contrario, los usuarios corren riesgos como:

Acceso no autorizado a sus cuentas y datos personales

Distribución de malware y virus

Estafas y phishing

Daño a la reputación y la marca en la red

Es importante recordar que las redes sociales son un punto de entrada ideal para la distribución de malware y ataques cibernéticos, y que la ciberseguridad debe ser un proceso continuo y activo para protegerse contra estos riesgos.

Algunos consejos prácticos para mantener la ciberseguridad en redes sociales incluyen:

No compartir información personal o confidencial

No utilizar la misma contraseña para todas las cuentas

No aceptar amigos o seguidores no conocidos

No abrir archivos o enlaces sospechosos

Utilizar software de seguridad actualizado y antivirus

Monitorear constantemente las actividades en la cuenta y reportar cualquier incidente de seguridad

Es fundamental ser consciente de los riesgos y tomar medidas para protegerse en las redes sociales, ya que la ciberseguridad es un tema cada vez más importante en la era digital.

### **Malware**

Malware significa software malintencionado. Incluye una variedad de programas de software creados para permitir que terceras partes accedan de manera no autorizada a información confidencial o interrumpan el funcionamiento normal de una infraestructura crítica. Entre los ejemplos más comunes de malware se incluyen los troyanos, spyware y virus.

[El **malware** (contracción de “malicious software” en inglés) es cualquier tipo de software diseñado para dañar, infiltrarse o tomar control de sistemas informáticos sin el consentimiento del usuari](https://www.malwarebytes.com/es/malware)o. Aquí tienes algunos tipos comunes de malware y ejemplos de cada uno:

1. **Virus**: Programas que se adjuntan a otros archivos y se propagan cuando esos archivos se comparten.
   * **Ejemplo**: **ILOVEYOU** - Un virus que se propagó a través de correos electrónicos en el año 2000, causando daños masivos.
2. **Gusanos**: Similar a los virus, pero no necesitan adjuntarse a otros archivos para propagarse.
   * **Ejemplo**: **WannaCry** - Un gusano que afectó a miles de computadoras en 2017, cifrando archivos y pidiendo un rescate.
3. **Troyanos**: Programas que se disfrazan de software legítimo para engañar a los usuarios y obtener acceso a sus sistemas.
   * **Ejemplo**: **Zeus** - Un troyano que roba información bancaria y credenciales de acceso.
4. **Spyware**: Software que recopila información sobre el usuario sin su conocimiento.
   * **Ejemplo**: **Keylogger** - Un tipo de spyware que registra las pulsaciones del teclado para robar contraseñas y otra información sensible.
5. **Adware**: Software que muestra anuncios no deseados y a veces maliciosos.
   * **Ejemplo**: **Fireball** - Un adware que secuestra navegadores y muestra anuncios intrusivos.
6. **Ransomware**: Malware que cifra los archivos del usuario y exige un pago para desbloquearlos.
   * **Ejemplo**: **CryptoLocker** - Un ransomware que cifró archivos de usuarios y pidió un rescate en bitcoins.

Estos son solo algunos ejemplos de los muchos tipos de malware que existen. [Es importante mantener tus sistemas actualizados y utilizar software de seguridad para protegerte contra estas amenazas](https://latam.kaspersky.com/resource-center/threats/types-of-malware)

El \*\*ransomware\*\* es un tipo de malware que secuestra la información de un dispositivo y exige un pago para liberarla. Su nombre proviene de las palabras en inglés "ransom" (rescate) y "software"¹.

### ¿Cómo funciona?

1. \*\*Infección\*\*: El ransomware se introduce en el sistema a través de correos electrónicos maliciosos, descargas de software infectado o vulnerabilidades en la red.

2. \*\*Cifrado\*\*: Una vez dentro, cifra los archivos del dispositivo, haciéndolos inaccesibles para el usuario.

3. \*\*Demanda de rescate\*\*: Los atacantes exigen un pago, generalmente en criptomonedas, a cambio de la clave de descifrado que permite recuperar los archivos².

### Tipos de ransomware

- \*\*Ransomware de cifrado\*\*: Cifra los archivos y exige un rescate para descifrarlos.

- \*\*Ransomware de bloqueo\*\*: Bloquea el acceso al dispositivo y muestra una pantalla de bloqueo que exige el pago².

### Prevención 38041304

- Mantén tus sistemas y software actualizados.

- Realiza copias de seguridad periódicas de tus datos.

- No abras correos electrónicos o enlaces sospechosos¹.

[Un **ataque de intermediario** o **man-in-the-middle (MITM)** es un tipo de ciberataque en el que un atacante se inserta en la comunicación entre dos partes sin que estas lo sepan1](https://www.stackscale.com/es/blog/ataque-de-intermediario/). El objetivo es interceptar, espiar, y a veces modificar la información que se transmite entre las partes.

### **¿Cómo funciona?**

1. **Intercepción**: El atacante intercepta la comunicación entre dos partes. [Esto puede hacerse a través de redes Wi-Fi públicas, suplantación de IP, suplantación de ARP, o envenenamiento de DNS1](https://www.stackscale.com/es/blog/ataque-de-intermediario/)[2](https://blog.tecnetone.com/ataque-de-intermediario-qu%C3%A9-es-y-c%C3%B3mo-prevenirlo).
2. [**Desencriptación**: Una vez interceptada la comunicación, el atacante puede desencriptar los datos para acceder a información sensible como contraseñas, datos personales o información financiera1](https://www.stackscale.com/es/blog/ataque-de-intermediario/).

### **Tipos de ataques de intermediario**

* **Interceptación de datos**: Captura información sin modificarla.
* **Secuestro de sesiones**: Toma el control de una sesión activa, como en redes sociales.
* **Ataque de intermediario en redes**: Explota vulnerabilidades en redes Wi-Fi para interceptar datos.
* [**Man-in-the-browser**: Controla el navegador web del usuario para robar o modificar información directamente2](https://blog.tecnetone.com/ataque-de-intermediario-qu%C3%A9-es-y-c%C3%B3mo-prevenirlo).

### **Prevención**

* **Usar conexiones seguras (HTTPS)**.
* **Evitar redes Wi-Fi públicas no seguras**.
* **Implementar autenticación mutua**.
* [**Mantener el software actualizado**1](https://www.stackscale.com/es/blog/ataque-de-intermediario/).