1. Metodología

Para el desarrollo de este estudio se utilizó la metodología PoC de vulnerabilidad (Shah & Mehtre, 2015), cuyo propósito es validar si una vulnerabilidad identificada puede ser explotada. Las etapas de una PoC están diseñadas para demostrar que una vulnerabilidad identificada en un sistema puede ser explotada. Estas etapas ayudan a validar el riesgo asociado y a priorizar medidas de mitigación.

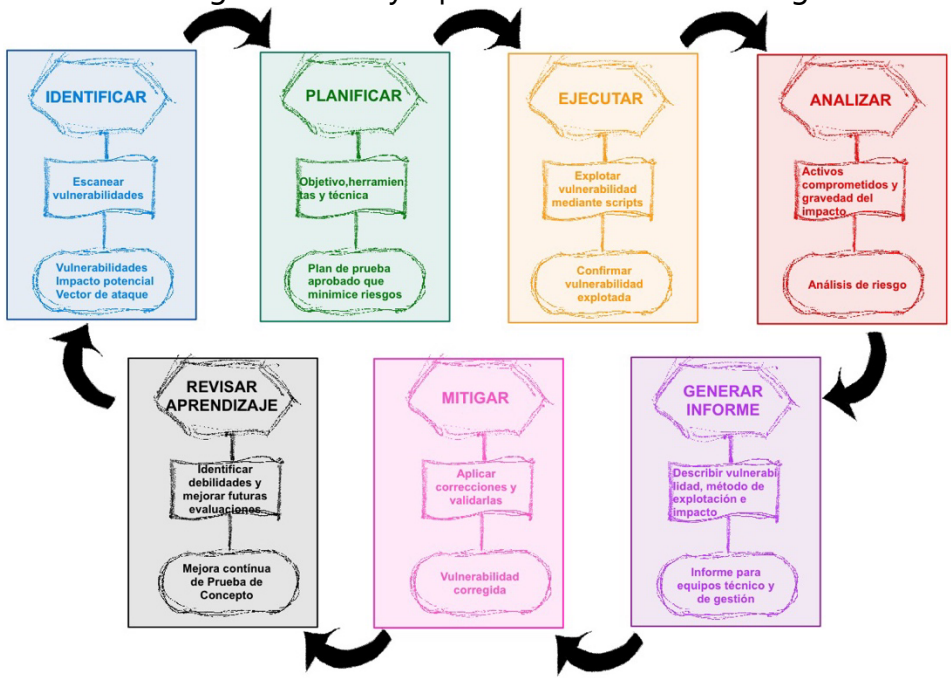

Figura 1. Metodología de prueba de concepto de vulnerabilidad

A continuación se definen en detalle las etapas de la PoC mostrado en la Figura 1.

I. **Identificar la vulnerabilidad**

En esta etapa se detecta y documenta una posible vulnerabilidad. Esto puede hacerse mediante herramientas de análisis, informes de auditoría o exploración manual. *Actividades*: Uso de escáneres de vulnerabilidades. Revisión de reportes de seguridad en las bases de datos de amenazas conocidas. Análisis del código fuente o configuraciones del sistema. *Resultado esperado*: Un informe detallado sobre la vulnerabilidad detectada, su impacto potencial y su vector de ataque.

II. **Planificar la prueba**

En esta etapa se define el alcance, los objetivos y las herramientas que se utilizarán para realizar la PoC. *Actividades*: Establecer los sistemas objetivo y los entornos de prueba. Seleccionar las herramientas y técnicas necesarias. Identificar posibles impactos y medidas de contención. *Resultado esperado*: Un plan de prueba claro y aprobado por las partes interesadas, que minimice riesgos durante la ejecución.

III. **Ejecutar la prueba**

Se intenta explotar la vulnerabilidad identificada para verificar su validez. *Actividades*: Implementar scripts o exploits para aprovechar la vulnerabilidad. Documentar el comportamiento del sistema bajo ataque. Analizar los resultados de la prueba. *Resultado esperado*: Confirmación o refutación de que la vulnerabilidad puede ser explotada.

IV. Analizar el impacto

Se evalúa el impacto potencial de la explotación exitosa de la vulnerabilidad en el sistema o red objetivo. *Actividades*: Identificar los activos comprometidos. Medir la gravedad del impacto en términos de confidencialidad, integridad y disponibilidad. *Resultado esperado*: Un análisis detallado del riesgo asociado a la vulnerabilidad.

V. Generar el informe

Se documentan los hallazgos de la prueba de concepto, incluyendo detalles técnicos y recomendaciones. *Actividades*: Preparar un informe con la descripción de la vulnerabilidad, el método de explotación, el impacto y las pruebas realizadas. Proporcionar recomendaciones de mitigación o corrección. *Resultado esperado*: Un informe estructurado para informar a los equipos técnicos y de gestión.

VI. Mitigar

Se aplican las medidas correctivas recomendadas y se valida su efectividad. *Actividades*: Implementar parches, configuraciones o controles de seguridad. Repetir la prueba para confirmar que la vulnerabilidad ha sido mitigada. *Resultado esperado*: Garantía de que el sistema ya no es vulnerable.

VII. Revisar y lecciones aprendidas

Reflexión sobre el proceso de la prueba para mejorar futuras evaluaciones. *Actividades*: Identificar debilidades en el enfoque de prueba. Incorporar aprendizajes en la documentación de procedimientos y políticas de seguridad. *Resultado esperado*: Mejora continua de los procesos de pruebas de concepto.

Además de la PoC, también se utilizó la taxonomía TRACI, que hace parte del modelo MoRCiTO, cuyo propósito es clasificar y medir ciberataques en los 16 sectores de infraestructuras críticas definidos por Cybersecurity and Infrastructure Security Agency (CISA, 2025). TRACI se organiza en tres dimensiones que tienen igual importancia en la representación gráfica. Cada dimensión cuenta con características derivadas de la literatura y entrevistas a expertos en ciberseguridad.

Figura 2. TRACI. Tomado de (Plachkinova & Vo, 2023)

i. **Activos**: Incluye componentes cibernéticos, físicos y ciber-físicos de cualquier CPS.
ii. **Gestión de riesgos**: Considera amenazas, vulnerabilidades y controles.
iii. **Motivación del adversario**: Explica las razones del ciberataque, como políticas, socioculturales, económicas o por emoción.

Cada categoría se mide en una escala de 1 a 5 según su relevancia, expandiéndose hacia el exterior (ver Figura 2). Un valor de 0 indica información insuficiente, lo que puede ocurrir debido a la sensibilidad de los datos en IC y ataques contra ellas.

1.1 Escenario de la PoC

A continuación se describe en detalle el escenario: "*La infraestructura crítica de telecomunicaciones de una de las empresas más importantes de Colombia, en adelante se llamará "la empresa", ofrece a sus clientes el servicio de Internet Service Provider (ISP). Los cable-modems que instala a sus clientes son marca Technicolor, modelo tc8305.e, estos dispositivos quedan configurados por los técnicos de la empresa con la contraseña de administración por defecto, lo que ha causado como consecuencia que adversarios realicen ataques masivos por diccionario haciéndose administradores del dispositivo y de esta forma con acceso a los diferentes dispositivos conectados al cable-modem con la posibilidad de escalar el ataque modificando el servicio DNS del dispositivo, engañando a los clientes para robar credenciales de acceso a sitios financieros, redes sociales y demás servicios que requieran autenticación. También pueden actualizar el firmware del dispositivo para para instalar un kit de herramientas de software malicioso (rootkit) y de esta forma garantizar persistencia, acceso de bajo nivel, sigilo y acceso remoto al dispositivo infectado*".

1.2 Evaluación de riesgo según TRACI

Se procede aplicar la taxonomía TRACI sobre el escenario de la PoC en cada una de sus tres dimensiones y se cuantifica la valoración de su relevancia en cada subdimensión con su respectiva descripción (ver Tabla 1).

Tabla 1. Aplicación de la taxonomía TRACI sobre el escenario de la PoC

Dimensión	Subdimensión	Descripción	Relevancia (1-5)
Activos	Cibernéticos	Acceso administrativo a los cable-modems de la empresa mediante ataque por diccionario.	5
	Ciber-físicos	Modificación del firmware del cable-modem para instalar rootkits.	5
	Físicos	Acceso remoto y persistencia sobre los dispositivos comprometidos.	5
Gestión de riesgo	Amenazas	Ataques de phishing mediante modificación de DNS para robar credenciales.	5
	Vulnerabilidades	Configuración con credenciales de administración por defecto en dispositivos Technicolor del modelo tc8305.e.	5
	Controles	Falta de implementación de medidas de seguridad en la configuración inicial del dispositivo.	4
Motivación del adversario	Política	Potencial explotación de vulnerabilidades de infraestructura de telecomunicaciones con fines estratégicos.	5
	Socio-cultural	Uso del ataque para generar desinformación o manipular contenido en redes sociales.	3
	Económica	Posibilidad de venta de credenciales robadas en el mercado negro.	4
	Búsqueda de emoción	Ataques realizados por curiosidad o reto técnico de los adversarios.	3

I. Activos afectados

Los activos comprometidos abarcan tres subdimensiones clave (ver Figura 3 y Tabla 1).

Impacto: Todos los activos evaluados presentan un riesgo crítico (5/5), lo que indica un nivel de vulnerabilidad extremo y una superficie de ataque que permite un control total del dispositivo por parte de los adversarios.

Consecuencia: Al comprometerse estos activos, los adversarios pueden secuestrar el tráfico de red, modificar configuraciones sensibles y establecer persistencia en la infraestructura.

II. Gestión del riesgo

El análisis de TRACI identifica tres subdimensiones clave en la gestión del riesgo (ver Figura 3 y Tabla 1).

Impacto: La principal vulnerabilidad es la configuración por defecto de las credenciales de administración, lo que permite ataques masivos con herramientas automatizadas. Además, la modificación del servicio DNS facilita ataques de phishing, aumentando la exposición de los usuarios.

Deficiencia de controles: La calificación de 4/5 indica que existen medidas de mitigación insuficientes, lo que significa que la empresa no ha implementado controles efectivos para reducir el riesgo.

III. Motivación del adversario

La taxonomía TRACI evalúa las razones detrás del ataque (ver Figura 3 y Tabla 1).

Motivación principal: El ataque puede ser explotado con fines estratégicos (5/5), lo que indica un posible interés en el control de infraestructura de telecomunicaciones para espionaje, sabotaje o ciber-operaciones avanzadas.

Amenaza económica: El mercado negro de credenciales robadas (4/5) es una motivación importante para los atacantes, lo que aumenta la probabilidad de ataques dirigidos y automatizados a gran escala.

Ataques con fines de desinformación: Si bien la manipulación de redes sociales y la desinformación (3/5) no es la motivación principal, podría ser un vector de explotación adicional.

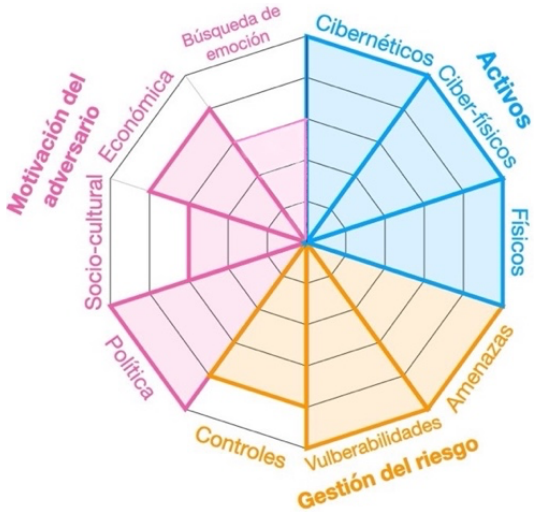

Figura 3. TRACI sobre el escenario de la PoC. Tomado de (Plachkinova & Vo, 2023)

1.3 Recomendaciones de mitigación

Con base en la evaluación de TRACI, se identifican acciones críticas para mitigar la vulnerabilidad:

I. Acciones sobre la infraestructura

Cambio obligatorio de credenciales por defecto: Implementar una política que exija el cambio de contraseña en la configuración inicial. Uso de contraseñas robustas generadas automáticamente por el sistema.

Limitación del acceso administrativo: Implementar autenticación multifactor (MFA) en la interfaz de administración de los cable-modems. Restringir el acceso remoto solo a direcciones IP autorizadas.

Actualización y validación de firmware: Asegurar que los dispositivos solo acepten actualizaciones de firmware firmadas y verificadas. Implementar monitoreo en tiempo real para detectar modificaciones no autorizadas.

Monitorización de actividad sospechosa: Implementar detección de accesos anómalos y bloqueo automático de intentos fallidos de autenticación.

II. Acciones sobre la gestión del riesgo

Mejora de controles de seguridad en la configuración inicial: Incluir medidas de seguridad obligatorias antes de la activación del servicio. Realizar auditorías periódicas en la configuración de dispositivos instalados.
Educación y concienciación de los clientes: Alertar a los clientes sobre los riesgos de seguridad y la importancia de actualizar credenciales. Implementar campañas informativas sobre ataques de phishing y cómo reconocer sitios fraudulentos.

III. Acciones contra la motivación del adversario

Reducción del valor del ataque en el mercado negro: Implementar técnicas de detección y respuesta temprana para limitar el tiempo de explotación de los dispositivos comprometidos.
Acciones contra ataques con fines estratégicos: Coordinar esfuerzos con organismos de ciberseguridad del país para monitorear amenazas avanzadas dirigidas a infraestructuras críticas.

IV. Conclusión de la aplicación de la taxonomía TRACI

Se evidenció que la infraestructura de telecomunicaciones presenta riesgos críticos en ciberseguridad debido a las deficientes configuraciones iniciales y la ausencia de medidas de mitigación efectivas. El acceso administrativo a los dispositivos, la modificación de DNS para ataques de phishing y la instalación de rootkits representan peligros elevados para los clientes y la empresa.
Las acciones recomendadas apuntan a disminuir las vulnerabilidades, reforzar la gestión de riesgos y minimizar la motivación del atacante, fortaleciendo la seguridad de la infraestructura crítica. Implementar estas medidas de mitigación reducirá significativamente la exposición a los ataques y el impacto en los clientes y en la estabilidad de la red.

1.4 Desarrollo de la PoC

1.4.1 Identificación de la Vulnerabilidad

El cable-modem proporcionado por el ISP utiliza credenciales de fábrica predefinidas como:
Usuario: *admin*
Contraseña: *admin* o en blanco.
Este patrón es conocido y ampliamente documentado en bases de datos públicas de contraseñas predeterminadas, como https://www.routerpasswords.com/.

1.4.2. Planificación de la prueba

Alcance: Dispositivos cable-modems marca Technicolor, modelo tc8305.e, que provee el ISP de la empresa en Colombia.
Objetivo específico: Acceder a la interfaz de administración del dispositivo y demostrar el control completo sobre la red interna del cliente.

1.4.3. Escaner de los dispositivos

Alcance: Dispositivos cable-modems marca Technicolor, modelo tc8305.e, que provee el ISP de la empresa en Colombia.
Objetivo específico: Obtener todas las IP´s que cumplen con el alcance definido.
Se utilizó shodan desde la línea de comandos para obtener todas las IP´s de los clientes conectados al ISP de la empresa en Colombia:

```
$ shodan search Technicolor country:CO --fields ip_str,city
```

Resultado esperado: Identificación de las IP´s por ciudad de Colombia.

Tabla 2. Cantidad de direcciones IP´s identificadas por ciudades colombianas

	Ciudades	Cantidad de IP´s
1.	Bogotá	28
2.	Pereira	3
3.	Cúcuta	2
4.	Chía	2
5.	Manizales	2
6.	Armenia	1
7.	Bucaramanga	1
8.	Cartago	1
9.	Dosquebradas	1
10.	Medellín	1
11.	Montería	1
12.	Pasto	1
13.	Sopó	1
14.	Yopal	1
	Total	**46**

El escáner con shodan arrojó como resultado 46 IP´s en 14 ciudades colombianas, las IP´s se pueden consultar en este enlace: https://github.com/sileramador/PoC/blob/main/ips-ciudad.txt

1.4.4 Prueba de acceso por diccionario

Se utilizó la herramienta Hydra para probar credenciales predeterminadas conocidas:

```
$hydra -l admin -P "$ARCHIVO_PASS" -e ns \
-s 8080 -o "$ARCHIVO_RESULTADOS" -vV \
-M "$ARCHIVO_IPS" http-get
```

Nota: el símbolo (\) representa que el comando continúa en la siguiente línea.
Resultado esperado: Identificar credenciales válidas (por ejemplo: admin:admin).

Tabla 3. Proporción de direcciones IP´s vulneradas por ciudades colombianas

Ciudades	Proporción de IP´s

1.	Bogotá	25/28
2.	Cúcuta	2/2
3.	Pereira	3/3
4.	Chía	1/2
5.	Manizales	2/2
6.	Armenia	1/1
7.	Bucaramanga	1/1
8.	Cartago	0/1
9.	Dosquebradas	1/1
10.	Medellín	1/1
11.	Montería	1/1
12.	Pasto	1/1
13.	Sopó	1/1
14.	Yopal	1/1
	Proporción Total	**41/46**

La prueba de credenciales predeterminadas conocidas arrojó como resultado 41 de 46 IP´s vulneradas en 14 ciudades colombianas, las IP´s se pueden consultar en: https://github.com/sileramador/PoC/blob/main/resultados_hydra-ciudad.txt.
Para automatizar todo el proceso de la PoC se realizó un script en python que se puede consultar en: https://github.com/sileramador/PoC.git.

2. Discusión

Los resultados obtenidos en esta investigación evidencian una vulnerabilidad crítica en la configuración de los cable-modems utilizados por la empresa ISP en Colombia, particularmente en el modelo Technicolor tc8305.e. A través de la prueba de concepto (PoC), se demostró la facilidad con la que un adversario puede obtener acceso con privilegios de administrador a estos dispositivos mediante ataques de fuerza bruta y diccionario, aprovechando credenciales predeterminadas. El impacto de esta vulnerabilidad es significativo, ya que permite a los atacantes modificar la configuración de DNS, interceptar datos y lanzar ataques masivos.

2.1 Análisis de resultados y comparación con estudios previos

Los hallazgos de esta investigación coinciden con estudios previos sobre vulnerabilidades en infraestructuras de telecomunicaciones. Por ejemplo, investigaciones recientes han demostrado que el uso de credenciales por defecto sigue siendo una de las principales debilidades en la seguridad de dispositivos ciberfísicos (Sheikh et al., 2022). Asimismo, la aplicación de la taxonomía TRACI ha permitido categorizar de manera estructurada las amenazas detectadas, lo que resalta la necesidad de una gestión de riesgos efectiva en las infraestructuras críticas (Plachkinova & Vo, 2023).
Al analizar los resultados obtenidos, se identificó que el 89.1% de los dispositivos escaneados en el estudio presentaban credenciales vulnerables. Esto sugiere una falta de implementación de controles de seguridad básicos por parte de los ISP, a

pesar de las advertencias y recomendaciones establecidas en estándares como la norma (IEC 62443-1-1, 2018) y la guía (NIST SP 800-82r2, 2011).

2.2 Implicaciones para la ciberseguridad en infraestructuras críticas

La vulnerabilidad analizada tiene implicaciones críticas para la seguridad de los CPS dentro de las infraestructuras de telecomunicaciones. Al comprometer estos dispositivos, los atacantes pueden realizar ataques de intercepción de datos y persistencia en la red, afectando la disponibilidad y confidencialidad de la información transmitida. Además, la capacidad de modificar la configuración de DNS introduce riesgos adicionales, ya que facilita el secuestro de sesiones y la redirección de los usuarios a sitios maliciosos (Amador Donado, Pardo Calvache, & Mazo Peña, 2024).

Desde la perspectiva de la ciberseguridad post-cuántica, estos hallazgos resaltan la urgencia de adoptar mecanismos de autenticación robustos y estrategias de mitigación para fortalecer la resiliencia de los CPS. Las soluciones propuestas en el modelo MoRCiTO enfatizan la necesidad de integrar criptografía resistente a la computación cuántica y la implementación de controles avanzados de seguridad en dispositivos críticos. Sin embargo, la aplicación de estas medidas enfrenta retos operacionales y financieros, lo que dificulta su adopción a gran escala en entornos industriales (Bernstein & Lange, 2017).

2.3 Limitaciones y direcciones futuras de investigación

A pesar de los hallazgos obtenidos, esta investigación presenta algunas limitaciones. Primero, el estudio se enfocó en un conjunto específico de cable-modems en un país determinado, por lo que los resultados podrían no ser generalizables a otras regiones o proveedores. Además, la PoC se realizó en un entorno real sin incluir escenarios en los que los ISP hayan aplicado medidas de mitigación adicionales.

Como futuras líneas de investigación, se recomienda:

- Analizar la efectividad de diferentes estrategias de mitigación en dispositivos ciber-físicos.
- Evaluar el impacto de las soluciones basadas en inteligencia artificial para la detección temprana de accesos no autorizados.
- Ampliar el estudio a otros modelos de cable-modems y dispositivos de telecomunicaciones en diferentes regiones geográficas.
- Investigar la viabilidad de aplicar criptografía post-cuántica en dispositivos IoT y CPS en infraestructuras críticas.

2.4 Recomendaciones para el sector de telecomunicaciones

Los resultados obtenidos muestran la necesidad urgente de los ISP para que implementen medidas más rigurosas y así proteger sus dispositivos de acceso a redes. Entre las principales recomendaciones se incluyen:

- Asignación de credenciales únicas por dispositivo, eliminando el uso de contraseñas predeterminadas.
- Obligatoriedad del cambio de credenciales en la configuración inicial por parte del usuario final.
- Deshabilitación de accesos remotos innecesarios y configuración segura de interfaces de administración.
- Implementación de autenticación multifactor (MFA) en la gestión remota de dispositivos.
- Monitoreo continuo y detección de accesos anómalos para prevenir ataques de fuerza bruta.
- Actualizaciones automáticas y seguras del firmware, con verificación de firmas digitales.

La aplicación de estas medidas contribuiría significativamente a reducir la exposición de dispositivos críticos a ciber-ataques, fortaleciendo la seguridad y resiliencia de las infraestructuras de telecomunicaciones.

3. Conclusiones y trabajos futuros

En esta investigación se ha demostrado una vulnerabilidad crítica en cable-modems de un ISP en Colombia, permitiendo a los adversarios obtener acceso con privilegios de administración mediante credenciales predeterminadas. A través de una PoC, se confirmó la viabilidad de explotar esta debilidad para modificar configuraciones de red, interceptar datos y establecer persistencia en el sistema.

El análisis mediante la taxonomía TRACI permitió categorizar la amenaza de manera estructurada, evidenciando riesgos en activos cibernéticos, gestión de riesgos y motivación de adversarios. Las recomendaciones propuestas incluyen medidas de seguridad críticas para mitigar esta vulnerabilidad, alineadas con el modelo MoRCiTO y los estándares internacionales de ciberseguridad.

A pesar de las limitaciones del estudio, los hallazgos refuerzan la necesidad de un enfoque proactivo en la seguridad de infraestructuras críticas de telecomunicaciones. Se recomienda continuar con investigaciones orientadas a la integración de criptografía post-cuántica y estrategias avanzadas de detección de amenazas para mejorar la protección de estos sistemas ante ataques emergentes.