UNIVERSIDAD AUTÓNOMA METROPOLITANA
Casa abierta al tiempo
DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

JDIE. 2025.1.01.03

Ciudad de México, a 14 de enero de 2025.

DR. ROMÁN LINARES ROMERO
PRESIDENTE DEL CONSEJO DIVISIONAL
DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA
P R E S E N T E

**Asunto:** Solicitud de Registro de Proyecto de Investigación.

Por este medio le solicito, atentamente, incluir en el orden del día de la próxima sesión del Consejo Divisional que usted, acertadamente, preside, el registro del Proyecto de Investigación

***SRIC: Evaluación e implementación de sistemas criptográficos para privacidad de la información en redes inalámbricas comunitarias***

cuyo responsable es el **DR. LEONARDO PALACIOS LUENGAS**, adscrito a este Departamento y, en particular, al **Área Académica de Redes y Telecomunicaciones**.

Le agradezco su atención y quedo a sus órdenes para cualquier duda o aclaración.

**A t e n t a m e n t e**
"Casa abierta al tiempo"

[redacted]

**M. en C. Omar Lucio Cabrera Jiménez**
**Jefe del Departamento de Ingeniería Eléctrica**

Casa abierta al tiempo
UNIVERSIDAD AUTÓNOMA METROPOLITANA
DIVISIÓN DE CIENCIAS BÁSICAS E INGENIERÍA
DEPARTAMENTO DE INGENIERÍA ELÉCTRICA

departamento de ingeniería eléctrica

# SRIC: Evaluación e implementación de sistemas criptográficos para privacidad de la información en redes inalámbricas comunitarias

***Fecha:*** *7 enero 2025*

**Palabras Clave:** Redes inalámbricas, seguridad de la información, OpenWRT, seguridad en redes de bajo costo, criptografía ligera.

## Responsable(s)

| Nombre | Tiempo de dedicación |
|---|---|
| Dr. Leonardo Palacios-Luengas, profesor de tiempo completo, RyT | 15 h |

## Participante(s)

| Nombre | Tiempo de dedicación |
|---|---|
| Dr. Ricardo Marcelín-Jiménez, profesor de tiempo completo, RyT | 15 h |
| Dr. Enrique Rodríguez-De-La-Colina, profesor de tiempo completo, RyT | 10 h |
| Dr. Michael Pascoe-Chalke, profesor de tiempo completo, RyT | 10 h |
| Ing. Mauricio López-Villaseñor, profesor de tiempo completo, RyT | 10 h |

## Área del responsable

**Área:** Redes y Telecomunicaciones
**Departamento:** Ingeniería Eléctrica

## Objetivo general

Evaluar esquemas de seguridad en sistemas criptográficos para la privacidad de datos, a través del diseño e implementación de soluciones específicas aplicadas a redes inalámbricas comunitarias de bajo costo, particularmente en donde no se tenga una infraestructura tecnológica.

## Objetivos particulares

- Analizar y revisar los requerimientos de seguridad de hardware y software de las redes inalámbricas de bajo costo.
- Evaluar los esquemas de cifrado asimétricos y simétricos ligeros para las redes inalámbricas de bajo costo.
- Proponer primitivas criptográficas ligeras para el desarrollo de un sistema criptográfico asimétrico y simétrico considerando requerimientos elementales como seguridad, rendimiento y costo.
- Diseñar e implementar un banco de pruebas con microcontroladores de gama baja, que permitan validar los algoritmos criptográficos que se desarrollen, así como probar su funcionamiento.
- Desarrollar y evaluar los sistemas criptográficos en la Intranet UAMI.

## Descripción del proyecto

Las redes inalámbricas comunitarias (RIC) son redes de telecomunicaciones implementadas y gestionadas por comunidades locales. Tienen un gran potencial para proporcionar una serie de beneficios a las comunidades, que incluyen: acceso a la Internet, reducción de la brecha digital, fortalecimiento de la comunidad, creación de oportunidades económicas, mejora de la seguridad pública, educación y salud a través de la telemedicina. Sin embargo, las RIC plantean una serie de desafíos, entre los que se incluyen la privacidad y la seguridad, debido a que las RIC son redes abiertas que utilizan el espectro radioeléctrico que es un recurso público. Esto significa que cualquier persona con un dispositivo compatible puede conectarse a una RIC [5].
La privacidad de los usuarios es una necesidad, debido a que los datos transmitidos a través de una RIC pueden ser interceptados por personas no autorizadas. Lo anterior puede incluir, información personal como números de teléfono, direcciones de correo electrónico, expedientes médicos, información sensible en general por mencionar solo algunos ejemplos. Por otro lado, la seguridad de la RIC podría estar comprometida por accesos de personas no autorizadas. Esto podría permitir a los atacantes acceder a los datos de la red o interrumpir su funcionamiento [6].

En la tabla 1, se muestra la taxonomía de diferentes amenazas a la que están expuestos los dispositivos inalámbricos, las cuales afectan la accesibilidad, integridad, identidad, disponibilidad, identificación y autenticación de la información.

Tabla 1. Taxonomía de las principales amenazas en las redes inalámbricas.

| Categoría | Amenaza | Breve descripción |
|---|---|---|
| Ataques | Programa malicioso | Programas de cómputo diseñados para realizar acciones no deseadas y no autorizadas de manera ilegal en un sistema. |
| | Denegación de servicio (DDoS) | Un conjunto de sistemas o equipos que atacan a un único objetivo para saturarlo. |
| | Falsificación de dispositivos | Cuando un dispositivo ajeno a la red se hace pasar por algún otro dentro de una red. |
| | Ataques de privacidad | Roba información de usuarios de manera ilegal. |
| | Modificación de información | Alterar la información generalmente para beneficios económicos. |
| Intercepción | Ataque de hombre en el medio | Es un ataque de intercepción, en donde el atacante se posiciona en medio de la comunicación entre dos víctimas, haciéndoles creer que están hablando directamente entre sí. |
| | Intercepción de información | Intercepción no autorizada de los datos. |
| | Secuestro de sesión | Robo de conexión de datos, donde el atacante actúa como un Host legítimo para robar o eliminar los datos. |
| | Obtención de información | Obtención pasiva de información sobre la red. |
| Caídas | Fallos de dispositivos | Amenaza de fallo del hardware. |
| | Fallo de sistema | Amenaza de fallo de los servicios o aplicaciones de software. |
| Daño | Filtrado de datos | Se revelan datos confidenciales de manera intencional. |
| Fallos | Vulnerabilidades de software | Los dispositivos IoT son vulnerables a causa de claves débiles, errores de software y errores de configuración. |
| Ataques físicos | Modificación de dispositivos | Manipulación de dispositivos utilizando sus puertos de comunicaciones abiertos. |

### Privacidad de los datos

La privacidad de los datos se basa en estrategias que se muestran en la Figura 1. Las técnicas de anonimización desde el punto de vista de seguridad no tienen interés criptográfico. Sin embargo, se pueden utilizar para otras necesidades como proteger base de datos o coordenadas de posicionamiento de un dispositivo. Con respecto a la criptografía asimétrica y simétrica se pueden utilizar juntas para proporcionar un alto nivel de seguridad en el cifrado de datos. La combinación de estos esquemas de cifrado se conoce como cifrado híbrido.

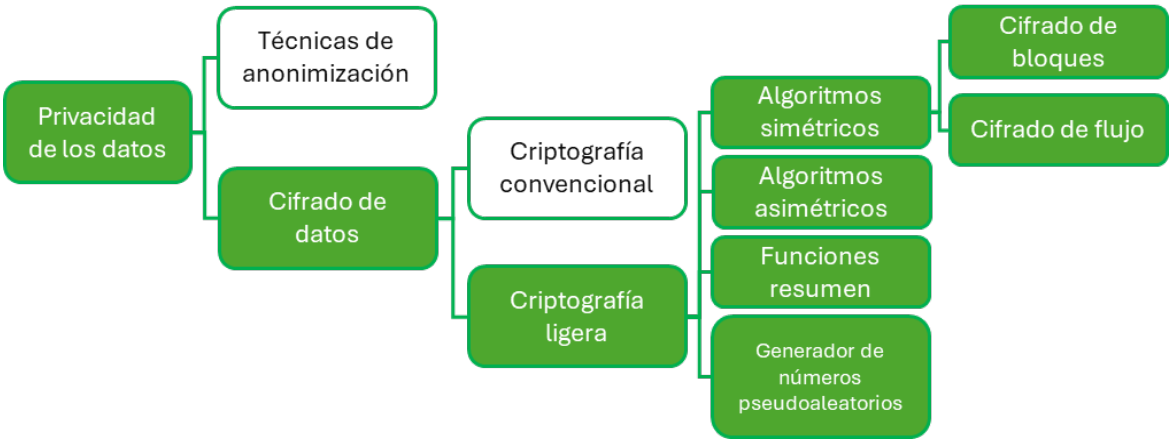


**Figura 1. Soluciones para la privacidad de datos en los dispositivos de baja gama.**

En la criptografía ligera se pueden aplicar diferentes mecanismos de seguridad en varias etapas de la red de comunicaciones. Con respecto a los dispositivos electrónicos, estos están experimentando un cambio significativo, ya que la mayoría de los fabricantes agregan una capa de seguridad para generar claves criptográficas, cifrado de datos y autenticación de claves [7]. Por ejemplo, la empresa “Secure Elements” realiza operaciones criptográficas en hardware, lo que permite que los algoritmos criptográficos se ejecuten de manera rápida y eficiente. Los elementos seguros también proporcionan una memoria a prueba de manipulaciones para almacenar datos criptográficos de forma segura [8]. Debido a que los microcontroladores comienzan a proporcionar operaciones criptográficas directamente en el hardware, el rendimiento de las primitivas criptográficas puede aumentar en muchos órdenes de magnitud, permitiendo que se ejecuten varias instancias del algoritmo de firma digital (DSA) de alto nivel de seguridad por segundo [9]. Por su parte ARM propone un mecanismo de hardware crítico que permite ejecuciones en un entorno de ejecución de confianza (TEE) en el que las aplicaciones esenciales pueden ejecutarse de forma segura [10].

## Sistemas de cifrado en las redes comunitarias actuales

El cifrado de datos es una parte fundamental en la seguridad de las redes comunitarias, protegiendo la privacidad e integridad de la información transmitida entre usuarios y dispositivos. A continuación, se describen algunos trabajos relevantes sobre el uso de sistemas de cifrado en redes comunitarias. Por ejemplo, el cifrado de extremo a extremo (E2EE), como la red Onion que Implementa un sistema de enrutamiento anónimo y cifrado E2EE para proteger la privacidad de la comunicación online. Con respecto a Briar ofrece una aplicación de mensajería segura y descentralizada que utiliza E2EE para proteger las comunicaciones [11]. Cifrado de punto a punto (P2P) a través de FireChat, el cual permite la comunicación offline entre dispositivos móviles cercanos mediante P2EE. Con respecto Meshnet se crea una red inalámbrica local autoorganizada y segura con cifrado P2P [12]. De igual manera existen protocolos de cifrado de la capa de transporte como el HTTPS, el cual es un protocolo estándar para la comunicación segura en la web, utilizando TLS/SSL para el cifrado [13]. Las VPNs permiten la conexión segura a redes privadas a través de Internet mediante túneles cifrados. Cifrado de datos almacenados utilizando VeraCrypt código abierto se usa para el cifrado de discos duros y archivos. En similar manera BoxCryptor es un servicio de cifrado en la nube que protege los archivos almacenados en plataformas como Dropbox o Google Drive [14]. En resumen, los sistemas de cifrado son una herramienta fundamental para garantizar la seguridad y privacidad en las redes comunitarias. La elección del sistema de cifrado adecuado dependerá de las necesidades específicas de la red, como el tipo de datos que se transmite, el nivel de seguridad requerido y la facilidad de uso. Es importante destacar que la investigación en el campo de los sistemas criptográficos para redes comunitarias continúa evolucionando, con el objetivo de desarrollar soluciones cada vez más seguras y eficientes.

## Caso de estudio

El sistema de privacidad de la información propuesto considera el siguiente esquema de funcionamiento similar al de las redes convencionales de comunicaciones. Una vez iniciada la conexión, y abierta la sesión, se considera el proceso para establecer el canal de comunicaciones seguro (Figura 2). Tanto el cliente (Cl) y el servidor (S) generan un par de claves denominada, clave pública (Kpu) y privada (Kpr), respectivamente. (1) realiza el intercambio de las claves públicas, tanto de Cl y S, (2) mediante un generador de números pseudoaleatorios se genera la clave de sesión (Ks). (3) A partir de un esquema de cifrado asimétrico se hace el cifrado de (Ks) para realizar el intercambio entre las dos entidades. (4) Entonces, el criptograma se envía por el canal de comunicaciones, por su parte el servidor descifra el criptograma. Cómo se puede observar en este punto, se realizó el intercambio de la Ks entre el Cl y S. (5) En este proceso de la comunicación, se puede utilizar criptografía simétrica para intercambiar la información, tanto

el Cl y S pueden enviar información cifrada y cada parte puede descifrar la información correspondiente. Recordemos que, el cifrado simétrico, cifra y descifra con la misma clave.

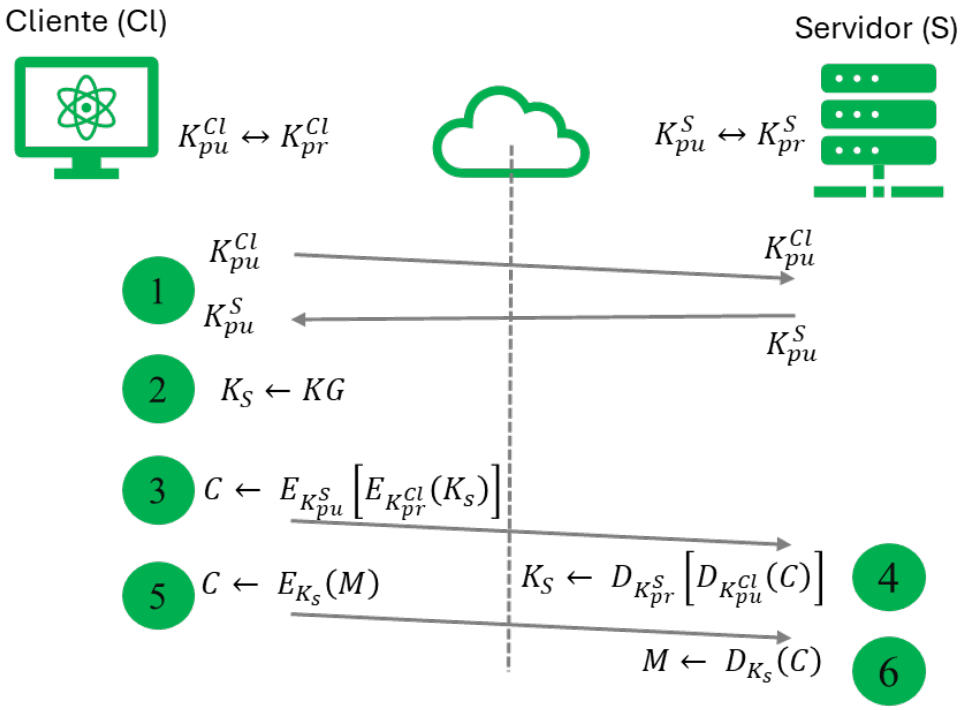


**Figura 2. Esquema de cifrado hibrido propuesto.**

El esquema de cifrado híbrido es considerado como la creación del canal seguro, donde inicialmente se debe compartir la una clave de sesión. La clave de sesión se debe generar a partir de un generador de número pseudoaleatorios que utiliza el sistema de cifrado simétrico.

**Pregunta de investigación**

**¿Qué primitivas criptográficas ligeras podrán proporcionar seguridad similar que las utilizadas en las redes convencionales?**

Para contestar esta pregunta tenemos que abordar las diferencias existentes entre la criptografía convencional y la criptografía ligera. Básicamente la diferencia entre estas dos criptografías es la precisión de la clave y las operaciones que se realizan [15]. En consecuencia, la criptografía convencional es más segura que la criptografía ligera debido a los tamaños de la clave. Sin embargo, de acuerdo con la tabla 1, en ambos esquemas criptográficos se tiene algunos

problemas similares de seguridad. Entonces, ¿cuáles son los problemas de los sistemas de cifrado ligero?

Al igual que los sistemas criptográficos desarrollados para la seguridad de las redes convencionales, la tecnología de bajo costo es un proceso en evolución pues se sigue explorando en los mecanismos de seguridad. La mayoría de los ataques se basan en huecos de seguridad de los esquemas criptográficos, no tanto en la vulnerabilidad de los esquemas de cifrado. Por ejemplo, en la tecnología LoRaWAN, un problema de software en la limitación del contador de 16 bits en "FRMPayload" podía ser explotada para interrumpir la comunicación en redes LoRaWAN mediante la técnica de reenvío de paquetes y colisiones. Es importante tener en cuenta que este ataque se aplicaba a la versión 1.0 de LoRaWAN y se han implementado mejoras en versiones posteriores para mitigar este tipo de vulnerabilidades [16]. Otros ataques de los sistemas de cifrado ligero, se basa en que la clave de sesión permanece fija hasta que se actualice el firmware o se cambian de manera manual [17]. De igual manera, algunos sistemas criptográficos utilizan claves débiles y predeterminadas, lo cual hace una vulnerabilidad sobre el esquema de cifrado [18].
De acuerdo con lo anterior, la propuesta de este trabajo de investigación es pertinente, y conlleva la evaluación de los sistemas de cifrado simétricos y asimétricos. También, se deben considerar las siguientes acciones:

- Mejorar la seguridad del sistema de cifrado simétrico en una RIC, para ello se pueden utilizar algoritmos de cifrado robustos, los cuales son más difíciles de descifrar por ataques de fuerza bruta. Algunos ejemplos de algoritmos de cifrado robustos son AES-256 y ChaCha20 [19].
- Utilizar claves de longitud larga debido a que son más difíciles de descifrar por ataques de fuerza bruta. Se recomienda utilizar claves de al menos 256 bits.
- Implementar técnicas de autenticación, las cuales pueden ayudar a verificar la identidad de las partes que se comunican.
- Con respecto al cifrado asimétrico se pueden utilizar cifrado robustos ya que son más difíciles de descifrar por ataques de fuerza bruta. Algunos ejemplos de algoritmos de cifrado robustos son CCE y ECDSA [20].
- Utilizar claves de longitud larga de al menos 2048 bits. Además, utilizar firmas digitales para ayudar a verificar la integridad de los datos.
- También se deben implementar protocolos de seguridad robustos, los cuales incluyen medidas para proteger contra ataques comunes, como ataques de fuerza bruta, ataques de análisis de tráfico y ataques de intermediario.
- Mantener los dispositivos actualizados y educar a los usuarios sobre la Ciberseguridad. Esto puede ayudar a prevenir ataques causados por errores humanos.

En conclusión, existen una serie de técnicas que se pueden utilizar para mejorar la seguridad de los sistemas de cifrado simétricos y asimétricos en las RIC. Con base a lo descrito anteriormente, nuestra propuesta es interesante y pertinente debido a que las principales vulnerabilidades de los esquemas criptográficos se basan principalmente por defectos de diseño e implementación, entonces es importante considerar una serie de factores. En este contexto se proponen las siguientes preguntas de investigación:

1. ¿Puede un sistema criptográfico ligero adecuarse a las necesidades de seguridad de las redes inalámbricas comunitarias?
2. ¿Teniendo en cuenta la arquitectura de la red será posible implementar un sistema criptográfico especifico a las necesidades de la red para tener un entorno seguro de los datos?
3. ¿Implementando los controles de seguridad en la RIC se pueden remediar los huecos de seguridad que se reportan en las redes IoT?

**Metas**

1. Realizar un análisis de los esquemas de cifrado usados en IoT que sean criptográficamente seguros de manera teórica para identificar la fortaleza de tales esquemas.
2. Revisar el protocolo de comunicación desarrollado en RIC, específicamente de la Intranet de la UAMI para conocer las posibles vulnerabilidades.
3. Proponer un banco de pruebas que permita evaluar los sistemas criptográficos y la red de comunicaciones para detectar posibles huecos de seguridad.
4. Implementar el esquema de cifrado hibrido en la Intranet UAMI, que permita validar los puntos anteriores.
5. Obtener el rendimiento de los sistemas de cifrado que se implementen en la RIC.
6. Establecer las métricas de evaluación a partir de pruebas estadísticas de Organismos internacionales sobre los criptogramas generados.
7. Publicación de los resultados en foros, revistas o congresos.

**Metodología**

- Para alcanzar los objetivos planteados se seguirán pasos del método científico. Además, se hará una comparación de diversas soluciones y planteamientos para su análisis, así como la selección de metodologías adecuadas basadas en la experimentación.
- Investigación: Buscará documentar la información necesaria para conocer el “Estado de la técnica”.
- Descriptivo: Permitirá detallar cada una de las características de las variables de interés.

- Analítico: Identificar y definir la influencia de cada una de las variables de interés en el sistema.
- Predictivo: buscará aplicar soluciones de otras situaciones al contexto de interés, y finalmente.
- Experimental: permitirá la realización de pruebas de comprobación y validez a los desarrollos y análisis efectuados.

**Actividades de los participantes**

Tabla 2. Participantes, actividades y tiempo de dedicación.

| Participantes | Actividad | Tiempo dedicación (h/s) |
|---|---|---|
| Dr. Leonardo PALACIOS-LUENGAS | Análisis y desarrollo de las primitivas criptográficas ligeras para los esquemas simétricos y asimétricos. | 15 |
| Dr. Ricardo MARCELÍN-JIMÉNEZ | Optimización de las primitivas criptográficas desarrolladas para su implementación en software. | 15 |
| Dr. Enrique RODRÍGUEZ-DE LA COLINA | Desarrollo y análisis de las pruebas estadísticas de los sistemas criptográficos desarrollados. | 10 |
| Dr. Michael PASCOE-CHALKE | Revisión de las necesidades técnicas para integración de los sistemas criptográficos en la red comunitaria, validar configuraciones y lo necesario para su funcionamiento. | 10 |
| Ing. Mauricio LÓPEZ-VILLASEÑOR | Validar las implementaciones de los esquemas criptográficos desarrollados a partir de un banco de pruebas, los cuales deben generar reportes y validar el funcionamiento con base a normas o buenas prácticas de seguridad. | 10 |

**Recursos disponibles para el desarrollo del proyecto**

Se cuenta con sistemas de cómputo de uso común del área académica de redes y telecomunicaciones (RyT). De igual manera, se cuenta con una Intranet UAMI para realizar pruebas y se cuenta con paquetes computacionales de uso libre.

**Fuentes de financiamiento**

Se buscará dentro de la ejecución de esta línea de investigación la continuidad de proyectos buscando patrocinadores externos. Por ejemplo, fondos LANIC-FRIDA y el CONAHCyT. Cabe destacar que la Intranet comunitaria fue beneficiada con fondos LANIC-Frida hace dos años.

**Infraestructura necesaria y disponible**

Se cuenta con los laboratorios del área de RyT que se encuentran ubicados en el Edificio T, 3er piso. Un cubículo de trabajo que cuente con una estación de trabajo (impresora y computadora con herramientas de simulación), así como el acceso a la base de datos de revistas indexadas de Bindani.

**Pertinencia de la propuesta**

Las redes inalámbricas comunitarias (RIC) son una alternativa para comunicar a poblaciones no atendidas o precariamente atendidas, inclusive en zonas rurales y/o urbanas que no cuenten con los recursos para aprovechar los beneficios de acceso a la Internet. Sin embargo, las RIC son vulnerables a una cantidad de ataques que pueden poner en riesgo la privacidad y la seguridad de los usuarios.
En la actualidad existen los siguientes problemas más comunes en las redes inalámbricas comunitarias, las cuales incluyen. Los ataques de escuchas en la red, inyección de paquetes, denegación de servicio. Debido a esta problemática, se propone un mecanismo de privacidad de los datos, a partir del cifrado de información. Esta propuesta ayudara a expandir las fronteras del conocimiento, teniendo un impacto en el desempeño de las redes de comunicación, ayudando a preservar la seguridad de los datos, mejorando la calidad de servicio para el usuario. Cabe destacar que durante el desarrollo de este proyecto se promoverá la colaboración con otros investigadores interesados en el tema. De igual manera, se buscará impulsar la generación de recursos humanos a través de estudiantes de licenciatura, maestría, doctorado y/o posdoctorado. Con el desarrollo del proyecto se busca la creación de una línea de investigación para contribuir al acceso universal del conocimiento.

**Cronograma de actividades**

La tabla 3 muestra el cronograma de actividades del proyecto, el cual está diseñado para desarrollarse en tres años. Durante el primer año se establecen los requerimientos del proyecto, en el segundo año el desarrollo del mismo, así como una publicación de los resultados obtenidos; mientras que durante el tercer año se tendrá otra publicación, así como la documentación necesaria para generar material didáctico referente al tema de seguridad. Siguiendo este cronograma, en noviembre del 2024 se entregó el informe de avances del primer año. Cabe mencionar que este proyecto fue sometido y aprobado en la convocatoria “Apoyo institucional al personal académico de recién ingreso 2024 “. Las actividades propuestas para los dos primeros

años se apegan a la convocatoria mencionada, mientras que el tercer año se establece para reforzar la línea de investigación que se propone permitiendo su evaluación y adecuación para darle continuidad.

Tabla 3. Cronograma de actividades.

| Resumen de actividades | 1er año | | | | | | | | | | | | 2do año | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | E | F | M | A | Ma | J | Ju | A | S | O | N | D | E | F | M | A | Ma | J | Ju | A | S | O | N | D |
| Analizar y revisar los requerimientos de seguridad de hardware y software de las redes inalámbricas de bajo costo. | | | | | | | | | | | | | | | | | | | | | | | | |
| Evaluar los esquemas de cifrado asimétricos y simétricos ligeros para las redes inalámbricas de bajo costo. | | | | | | | | | | | | | | | | | | | | | | | | |
| Proponer primitivas criptográficas existentes para el desarrollo del sistema criptográfico asimétrico y simétrico considerando la seguridad, rendimiento, costo y sus características de implementación. | | | | | | | | | | | | | | | | | | | | | | | | |
| Diseñar e implementar un banco de pruebas con microcontroladores de gama baja, que permita validar los algoritmos criptográficos que se implementen, así como de su funcionamiento. | | | | | | | | | | | | | | | | | | | | | | | | |
| Implementar los sistemas criptográficos en las redes comunitarias desarrollada en la UAMI. | | | | | | | | | | | | | | | | | | | | | | | | |
| Validar el sistema criptográfico en la red inalámbrica de prueba que se tiene en la UAMI. | | | | | | | | | | | | | | | | | | | | | | | | |
| Publicación de los resultados a través de foros de investigación, revistas o congresos. | | | | | | | | | | | | | | | | | | | | | | | | |

| Resumen de actividades | 3er año | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | E | F | M | A | Ma | J | Ju | A | S | O | N | D |
| Publicación de los resultados a través de foros de investigación, revistas o congresos. | | | | | | | | | | | | |
| Desarrollos tecnológicos para apoyo a docencia (Esquema de cifrado y conjunto de pruebas para evaluar su desempeño en una red inalámbrica | | | | | | | | | | | | |

**Propuesta económica**

| Recurso | Descripción | Cantidad | Costo unitario | Costo total |
|---|---|---|---|---|
| Raspberry Pi-5 8gb de RAM | Dispositivo de pruebas para la red, antes de integrarse a la Intranet. | 3 | $2,500.00 | $7,500.00 |
| Publicaciones | Publicación de los resultados en revista de alto impacto de acceso libre. | 1 | $50,000.00 | $50,000.00 |
| Viáticos | Pago de hospedaje, alimentación y pasajes, para asistencia a congreso o eventos para difusión. | 4 | $5,000.00 | $20,000.00 |
| USRP N200 | Equipo para pruebas de la red (sistemas de radio definidos por software). | 1 | $60,000.00 | $50,000.00 |
| LimeSDR | Módulos RF An SDR in a Mini PCIe form factor with an AMD Artix 7 XC7A50T-2CPG236I FPGA. | 1 | $20,000.00 | $20,000.00 |
| Accesorios | Antenas, filtro y módulo amplificador. | 1 | $2,500.00 | $2,500.00 |
| | | | Total | $150,000.00 |

## Indicadores de desempeño 2024-2026

La siguiente tabla muestra los resultados esperados para el trienio 2024-2026

| Componente | Productos de trabajo | Cantidad |
|---|---|---|
| Investigación | Artículos en revistas indizadas | 1 |
| | Artículos en memorias in extenso | 1 |
| | Presentaciones en congresos | 1 |
| | Capítulos de libro | 0 |
| | Artículos de divulgación | 1 |
| Docencia | Alumnos de licenciatura | 2 |
| | Alumnos de posgrado | 1 |
| | Desarrollos tecnológicos para apoyo a docencia (Esquema de cifrado y conjunto de pruebas para evaluar su desempeño en una red inalámbrica | 1 |

## Duración o vigencia del proyecto

Tres años

## Resumen de cambios

En la sección “cronograma de actividades” se establecen las actividades a realizar durante los tres años del proyecto. Se hace referencia el proyecto aprobado en la convocatoria “Apoyo institucional al personal académico de recién ingreso 2024”.

## Bibliografía

[1] Moisés Reyes Bernabé, “Diseño de enlaces para una red inalámbrica comunitaria,” Licenciatura, Universidad Autónoma Metropolitana, México, 2014.

[2] G. A. Z. R. Kenia López Salazar, “Diseño y logística de instalación de una red inalámbrica comunitaria,” Licenciatura, Universidad Autónoma Metropolitana, unidad Iztapalapa, México, 2014.

[3] D.-T. Dam, T.-H. Tran, V.-P. Hoang, C.-K. Pham, and T.-T. Hoang, "A Survey of Post-Quantum Cryptography: Start of a New Race," *Cryptography*, vol. 7, no. 3, p. 40, Aug. 2023, doi: 10.3390/cryptography7030040.

[4] L. Ning, Y. Ali, H. Ke, S. Nazir, and Z. Huanli, "A Hybrid MCDM Approach of Selecting Lightweight Cryptographic Cipher Based on ISO and NIST Lightweight Cryptography Security Requirements for Internet of Health Things," *IEEE Access*, vol. 8, pp. 220165–220187, 2020, doi: 10.1109/ACCESS.2020.3041327.

[5] D. Christin, M. Hollick, and M. Manulis, "Security and Privacy Objectives for Sensing Applications in Wireless Community Networks," in *2010 Proceedings of 19th International Conference on Computer Communications and Networks*, IEEE, Aug. 2010, pp. 1–6. doi: 10.1109/ICCCN.2010.5560129.

[6] A. Majeed, S. Khan, and S. O. Hwang, "A Comprehensive Analysis of Privacy-Preserving Solutions Developed for Online Social Networks," *Electronics (Basel)*, vol. 11, no. 13, p. 1931, Jun. 2022, doi: 10.3390/electronics11131931.

[7] A. Belous and V. Saladukha, *Viruses, Hardware and Software Trojans*. Cham: Springer International Publishing, 2020. doi: 10.1007/978-3-030-47218-4.

[8] J. Jung, B. Kim, J. Cho, and B. Lee, "A Secure Platform Model Based on ARM Platform Security Architecture for IoT Devices," *IEEE Internet Things J*, vol. 9, no. 7, pp. 5548–5560, Apr. 2022, doi: 10.1109/JIOT.2021.3109299.

[9] S. R. Niya, E. Schiller, I. Cepilov, and B. Stiller, "BIIT: Standardization of Blockchain-based I $^{2}$ oT Systems in the I4 Era," in *NOMS 2020 - 2020 IEEE/IFIP Network Operations and Management Symposium*, IEEE, Apr. 2020, pp. 1–9. doi: 10.1109/NOMS47738.2020.9110379.

[10] R. Stajnrod, R. Ben Yehuda, and N. J. Zaidenberg, "Attacking TrustZone on devices lacking memory protection," *Journal of Computer Virology and Hacking Techniques*, vol. 18, no. 3, pp. 259–269, Sep. 2022, doi: 10.1007/s11416-021-00413-y.

[11] C. Gupta, "The Market's Law of Privacy: Case Studies in Privacy and Security Adoption," *IEEE Secur Priv*, vol. 15, no. 3, pp. 78–83, 2017, doi: 10.1109/MSP.2017.57.

[12] S. Shukla *et al.*, "Network analysis in a peer-to-peer energy trading model using blockchain and machine learning," *Comput Stand Interfaces*, vol. 88, p. 103799, Mar. 2024, doi: 10.1016/j.csi.2023.103799.

[13] M. J. A. Baig, M. T. Iqbal, M. Jamil, and J. Khan, "Blockchain-Based Peer-to-Peer Energy Trading System Using Open-Source Angular Framework and Hypertext Transfer Protocol," *Electronics (Basel)*, vol. 12, no. 2, p. 287, Jan. 2023, doi: 10.3390/electronics12020287.

[14] M. Bhattacharya, S. Roy, S. Chattopadhyay, A. K. Das, and S. Shetty, "A comprehensive survey on online social networks security and privacy issues: Threats, machine learning-based solutions, and open challenges," *SECURITY AND PRIVACY*, vol. 6, no. 1, Jan. 2023, doi: 10.1002/spy2.275.

[15] M. Rana, Q. Mamun, and R. Islam, "Lightweight cryptography in IoT networks: A survey," *Future Generation Computer Systems*, vol. 129, pp. 77–89, Apr. 2022, doi: 10.1016/j.future.2021.11.011.

[16] H. Noura, T. Hatoum, O. Salman, J.-P. Yaacoub, and A. Chehab, "LoRaWAN security survey: Issues, threats and possible mitigation techniques," *Internet of Things*, vol. 12, p. 100303, Dec. 2020, doi: 10.1016/j.iot.2020.100303.

[17] F. L. Coman, K. M. Malarski, M. N. Petersen, and S. Ruepp, "Security Issues in Internet of Things: Vulnerability Analysis of LoRaWAN, Sigfox and NB-IoT," in *2019 Global IoT Summit (GIoTS)*, IEEE, Jun. 2019, pp. 1–6. doi: 10.1109/GIOTS.2019.8766430.

[18] R. Fujdiak *et al.*, "Security in low-power wide-area networks: state-of-the-art and development toward the 5G," in *LPWAN Technologies for IoT and M2M Applications*, Elsevier, 2020, pp. 373–396. doi: 10.1016/B978-0-12-818880-4.00018-1.

[19] W. Cai, H. Chen, Z. Wang, and X. Zhang, "Implementation and optimization of ChaCha20 stream cipher on sunway taihuLight supercomputer," *Journal of Supercomputing*, vol. 78, no. 3, 2022, doi: 10.1007/s11227-021-04023-9.

[20] K. N. Devika and R. Bhakthavatchalu, "Efficient hardware prototype of ECDSA modules for blockchain applications," *Telkomnika (Telecommunication Computing Electronics and Control)*, vol. 19, no. 5, 2021, doi: 10.12928/TELKOMNIKA.v19i5.19416.