Chimalli: Servicio de acceso seguro a servicios de e-salud y/o sistemas de analítica.

Entregable **2.1**
Proyecto **41756**

Responsable técnico:
Dr. José Luis González Compeán
Profesor-Investigador, Cinvestav Tamaulipas

Muyal-Ilal:
Plataforma tecnológica para la gestión, aseguramiento, intercambio y preservación de grandes volúmenes de datos en salud y construcción de un repositorio nacional de servicios de análisis de datos de salud.

Muyal-Ilal

1. Resumen Ejecutivo

El presente reporte describe el entregable 2.1 del Proyecto Número 41756 llamado Chimalli[1]: servicio de acceso seguro a servicios de e-salud y/o sistemas de analítica. Este servicio permite a las dependencias de salud pública asegurar que los sistemas de e-salud cumplan los requerimientos no funcionales de las normas nacionales (NOM-024-SSA3-2010 y NOM-004-SSA3-2012) e internacionales (NIST, ISO 27001:2013 y COBIT5) durante el intercambio, tratamiento/análisis de datos sensibles y protección de datos privados. Chimalli garantiza los siguientes requerimientos no funcionales:

- **Seguridad:** Garantiza privacidad, confidencialidad e integridad de datos y establece controles de acceso automáticamente. Además, verifica y crea reportes del grado de cumplimiento de las normas.
- **Confiabilidad y disponibilidad:** Garantiza acceso a datos y sistemas en escenarios de fallas de servidores, almacenamiento, así como apagones en los centros de datos. Chimalli permite configurar los servicios de confiabilidad y disponibilidad dependiendo de los recursos disponibles.
- **Trazabilidad:** Crea automáticamente redes de blockchain para auditoría continua durante el intercambio de datos. Chimalli elimina los costos derivados de contratar un servicio de blockchain con terceros (e.g., 3,400 dólares por uso red por 4 meses en la nube).
- **Eficiencia:** Chimalli maneja los datos hasta 10 veces más rápido que opciones disponibles en mercado, reduce 34% costos de utilización de la nube y 70% de costos de almacenamiento. Además, Chimalli permite compartir sistemas con otras instituciones en minutos y de forma segura.

En este reporte también se presentan los contenidos desarrollados con propósito de difusión, así como la documentación técnico-científica de los productos conseguidos por Chimalli en el contexto del proyecto ProNacEs Número 41756, los cuales se enlistan a continuación

Comprometidos en CAR

- Servicios de preparación y recuperación de datos médicos configurables que incluya los requerimientos de seguridad, trazabilidad, integridad y eficiencia.
- Mecanismos de trazabilidad de datos basados en blockchain.
- Mecanismos de control de acceso de usuarios.
- Servicios de validación de normas oficiales mexicanas y protocolos DICOM/HL7.
- Servicio que permita la utilización de técnicas de criptografía de siguiente generación para la transformación de datos en objetos seguros.
- Un sistema de verificación del cumplimiento de las normas y protocolos oficiales.
- Esquemas de preparación/recuperación de datos para cumplir y verificar cumplimiento de requerimientos no establecidos en normas nacionales e internacionales **sobre tratamiento de datos sensibles/personales.**
- **Esquemas de preparación de datos para** el cifrado e intercambio seguro de datos y búsqueda de datos cifrados.

1.1. Productos científicos

La Figura 1 muestra el resumen de los productos de Chimalli. En él se encuentran el estado de cada uno de los productos (comprometido y no comprometido, así como un resumen de su estado).

Entregable	ID	Producto	Estado					Etapa		Comprometido	NMT
			Diseño	En desarrollo	En Evaluación	Prototipado	En Producción	1	2		
Zamná	Muyal-Chimalli-P1	Servicios de preparación y recuperación de datos médicos configurables que incluya los requerimientos de seguridad, trazabilidad, integridad y eficiencia.	*	*	*	✲		✓		Si	5
	Muyal-Chimalli-P2	Mecanismos de trazabilidad de datos basados en blockchain.	*	*	*	✲		✓		Si	4
	Muyal-Chimalli-P3	Mecanismos de control de acceso de usuarios.	*	*	*	✲		✓		Si	6
	Muyal-Chimalli-P4	Servicios de validación de normas oficiales mexicanas y protocolos DICOM/HL7.	*	*		✲		✓		Si	4
	Muyal-Chimalli-P5	Servicio que permita la utilización de técnicas de criptografía de siguiente generación para la transformación de datos en objetos seguros.	*	*	*	✲		✓		Si	5
	Muyal-Chimalli-P6	Un sistema que permita cumplimentar con las normas y protocolos oficiales.	*	*		✲			✓	No	4
	Muyal-Chimalli-P7	Esquemas de preparación y recuperación de datos que permitan cumplir con los requerimientos no funcionales establecidos en las normas.	*	*	*	✲			✓	No	5
	Muyal-Chimalli-P8	Esquemas de preparación de datos para el cifrado e intercambio seguro de datos.	*	*	*	✲			✓	No	5
	Muyal-Chimalli-P9	Esquema de búsqueda de datos cifrados en la nube	*	*		✲		✓		No	5

Simbología	
*	Terminado
X	En proceso
NMT	Nivel de Madurez Tecnológica

Figura 1 Resumen de los productos de Chimalli.

[1] Nombre náhuatl **Chimalli: Escudo**

1.2. Productos académicos[2]:

A continuación, se listan los productos académicos resultantes durante la primera etapa del proyecto:

- Artículos de investigación:
  - Carrizales-Espinoza, D., Gonzalez-Compean, J. L., & Morales-Sandoval, M. (2022, August). Zamna: a tool for the secure and reliable storage, sharing, and usage of large data sets in data science applications. In 2022 IEEE Mexican International Conference on Computer Science (ENC) (pp. 1-8). IEEE.
    - https://repositorio-salud.conacyt.mx/jspui/handle/1000/266
    - https://1drv.ms/b/s!AtMgnjYpElvzg4x9_4LDRn2up3_etg?e=ZUhE53
  - Carrizales-Espinoza, D., Sanchez-Gallegos, D. D., Gonzalez-Compean, J. L., & Carretero, J. (2022). FedFlow: A federated platform to build secure sharing and synchronization services for health dataflows. Computing, 1-19.
    - https://repositorio-salud.conacyt.mx/jspui/handle/1000/268
    - https://1drv.ms/b/s!AtMgnjYpElvzg40ERxR0jtjMzXgk0A?e=OKcGRO
- Reportes:
  - Reporte Técnico de Muyal-Chimalli
    - https://repositorio-salud.conacyt.mx/jspui/handle/1000/275
    - https://1drv.ms/b/s!AtMgnjYpElvzg457qxfavIer5nv2eQ?e=GuHJ9g
  - Reporte Técnico del Trazabilidad
    - https://1drv.ms/u/s!AtMgnjYpElvzg5YPOW6iVI7oBR4eBQ?e=qhFNJ9
  - Reporte Técnico del Servicio de Validación
    - https://1drv.ms/b/s!AtMgnjYpElvzg5Aq7h6tuZLffcfhAg?e=IhtkH6
- Infografías:
  - Infografía técnica y de público general
    - https://1drv.ms/u/s!AtMgnjYpElvzg5AwxpdAw7EnNgxGeQ?e=yrcy7z
- Posters de divulgación:
  - Poster cualitativo y cuantitativo de Chimalli
    - https://1drv.ms/u/s!AtMgnjYpElvzg5YQR6QXGO9pjPTZLg?e=rkD2Sk
  - Poster de Blockchain
    - https://1drv.ms/b/s!AtMgnjYpElvzg5YR_zqbSiD53oPLoA?e=LamNgU
- Tesis de Maestría:
  - Método de construcción de servicios de seguridad informática para sistemas de continuidad en infraestructuras heterogéneas de cómputo. Catherine A. Torres-Charles, J. L. Gonzalez-Compeán, and Miguel Morales-Sandoval. 2021-2022.
    - https://repositorio-salud.conacyt.mx/jspui/handle/1000/122
    - https://1drv.ms/b/s!AtMgnjYpElvzg40MU0yUFWbzDJ1DPA?e=pBJxHb

2. Servicio de acceso seguro a servicios de e-salud y/o sistemas de analítica.

Chimalli es una herramienta computacional compuesta por un conjunto de servicios para el acceso, manejo, preparación y entrega de datos médicos en formato digital, de forma segura, fiable, y confiable. Los servicios que conforman a Chimalli hacen factible que las instituciones de salud, profesionales de la salud, pacientes y/o comunidad científica pueda acceder a servicios de e-salud y/o sistemas de analítica para obtener información útil, sin comprometer la seguridad de los datos, que ayude a mejorar la toma de decisiones en escenarios de cuidado de la salud. Chimalli permite alcanzar un 70% de las regulaciones estandarizadas en forma internacional para el manejo seguro de datos sensibles, y cubre todas las fases de interconexión establecidas por las normas oficiales tales como NOM-024-SSA3-2010 y NOM-004-SSA3-2012; así como por los protocolos DICOM/HL7. Durante los procesos de acceso, uso y almacenamiento de datos, Chimalli garantiza los servicios de seguridad de confiabilidad, integridad, autenticación y control de acceso, además de que sus servicios se han diseñado para ser eficientes y seguros. Con ello, Chimalli asegura el anonimato de los datos, así como la confidencialidad mediante el cifrado de los datos entrantes y salientes de los sistemas de e-Salud. Además, permite detectar alteraciones en los datos. Lo anterior, se consigue mediante esquemas de criptografía de siguiente generación, lo que permite el manejo de datos como objetos seguros. Los requerimientos de seguridad, fiabilidad, eficiencia y de trazabilidad de Chimalli se encuentran encapsulados en esquemas de preparación y de recuperación de datos. Mediante un servicio de blockchain, Chimalli permite validar y registrar cualquier operación de compartición de datos que se realice dentro del sistema de e-salud. Esto lo consigue mediante la gestión automática de contratos inteligentes, la gestión automática de transacciones y la verificabilidad de transacciones de forma confidencial.

[2] Para acceder a la carpeta compartida Chimalli, da clic aquí

2.1. Servicios de preparación y recuperación de datos médicos configurables que incluya los requerimientos de seguridad, trazabilidad, integridad y eficiencia.

En los procesos de preparación de datos para escenarios reales de gestión de datos, diferentes requerimientos no funcionales (RNFs) (por ejemplo, seguridad, eficiencia, y confiabilidad) deben ser considerados debido a las normas de gestión de la salud (por ejemplo, las normas oficiales mexicanas NOM-024-SSA3-2010 y NOM-004-SSA3-2012) y las leyes impuestas por los gobiernos y organizaciones, La Figura 2 muestra un ejemplo del DAG de un esquema de preparación. Este DAG tiene cuatro etapas (compresión, deduplicación, codificación y cifrado) para añadir RNFs tales como confiabilidad, seguridad, integridad y costo-eficiencia.

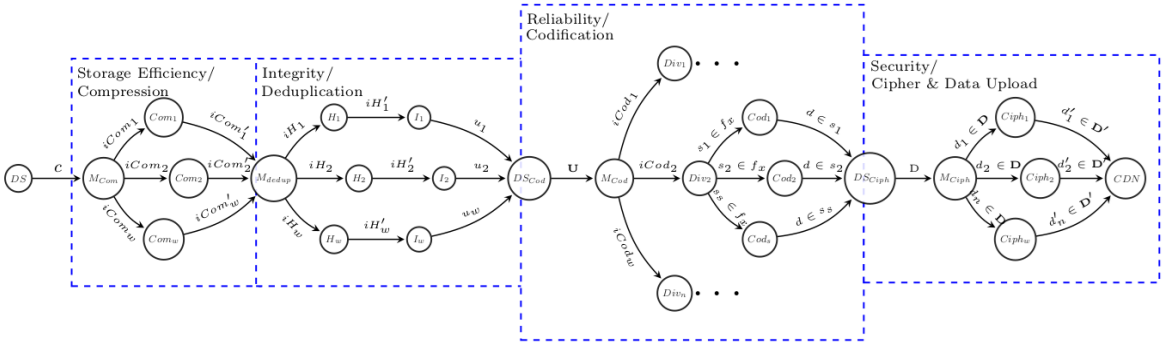

Figura 2. Esquemas de preparación de datos modelados como un DAG.

2.2. Mecanismos de trazabilidad de datos basados en blockchain.

El servicio de trazabilidad y verificabilidad de contenidos médicos tiene el objetivo de asegurar el registro inmutable de cada una de las acciones que se realicen sobre cada uno de los activos digitales que son procesados en las diferentes cadenas de valor generadas a través del servicio de construcción de servicios de e-Salud. La Figura 3 muestra la interacción entre ambos servicios.

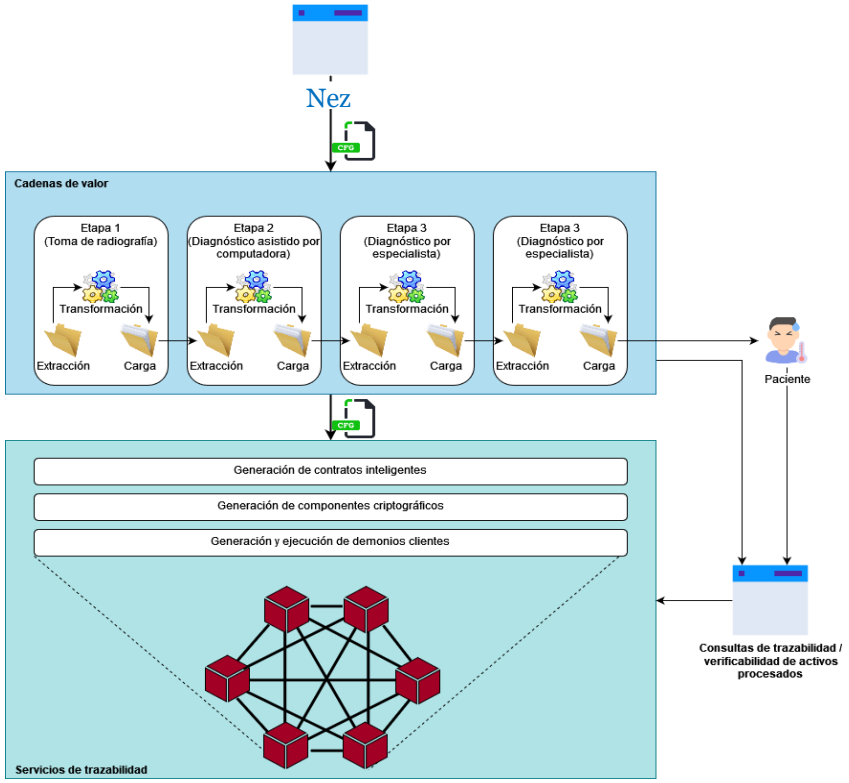

Figura 3. Diseño conceptual e interacción

Por otro lado, la Figura 4. muestra el diseño del servicio de validación. Como se puede observar, el servicio cuenta con los siguientes módulos:

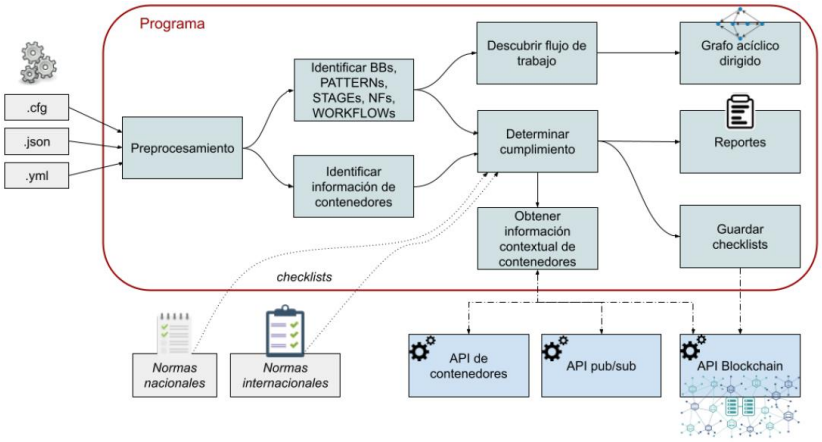

Figura 4. Representación conceptual del servicio de validación.

2.3. Servicio que permita la utilización de técnicas de criptografía de siguiente generación para la transformación de datos en objetos seguros.

La *primera fase* comprende la definición de los participantes autorizados para acceder a los datos, así como la secuencia válida de interacciones esperadas al compartir e intercambiar datos. Como resultado de esta fase, se crea un esquema de gestión de la información que describe un flujo de trabajo organizacional. Un ejemplo de tal esquema se muestra en la Figura 5.

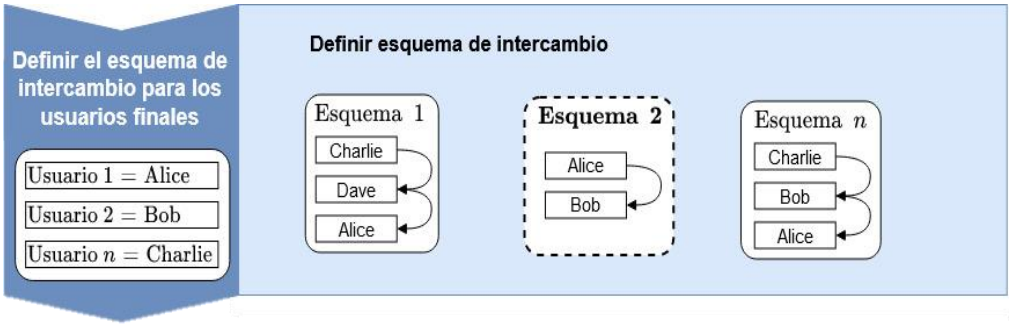

Figura 5. Fase 1 para la creación de servicios de intercambio de información eficientes y seguros.

En la segunda fase, los diseñadores pueden elegir bloques de seguridad para un cripto-contenedor entre los bloques disponibles en el repositorio de servicios de seguridad. Los bloques elegidos están organizados en forma de patrón.
En este sentido, existen dos tipos de patrones disponibles: i) **Pipelines paralelos** (vea **PFP** en la Figura 6) o **Pipelines Overlapped** (vea **Overlapped** en la Figura 6). Cuando los usuarios finales lanzan un cripto-contenedor, los criptosistemas elegidos por ellos siguen el patrón asignado al cripto-contenedor.

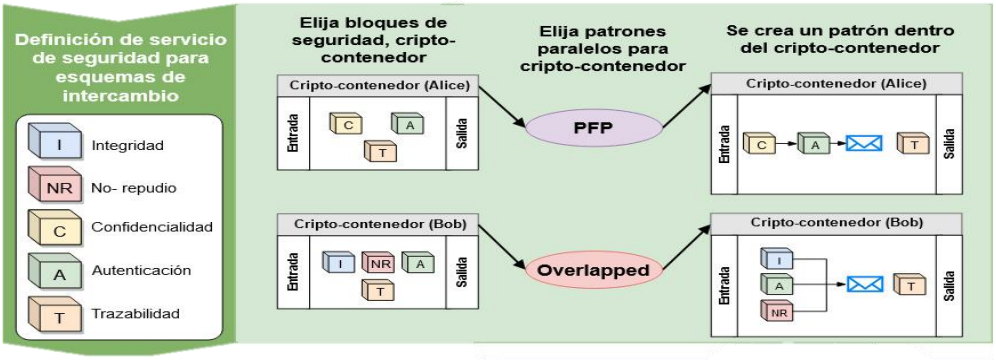

Figura 6. Fase 2 para la creación de servicios de intercambio de información eficientes y seguros.

En la *tercera fase* (ver Figura 7), los parámetros de nivel de seguridad y eficiencia son agregados al cripto-contenedor creado en la fase anterior. El parámetro de seguridad indica la resistencia de la seguridad (por ejemplo, la longitud de la clave criptográfica). El parámetro de eficiencia viene dado por el número de trabajadores utilizados por el patrón de ese cripto-contenedor. Este parámetro determina la cantidad de tuberías que se ejecutarán de manera concurrente.
Para crear un flujo de trabajo, se crea un cripto-contenedor para cada etapa de ese flujo (uno por cada participante considerado en los esquemas definidos en la *fase 1*). Esto significa que las tres fases descritas anteriormente se repiten hasta crear tantos cripto-contenedores como etapas consideradas en un flujo de trabajo.

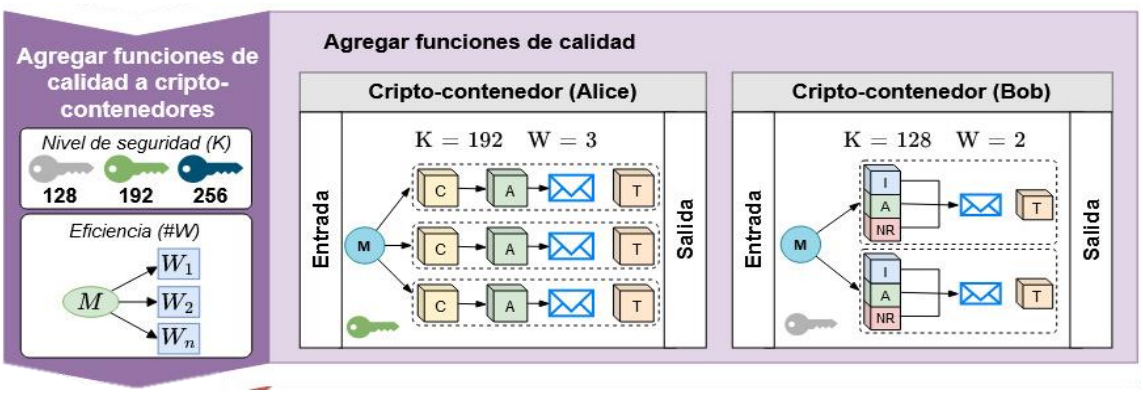

Figura 7. Fase 3 para la creación de servicios de intercambio de información eficientes y seguros.

En la *última fase* (ver Figura 8), los cripto-contenedores se encadenan para crear un servicio de información seguro, que establecerá controles sobre el intercambio de datos a través del flujo de trabajo resultante definido por cada esquema.
Esto significa que los participantes en los flujos de trabajo de intercambio de información confidencial no están obligados a hacer cumplir las políticas de seguridad (encriptar los datos antes de enviarlos a otro participante), ya que esta misma tarea la realizan los cripto-contenedores de manera automática y transparente. Lo anterior es clave para que las organizaciones enfrenten la paradoja de la información de privacidad, donde los usuarios finales no aplican la seguridad a sus operaciones de intercambio, incluso cuando saben que esta es una tarea crítica antes de compartir datos confidenciales.

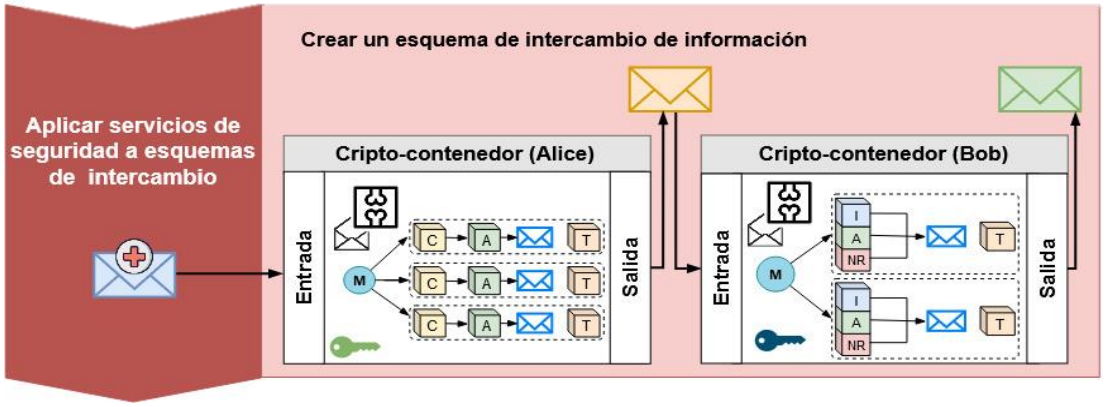

Figura 8. Fase 4 para la creación de servicios de intercambio de información eficientes y seguros.

Importante: Para más información acerca de Chimalli: Servicio para el acceso seguro y confiable de datos médico, ver el reporte técnico [”Chimalli: Servicio de acceso seguro a servicios de e-salud y/o sistemas de analítica”.]