UBA
Universidad de Buenos Aires
Argentina virtus robur et stadium

Universidad de Buenos Aires

Facultad de Ciencias Económicas
Facultad de Ingeniería
Facultad de Ciencias Exactas y Naturales

Carrera de Especialización en Seguridad Informática

Trabajo Final de Especialización

Diseño de un sistema seguro de prescripciones médicas electrónicas

Autor: Leandro Augusto Ordoñez

Tutor: Dr. Pedro Hecht

Año de presentación: 2020
Cohorte del cursante: 2019

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Trabajos Finales vigente y se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO
Leandro Augusto Ordoñez
DNI 24.632.770

Resumen

Un sistema electrónico de prescripciones médicas es aquel que permite transmitir las recetas de medicamentos desde el sistema informático del profesional prescriptor hasta la farmacia o proveedor de medicamentos. Tal sistema presenta abundantes ventajas por sobre el sistema tradicional de recetas en papel, que van desde evitar los errores y problemas administrativos hasta reducir el fraude. Dado que este sistema maneja información sensible de las personas se debe diseñar de forma segura. Para poder reemplazar a las firmas de puño y letra se debe implementar un esquema de firmas digitales que garantice la identidad del profesional que realiza la prescripción.

En el presente trabajo se plantean los aspectos que hay que tener en cuenta para diseñar un sistema seguro de prescripciones médicas electrónicas. Primeramente, se realiza una exposición acerca del funcionamiento propuesto del sistema y se evalúa el marco legal que da soporte a su funcionamiento. Por último, se revisan cada uno de los aspectos de seguridad que hay que tener en cuenta para diseñar un sistema seguro de prescripciones médicas y se brindan sugerencias y ejemplos concretos de implementaciones y código.

Palabras Claves

Prescripción electrónica; *Electronic prescription system (EPS)*; protección de información médica; recetas electrónicas; informática médica;

Tabla de contenido

Introducción

El área de salud no escapa a la aplicación de las tecnologías de la información y la interconexión entre proveedores y usuarios. La información sobre el paciente es estratégica para los servicios de salud. Los profesionales requieren que esta esté disponible en el lugar de atención y en el momento oportuno y muchas veces, para lograr satisfacer esta necesidad, se deben enviar y recibir datos de salud. Pero no es solo por la simple transferencia de datos, sino que la información compartida deriva en decisiones médicas para el cuidado de los pacientes. Si se produjera un ataque sobre esta información puede haber consecuencias sobre la vida de una persona. Cualquier solución informática que utilice tecnologías de comunicación debe ser segura debido a la información sensible que maneja.

En nuestro país el sistema de provisión de medicamentos y drogas es principalmente manual basado en una receta médica hecha en papel y firmada de puño y letra por el prescriptor. Aunque el sistema manual ha probado ser útil por años posee algunas desventajas, como la legibilidad, la posibilidad de error y el fraude por falsificación.

La transformación digital está llegando al sistema de provisión de medicamentos. Un sistema de prescripciones electrónicas permite a los profesionales de salud realizar la prescripción de medicamentos y transmitirla electrónicamente a las farmacias. El objetivo es mejorar la seguridad del paciente y la calidad del servicio. Algunas obras sociales –como PAMI, por ejemplo–, empresas de medicina prepaga o colegios de farmacéuticos ya están incursionando en la implementación de un sistema de recetas digitales.

Este trabajo está inspirado en la experiencia laboral del autor en el sistema privado de salud. Si bien en este ámbito existen numerosas soluciones para la validación, procesamiento y facturación

de prestaciones médicas, el tratamiento de las recetas de medicamentos es prácticamente manual. La liquidación, auditoría y facturación de farmacias y droguerías tienen a la receta como documento principal y los controles se suelen realizar sobre el papel.

El objetivo del trabajo es presentar un sistema de prescripciones médicas electrónicas ideal, con una descripción completa de su funcionamiento y los actores que participan. Se explican las ventajas que tendría este sistema sobre el sistema manual y los riesgos a los que está expuesta la información que maneja. También se explora el marco legal actual que podría justificar su uso en reemplazo de las recetas firmadas manualmente.

Debido a que este sistema administra información sensible de los pacientes y que, por tanto, debe ser protegida es que se revisan detalladamente los elementos de seguridad que se deben tener en cuenta en su diseño, desde la encriptación de la información y firma digital hasta la seguridad en las comunicaciones y bases de datos.

El trabajo está enfocado desde el punto de vista de un financiador de servicios de salud, como por ejemplo una obra social o una empresa de medicina prepaga, que requiere optimizar los procesos de dispensa, auditoría, liquidación y control de la provisión de medicamentos a sus pacientes afiliados. El propio financiador será quien diseñará este sistema de prescripción médica electrónica y lo pondrá a disposición de sus afiliados, prestadores de salud contratados y farmacias de su red de proveedores.

Descripción de un sistema de prescripciones médicas electrónicas

Un sistema de prescripciones médicas electrónicas -o *e-Prescribing* por su nombre en inglés– consiste en un sistema informático para que un profesional de la salud pueda registrar una receta con indicaciones de medicamentos y que esta información sea transmitida al agente que realiza la dispensa del medicamento. Por medio del tal sistema, los médicos acceden a una plataforma de servicios provista por una entidad de salud para transmitir sus prescripciones, a través de una red. Cuando el paciente concurre a una farmacia o proveedor de medicamentos, la prescripción es recibida y se produce la dispensa.

Este sistema trabaja siguiendo el siguiente modelo de funcionamiento:

- El médico genera la prescripción electrónica desde un dispositivo informático.
- La receta se transmite electrónicamente al financiador para su autorización sin necesidad de hacer ninguna gestión administrativa.
- El paciente concurre a la farmacia de su elección sin necesidad de llevar ningún papel.

La implementación de un sistema de prescripciones electrónicas persigue varios objetivos: reducir los errores de prescripción y así mejorar la seguridad del paciente, optimizar el proceso de prescripción para reducir costos, tanto en medicamentos como de gestión, evitar trámites administrativos, reducir la burocracia y mejorar la calidad de atención y velocidad del proceso de receta y provisión de una medicación [1] [2].

Actores

El paciente es el beneficiario final de los servicios de salud y de los servicios del sistema de prescripción electrónica. El prescriptor es el profesional de la salud que brinda los servicios de salud al paciente y que está autorizado a emitir prescripciones de medicamentos. No solo médicos cumplen este rol, sino también psiquiatras y odontólogos[1]. El dispensador es el proveedor de medicamentos, que puede ser una farmacia, droguería o un laboratorio. El financiador es la entidad que gestiona los servicios de salud para atender a la población a la que brinda cobertura; son las obras sociales –sindicales, de empresas, de dirección, etc.– o empresas de medicina prepaga o mutuales [3].

Para el presente trabajo se circunscribirá el escenario a un financiador único que desea diseñar e implementar un sistema de prescripciones médicas electrónicas. Este sistema deberá mejorar la calidad del proceso de prescripción al brindar más información a médicos al momento de realizarla, evitar errores, reducir los requerimientos administrativos para todos los actores y contribuir a reducir el gasto farmacéutico. El universo de pacientes será todos los que están afiliados o asociados a este financiador y el de profesionales prescriptores será aquellos que estén habilitados profesional y administrativamente a realizar prescripciones. Se dejará de lado el escenario de un sistema de prescripción electrónica a nivel nacional debido a que los actores serán otros: debería intervenir el Ministerio de Salud con resoluciones que habiliten el uso de tal sistema, los médicos prescriptores serían todos los médicos del país que tengan matrícula profesional y las personas beneficiarias, todos los habitantes del país.

[1] Médicos veterinarios también pueden emitir recetas de medicamentos, pero para este trabajo no se tendrán en cuenta por estar fuera del alcance específico.

Componentes [4]

Un sistema de prescripciones electrónicas está formado principalmente por una base de datos de pacientes de un centro asistencial o de afiliados a una obra social o prepaga, que son aquellas personas que pueden recibir prescripciones médicas. Debe contener los datos identificatorios y filiatorios: número de identificación o número de afiliado, nombre y apellido, edad, sexo y plan de cobertura son los más importantes. Además, contiene su información clínica como ser diagnósticos, problemas médicos, patologías, historial médico, medicación que consume, resultados de estudios de diagnóstico, etc. La información de alergias a ciertos medicamentos o de efectos adversos sería útil para que el sistema muestre una alerta en los casos necesarios. Idealmente esta información estaría contenida en una historia clínica electrónica única de la persona. El plan de cobertura médica de la persona le permitirá al sistema validar o autorizar la provisión de un medicamento.

El segundo componente es una base de datos de especialidades medicinales. Son los productos comerciales disponibles en las farmacias que podrán recetarse y que los pacientes o afiliados podrán adquirir. Se incluye su nombre comercial, drogas que lo componen, presentación, dosis, posología, laboratorio que lo produce, precio, cobertura brindada según cada plan de atención, etc. Esta información se obtiene de fuentes de datos publicados por la industria farmacéutica o los financiadores. Manual Farmacéutico [5] y Kairos [6] son dos ejemplos de empresas privadas que publican esta información en Argentina.

Otro elemento básico de un sistema de prescripción electrónica es una base de datos con información sobre monodrogas que son los componentes de los medicamentos. Contiene datos como el nombre de cada una, nombres alternativos o sinónimos, clasificación farmacológica, dosis recomendadas, efectos adversos, indicaciones y contraindicaciones, como así también información útil y

recomendaciones para el paciente. Las interacciones entre medicamentos podrían permitir mostrar alarmas cuando se receten medicamentos que producen efectos no deseados cuando se combinan.

Hay otras bases de datos relacionadas a la administración del sistema. Por ejemplo, una base de datos de prestadores médicos habilitados para emitir recetas de medicamentos y de farmacias que pueden proveerlos.

Si la información está disponible en bases de datos estructuradas el sistema podrá aplicar reglas al momento de confeccionar la prescripción. Se podría mostrar una advertencia si se está recetando un medicamento cuyos principios activos han sido recetados recientemente a la misma persona, si el paciente presenta alergia al principio activo recetado o si existe una interacción negativa entre dos drogas recetadas.

Ciclo de vida de una prescripción

A efectos del presente trabajo, se reconocerán los siguientes pasos en el ciclo de vida de una prescripción de medicamentos. El sistema de prescripción médica electrónica deberá asistir y facilitar cada una de estas etapas.

Prescripción

La prescripción o receta de medicamentos es un acto médico por el cual un profesional de la salud emite una indicación terapéutica [7]. El sistema propuesto será la herramienta que utilizará para realizar este proceso.

Autorización

Es el proceso de validación de los datos ingresados. El sistema propuesto automatizará la autorización en la medida de lo posible. Algunas prescripciones o ciertos medicamentos no podrán ser

autorizados por el sistema y serán derivados a un auditor médico perteneciente al financiador quien autorizará o no la prescripción.

Dispensa

En esta etapa, el paciente concurre al proveedor o farmacia de su preferencia, quien suministrará la medicación recetada, según la cobertura brindada por el financiador de servicios.

Facturación

Cada dispensador facturará la cobertura en medicamentos al financiador de forma periódica, según el procedimiento previamente definido en el contrato con cada uno.

Auditoría, liquidación y pago

Estas etapas son procedimientos administrativos realizados por el financiador. La auditoría médica realiza un control de la facturación con criterio médico–administrativo. El proceso de liquidación consiste en determinar los importes a pagar a cada dispensador. Finalmente se produce el pago por las coberturas de medicamentos a cada proveedor.

Ventajas sobre el sistema tradicional

Un sistema de prescripciones electrónicas debe ser diseñado con el objetivo de superar los problemas del sistema tradicional de recetas en papel. Los beneficios serán para el paciente, para el prescriptor, para el dispensador y para el financiador.

El sistema deberá poder reducir los errores médicos en las prescripciones causados por letra ilegible o por equivocación al seleccionar el medicamento recetado. Los procesos de validación y control que se implementen tenderán a reducir el daño al paciente [8].

Los errores de medicación son muy comunes. En nuestro país hay poca información sobre los eventos adversos relacionados a errores de medicación; el último informe oficial se publicó en 2010. Argentina participó en el Estudio Iberoamericano de Efectos Adversos (Ibeas) en 2007 y 2008 [9] que determinó que el 9,13% de los efectos adversos estaban relacionados al uso de la medicación y el 55% de los casos podría haber sido evitado. En un estudio realizado en un hospital de Argentina entre 2012 y 2013 un 16,4% del total de prescripciones validadas contenían un error, un 0,2% de casos fueron errores de transcripción y un 0,6% de dispensa [10]. Los errores de medicación, como ser dosis no adecuadas, instrucciones de posología que no son claras para el paciente o el uso de abreviaturas son una de las causas evitables más importantes de daño en salud en todo el mundo. La Organización Mundial de la Salud estima los costos relacionados a errores de medicación en todo el mundo en 42 mil millones de dólares [11] lo que representa el 0,7% del gasto total mundial en salud [12]. Además, los errores de medicación son una causa de aumento de la duración y de reingreso en una internación [9, p. 54].

En otro estudio realizado en seis hospitales de Cataluña, España, se detectaron 16,94 errores de prescripción por cada 100 pacientes-día; 16% de estos errores se dieron en el proceso de

prescripción de medicamentos, 27% en la transcripción y 48% en la dispensación [13]. Un sistema de prescripciones médicas electrónicas ayudará al médico prescriptor en el proceso de seleccionar correctamente la droga recetada y al farmacéutico en el momento de la dispensa.

Para facilitar la tarea de prescripción el sistema de prescripciones médicas electrónicas estará alimentado por una base de datos de medicamentos. El prescriptor identificará la droga o la marca comercial que desee recetar y el sistema mostrará una lista con las distintas dosis, presentaciones y cantidad de unidades. La selección estará asociada al código numérico de medicamento que formará parte integral de la receta electrónica y así se facilitará la dispensa ya que no habrá ambigüedad [14].

Las recetas médicas tradicionales confeccionadas de puño y letra tienen el problema de la ilegibilidad de la letra del prescriptor que puede causar error en la dispensa. Por ejemplo, en Escocia una mujer debió ser internada por lesiones causadas por la dispensa incorrecta de un medicamento debido a la letra ilegible en la receta y cuyo nombre comercial era similar a lo realmente recetado [15]. Los medicamentos llamados "LASA"[2], que son medicamentos parecidos visualmente entre sí o con nombres similares fonéticamente [16] también presentan un problema serio al momento de interpretar la letra manuscrita. Por ejemplo, puede presentarse confusión entre las drogas "Cefalotina" y "Cefalexina", dos antibióticos para tratar distintas patologías; o entre "Dexametasona" –un antinflamatorio– y "Betametasona" –para problemas de la piel. También pueden presentarse errores debido a la similitud de los nombres comerciales que podrían confundirse si la letra del profesional que los prescribe no es lo suficientemente clara. El medicamento con nombre comercial "I.U.400" –un suplemento dietario– podría confundirse fácilmente con

[2] LASA: *Look-Alike, Sound-Alike*

el medicamento “IBU 400” –un analgésico– por tener nombres similares, o medicamentos con nombres idénticos pero distintas drogas como por ejemplo “Dulcolax” en gotas (que contiene la droga llamada picosulfato de sodio) y en grageas (que contiene bisacodilo). Un sistema de prescripciones electrónicas podría acabar con este problema al registrar los medicamentos recetados y dispensados a través de códigos numéricos únicos.

Si el sistema de prescripciones electrónicas se complementa con una base de conocimiento acerca del paciente, como ser su información clínica –sexo, edad, enfermedades prexistentes, etc.–, información sobre sus condiciones médicas –diabetes, embarazo, enfermedad pulmonar crónica, enfermedad renal, etc.– e información farmacológica –como ser alergias– se podría visualizar una advertencia cuando un profesional intente realizar una prescripción de un medicamento que posea contraindicaciones a alguna de sus condiciones [7]. Por ejemplo, el sistema podría mostrar una alerta si el paciente tiene diagnóstico de presión arterial elevada y el profesional intenta recetar algún medicamento contraindicado en esta situación. Esto es una clara ventaja sobre el sistema tradicional de recetas que depende del conocimiento del profesional, de su memoria o de la calidad de su historia clínica.

Al momento de prescribir el sistema podría examinar el historial de prescripciones médicas del paciente y detectar contraindicaciones o interacciones medicamentosas adversas entre el medicamento que va a ser recetado y aquellos que fueron recetados recientemente [14]. En cambio, en el sistema tradicional puede que el profesional no conozca la medicación recetada por otros médicos al mismo paciente. Del mismo modo el sistema podría detectar prescripciones duplicadas en un corto período de tiempo. Si un profesional prescribe la misma droga que ha sido prescripta al mismo paciente por otro profesional el

sistema mostrará un aviso. De esta forma se puede mitigar la práctica conocida como "*doctor shopping*"[3].

Otra ventaja es que se posibilitaría el seguimiento de las prescripciones. Con el sistema tradicional, un profesional no tiene forma de saber si el paciente obtuvo la medicina recetada ya que, con la receta manuscrita, este puede o no adquirirlas. Sin embargo, si se realiza el seguimiento de la receta, el profesional podría enterarse si los medicamentos fueron dispensados.

La prescripción de medicamentos para patologías crónicas también se simplificaría con el uso de un sistema electrónico de recetas. Enfermedades como diabetes, hipotiroidismo, asma bronquial o Parkinson requieren la prescripción regular de los mismos medicamentos y dosis. Actualmente un paciente debe concurrir al médico a renovar su receta cada vez que lo necesite, lo cual consume tiempo tanto del paciente como del médico y de su personal. Con la utilización del sistema propuesto el médico podría revisar y generar la repetición de la misma prescripción rápidamente.

Debido a que se encuentran digitalizadas y disponibles en bases de datos, la pérdida de prescripciones se reducirá. La gente suele extraviar las recetas en papel y, en ese caso, es necesario concurrir nuevamente al profesional para obtener una nueva. Esta situación se evitará ya que el paciente tendrá acceso a sus prescripciones electrónicas, lo que ahorrará tiempo y trabajo del médico y de su personal. También se reducirá el trabajo administrativo en los procesos de prescripción, validación, autorización, dispensación y facturación. Al momento de la prescripción, el sistema mostrará cuáles son los medicamentos que están cubiertos por su financiador y por su plan médico. De esta forma, el profesional tendrá la posibilidad de seleccionar el medicamento o presentación más

[3] *Doctor shopping consiste en visitar varios médicos para obtener múltiples recetas de la misma medicación. El caso es más grave cuando los medicamentos recetados son sustancias controladas como psicofármacos o estupefacientes* [55].

adecuado según la cobertura. Del mismo modo facilitará el trabajo del médico auditor en el proceso de autorización de una medicación no cubierta ya que la información estará volcada en el sistema en un estado pendiente de autorización. Al momento de concurrir a la farmacia, la información previamente validada de los medicamentos recetados estará disponible de forma inmediata lo que redundará en una reducción del tiempo de atención. Por último, la información generada al momento de la venta de los medicamentos quedará automáticamente preparada para su facturación y así se evitarán los tiempos de carga manual de datos y de liquidación en el financiador. Como última consecuencia, esto podría redundar entonces en la reducción de los tiempos de pago [17].

El sistema tradicional de recetas en papel permite el fraude cuando prescriptores y dispensadores se asocian para cometerlo. Las estafas más comunes incluyen la falsificación de recetas, el robo de sellos, la prescripción de medicamentos con datos falsos de pacientes o con pacientes falsos, o para patologías falsas, y la facturación de medicamentos no dispensados. Recientemente en nuestro país se denunció una estafa millonaria con la utilización datos falsos de pacientes o que ya habían fallecido [18]. El fraude incluso puede ser en connivencia con las asociaciones farmacéuticas [19]. Si el sistema electrónico se diseña teniendo en cuenta las medidas de seguridad adecuadas estos casos se pueden reducir con métodos fehacientes de validación del paciente, de la receta y de la dispensa.

Funcionamiento propuesto

En esta sección se expone la propuesta de funcionamiento del sistema de prescripciones médicas electrónicas. Se tiene en cuenta el escenario expuesto anteriormente.

El sistema será provisto por el financiador. Este será quien valide las identidades, asigne permisos de acceso y establezca los perfiles y grupos de usuarios. Además, proveerá una aplicación para dispositivos móviles que será destinado a sus afiliados para que puedan realizar algunos trámites administrativos, como registrar o modificar su dirección de correo electrónico, su contraseña, su número telefónico y acceder a las prescripciones médicas que hayan sido emitidas a su nombre, como funciones relevantes al proceso de prescripción. El financiador podrá además agregar a la aplicación otras funcionalidades propias de su actividad. El afiliado titular además podrá consultar la misma información de cada miembro de su grupo familiar.

El financiador será también el encargado de validar las identidades de prestadores, farmacias y afiliados y será quien deba implementar los procesos administrativos necesarios para cumplir esta función. Muchos de estos procesos ya se encuentran en uso como parte del proceso de contratación de prestadores y farmacias y del proceso de afiliación de las personas por medio de requisitos de documentación, firma de contratos y declaraciones juradas.

Para explicar el funcionamiento se repasará un caso de uso típico. Todo comienza con un paciente que es beneficiario del financiador de servicios de salud, quien concurre a su profesional para recibir atención médica. Cuando el médico decide realizar una prescripción médica accede al portal de servicios identificándose fehacientemente. El financiador está en condiciones de validar no solo la identidad del médico sino también que esté contratado para prestar

servicios y que su perfil coincida con uno que pueda realizar prescripciones médicas.

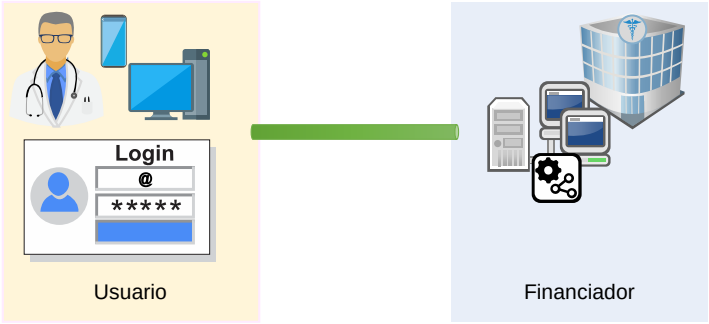

Figura 1 El usuario accede al portal de servicios del financiador con usuario y clave

Seguidamente, el profesional debe realizar la búsqueda de los datos del paciente con los datos que constan en su credencial de afiliación. Al ingresar su número de beneficio y corroborar los datos filiatorios el profesional estará totalmente seguro de que no se cometerá ninguna equivocación en la identificación de la persona. Esto constituye el primer paso para eliminar un posible error de prescripción y es también un factor para disminuir posibles fraudes.

El profesional procede entonces a registrar el o los medicamentos que forman la prescripción. El sistema facilitará la búsqueda a través del nombre de la droga o el nombre comercial y desplegará una lista de posibles opciones de la cual el prescriptor podrá seleccionar. Se indica la droga de cada uno, su presentación, dosis y nombre del laboratorio de lo produce. Además, la información se cruzará con el plan de cobertura del paciente y se indicará si el producto es cubierto por el financiador o si existe alguna restricción.

Cuando la prescripción está completa y antes de su envío, el sistema solicitará que sea firmada digitalmente. El proceso requiere el ingreso de una clave secreta o un PIN[4]. El tiempo y esfuerzo que

[4] Número de identificación personal

insume generar la firma digital es el equivalente al que demanda hacer la firma manuscrita y aplicar un sello. El sistema asigna un identificador único a la receta, aplica la firma digital de forma automática [17], la encripta y transmite al financiador. Opcionalmente se puede imprimir un comprobante para el paciente.

El sistema enviará una confirmación al teléfono celular del paciente.

Por medio de una aplicación para teléfonos inteligentes, el usuario podrá realizar la compra de su medicamento. La aplicación mostrará un código QR[5] que contiene el número de receta generado anteriormente y un *hash* de los datos de la receta para poder validar su contenido. La ventaja del uso de una aplicación es la de evitar posibles fraudes. Si el profesional hiciera una receta a un paciente inexistente el sistema no podría mostrar esta confirmación por lo que sería imposible que se produzca la venta. Si, en cambio, la receta estuviera hecha a un paciente válido pero que no ha visitado a este médico, este paciente recibirá la confirmación de una prescripción que nunca solicitó. La presentación de esta confirmación en la farmacia o droguería será obligatoria para poder acceder a los medicamentos recetados y validar los datos de la prescripción. Aquellas personas que no posean un dispositivo celular podrán utilizar un comprobante impreso en su reemplazo que contenga la misma información. Las prescripciones de los niños estarán disponibles en la aplicación para celular de sus padres o titulares de la cobertura.

[5] *Quick Response Code.* Código de respuesta rápida.

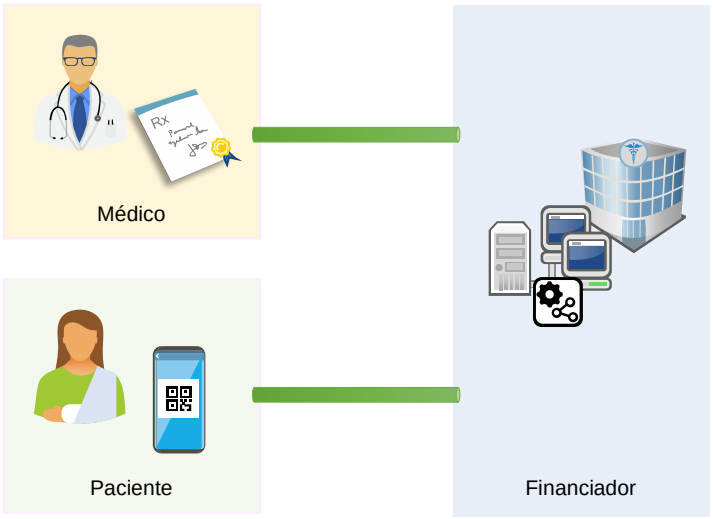

Figura 2 Código QR en el celular del paciente

Cuando el paciente concurre a la farmacia de su elección, presentará el código QR en la aplicación de su dispositivo o en una copia impresa junto con su identificación. El financiador puede determinar que es obligatoria la presentación de su carnet de servicios y el documento de identidad como medios de identificación y con el objetivo de reducir la posibilidad de fraude.

El código QR es leído con un escáner por el personal de la farmacia o droguería. El sistema obtiene el identificador único de la receta y accede a la información de la prescripción. Luego realiza las verificaciones de seguridad necesarias, como desencriptar y validar la firma digital del prescriptor y visualiza los datos del paciente y de la prescripción. El encargado podrá realizar una validación de la identidad de la persona al comparar con los datos personales del paciente. El objetivo es reducir la posibilidad de errores de prescripción ya que se evita la venta irregular de medicamentos a personas no autorizadas, o que no tengan una prescripción válida. Si todos los controles son exitosos se puede producir la dispensa de la medicación. El encargado confirmará la venta en el sistema y la información será enviada de forma encriptada al servicio.

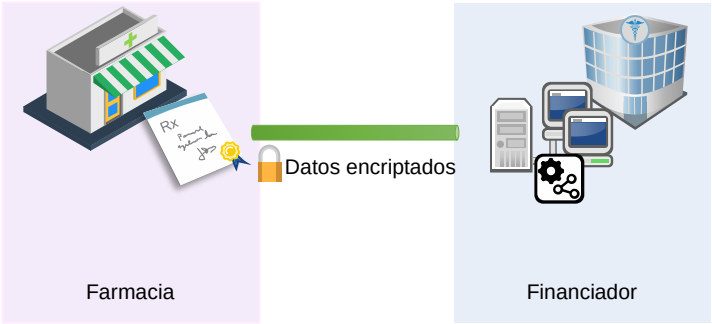

Figura 3 Envío de datos firmados y encriptados

El financiador conocerá en tiempo real la facturación de los proveedores de medicamentos mientras que estos tendrán la información ya cargada de todas sus ventas al momento del cierre del período de facturación.

Marco Legal

En esta sección se evalúan las normas jurídicas aplicables que aprueban el uso de un sistema de prescripciones médicas digitales en reemplazo de aquellas en papel y que le dan un marco jurídico a su validez.

El artículo 15 de la Ley de Derechos del Paciente (ley número 26529) enumera los asientos que debe tener una historia clínica. El inciso g) indica que todo acto médico de prescripción de medicamentos –entre otros– es uno de ellos [20]. Por lo tanto, la receta médica forma parte de la historia clínica.

Por un lado, el artículo 19, inciso 7º de la Ley de Ejercicio de la Medicina (ley 17132) establece que los profesionales médicos están obligados a realizar las prescripciones médicas de forma manuscrita, fechadas y firmadas [21].

Por otro lado, la ley de Firma Digital (Ley 25506) indica, en el artículo tercero, que "…cuando la ley requiera una firma manuscrita, esa exigencia también queda satisfecha por una firma digital. Este principio es aplicable a los casos en que la ley establece la obligación de firmar…" [22]. Como consecuencia, la firma digital del prescriptor puede reemplazar la firma manuscrita exigida en las recetas médicas. De aquí entonces sale el requerimiento de que, en un sistema de prescripción médica electrónica, las recetas que se registren deben estar firmadas digitalmente. Además, el artículo 6 dispone que "… Un documento digital también satisface el requerimiento de escritura". De esta forma, las recetas médicas digitales equivalen a aquellas manuscritas.

El artículo 12 de la misma ley indica que "la exigencia legal de conservar documentos, registros o datos también queda satisfecha con la conservación de los correspondientes documentos digitales firmados digitalmente." Esto significa que una base de datos con las

recetas firmadas digitalmente satisface el requerimiento de conservación de la documentación médica.

El artículo 7 establece la presunción de autoría de la firma digital, ya que determina que "… toda firma digital pertenece al titular del certificado digital que permite la verificación de dicha firma." Es por ello que se considerará que el profesional que realiza y firma digitalmente una prescripción médica será fehacientemente su autor. Por último, el artículo 8 de la misma ley establece la presunción de integridad. Cuando el proceso de verificación de la firma digital de un documento da resultado positivo se presume que el documento no ha sido modificado. En el caso de una receta médica se puede asegurar que su contenido no ha cambiado con respecto a lo prescripto por el profesional si se puede validar la firma digital.

El decreto reglamentario de la ley 26529 sobre derechos del paciente en su relación con los profesionales e instituciones de la salud, en su artículo 12, realiza una salvedad relacionada a la información médica digital: "A excepción de los casos de la historia clínica informatizada, los asientos de la historia clínica escrita deben ser suscriptos de puño y letra por quien los redacta, para identificar quién es responsable del mismo…" [23]. La reglamentación del artículo 13 indica que "la historia clínica informatizada deberá adaptarse a lo prescripto por la Ley Nº 25506…" de Protección de Datos Personales.

Las normas legales repasadas anteriormente aprueban el uso de la firma digital como método para asegurar la identidad y la validez de las prescripciones médicas electrónicas. Aunque la ley de Derechos del Paciente determina que las recetas médicas deben ser manuscritas, la Ley de Firma Digital permite su confección de forma electrónica.

Riesgos y amenazas a la seguridad

Los registros médicos electrónicos contienen información altamente sensible. Están conformados por datos personales de los pacientes –como ser datos de identidad, sexo, edad, plan de cobertura, domicilio, etc.–, de patologías médicas, de las prestaciones médicas que han recibido y de las prescripciones de medicamentos que han consumido. Es información muy valiosa para ciberdelincuentes que se puede vender por valores que superan los cientos de dólares en el mercado negro, mucho más que los pocos centavos que vale un número de tarjeta de crédito [24]. El valor de la información médica es mayor debido a que se torna más difícil detectar el robo de identidad [25]. Una persona puede cambiar su número de tarjeta de crédito si fue extraviada o robada, o puede cerrar o cambiar su cuenta bancaria, su CBU[6] o su número de identificación personal si fueron comprometidos. Contrariamente, los datos médicos se mantienen inalterables en el tiempo y no pierden su valor. A diferencia del robo de datos financieros, que puede detectarse más o menos rápidamente, puede pasar mucho tiempo hasta que se descubra el robo o acceso no autorizado a datos médicos. El tiempo hasta descubrir la brecha y el tiempo para reportarla suelen ser mayores [26].

Por otro lado, compartir la información médica forma parte de la cultura de la práctica de la medicina; esta se transmite entre profesionales para brindar tratamientos médicos integrales que abarcan varias especialidades, en la que cada uno requiere acceso rápido a la información médica. Un sistema de prescripciones médicas como el propuesto no podría funcionar si no se comparte la información entre los profesionales médicos y los proveedores de medicamentos, aunque transmitir información de las recetas entre los

[6] Clave bancaria única o Clave bancaria uniforme. Permite identificar una cuenta bancaria de forma unívoca en todo el sistema financiero argentino.

distintos actores del sistema a través de canales de comunicación inseguros aumente la superficie de ataque. La interconexión –que forma parte de su naturaleza– crea numerosos riesgos y amenazas a la seguridad y a la privacidad.

El objetivo de los sistemas de salud es mantener a los pacientes seguros, inclusive su información [27]. Si la información médica de las personas es comprometida se pueden producir consecuencias indeseables como pérdida de confianza de los pacientes, daño reputacional, desventaja comercial del financiador y de los proveedores, robo de identidad o fraude médico o de prescripciones. La información médica altamente sensible puede llegar a entidades no autorizadas como ser la prensa, compañías de seguro, investigadores privados o abogados. Por ejemplo, durante el año 2016, año de las elecciones presidenciales de Estados Unidos, se publicaron informes médicos falsos de la candidata del partido Demócrata Hillary Clinton que supuestamente demostraban que sufría de convulsiones y demencia. Posiblemente, esta información médica –falsa– pudo haberle costado la elección [28].

Una vez que un atacante obtiene información médica la podrá vender o utilizar para sus propios beneficios. Por ejemplo, podría utilizar la información médica o de cobertura de salud para acceder a prestaciones médicas, obtener recetas de medicamentos a nombre de ciertos pacientes o realizar liquidaciones o facturaciones fraudulentas.

Hay una cantidad significativa de amenazas sobre la información de las prescripciones y en general sobre la información médica, que serán enumerados en esta sección. El financiador de servicios de salud será el responsable de asegurar esta información. Tanto este como los proveedores de los medicamentos también administran datos financieros de los pacientes, como ser información de pagos, de cuentas corrientes, números de tarjetas de crédito y de cuentas bancarias, que presentan riesgos inherentes.

Actualmente se está produciendo un aumento en la cantidad de ataques cibernéticos contra el sector de la salud [29]. La revista *Forbes* predice que, debido a que los prestadores de salud no se encuentran preparados y a que los ataques a los datos médicos son muy lucrativos, se espera un aumento de la cantidad de ataques de *malware* [30].

Según los datos publicados en el portal de filtración de datos del Departamento de Salud de los Estados Unidos, en 2020 se han reportado un total de 422 casos que afectaron a datos de más de 22 millones de personas. Los eventos de seguridad incluyen accesos no autorizados, pérdidas o robos de computadoras, laptops y servidores, de registros con datos médicos, de correos electrónicos o de documentación de papel, entre otros [31].

Tipo de filtración	Cantidad de casos
Incidente de TI	19.916.897
Descarte inadecuado de información	561.262
Pérdida	128.686
Robo	98.760
Acceso no autorizado	1.899.276

Tabla 1 Cantidad de eventos de seguridad denunciados en el portal de filtración de datos del Departamento de Salud de Estados Unidos en 2020, clasificado por tipo de filtración.

Riesgos de la información médica

La informática médica –y dentro de esta, el sistema de prescripciones médicas– es víctima típica de ciberataques.

El *ransomware*, el *malware* y el *phishing* son típicos en esta industria. Se produce cuando el atacante logra acceso a la red e instala algún tipo de software dañino con el que pueden bloquear servicios, encriptar archivos e incluso comprometer un sistema completo. Los ataques de *phishing* requieren un *link* aparentemente auténtico para introducir software no deseado. Por tanto, se torna esencial entrenar a los usuarios para que puedan reconocer los engaños de *phishing*.

El recurso humano también constituye un riesgo ya que los empleados de los proveedores de servicios de salud y de las farmacias tienen acceso a la información médica de pacientes. Si bien la gran mayoría no suele abusar de este poder, no se puede garantizar que algunas personas no utilicen información sensible de forma indebida. Por falta de capacitación el personal también puede ser un riesgo si no son conscientes de lo que deben y no deben hacer. Actividades como conectar dispositivos inseguros, instalar aplicaciones desconocidas o almacenar datos médicos o de prescripciones en dispositivos extraíbles deberían ser controladas y evitadas.

Los posibles usuarios de este sistema de prescripciones médicas, ya sean obras sociales, empresas de medicina prepaga, farmacias, droguerías, clínicas y profesionales de la salud, a su vez contratan otros proveedores quienes también pueden llegar a tener acceso a la información médica. Empresas o entidades intermedias que realizan auditorías o facturación, proveedores de medicamentos, empresas tercerizadas de procesamiento de datos o de digitalización de documentación, empresas de validación en línea o desarrolladores externos son algunos ejemplos de entidades externas que pueden requerir acceso a cierta información médica, cuyo riesgo se deberá evaluar.

Los dispositivos usados por proveedores y profesionales de la salud para acceder al sistema también constituyen un riesgo a tener en cuenta en el diseño de este sistema. Los médicos frecuentemente utilizan dispositivos móviles de su propiedad para acceder y realizar las prescripciones. Estos dispositivos no siempre disponen de niveles de seguridad adecuados, lo que hace que el ingreso al sistema de prescripción sea vulnerable a *malware* o *hackers*. Cuando uno de estos dispositivos se pierde o es robado se produce un riesgo muy grande de seguridad ya que, una vez que el dispositivo está en

posesión del ladrón, éste podría acceder al sistema con las credenciales almacenadas.

Todos estos riesgos enumerados afectan también a las farmacias y proveedores de medicamentos, porque utilizan las mismas tecnologías y protocolos que el proveedor de salud, además de procesar electrónicamente las prescripciones y realizar las validaciones en línea necesarias antes de dispensar el medicamento [32].

Aspectos de seguridad

Los datos médicos en general y los de las prescripciones médicas en particular son datos relativos a la salud y como tal son definidos por la ley 25326 de Protección de Datos Personales [33] como datos sensibles. Por lo tanto, un sistema de prescripción médica electrónica debe implementar las medidas de seguridad necesarias para resguardar la confidencialidad e integridad de la información médica que se maneje. La confidencialidad de los datos médicos y de la información de los pacientes debe estar asegurada por lo que la transmisión de los datos de las prescripciones médicas en texto plano a través de redes inseguras no es una opción. De igual modo se debe garantizar la seguridad en los accesos al sistema únicamente a aquellos profesionales médicos que participen en el proceso de prescripción y evitar aquellos que no estén autorizados. Este sistema debe entonces implementar métodos para autorizar el acceso de forma fehaciente. La integridad de los datos de las prescripciones también debe estar asegurada para evitar y detectar modificaciones mientras que las identidades de pacientes, profesionales y farmacias deben estar verificadas de forma fidedigna. En esta sección se examinarán detalladamente los elementos de seguridad que debe implementar un sistema de prescripción médica electrónica para satisfacer estos y otros requerimientos de seguridad.

Confidencialidad

Los datos de las recetas médicas deben estar protegidos para evitar su acceso y lectura a personas no autorizadas. Asegurar la confidencialidad consiste en impedir el acceso, uso y divulgación de la información almacenada y en tránsito. Una de las formas de lograrla es por medio de la encriptación.

Los sistemas de criptografía de clave simétrica utilizan una clave que es compartida entre los usuarios y que debe mantenerse en secreto. La misma clave es utilizada para la encriptación y

desencriptación del mensaje. Estos sistemas existen desde hace miles de años, primero con el Cifrado César hasta métodos más modernos como DES, 3DES y AES. [34]. La velocidad de encriptación y las claves de tamaño relativamente pequeño son sus principales ventajas. Sin embargo, su mayor desventaja es la distribución de la clave ya que ambas partes deben poder compartirla por algún canal seguro. Esto implicaría que el financiador debería generar y asignar una clave a cada entidad usuaria del sistema y cada vez que sea necesario cambiarla, lo cual no es una solución escalable.

El trabajo de Whitfield Diffie y de Martin Hellman [35] permitió el desarrollo de los sistemas de criptografía asimétrica o algoritmos de clave pública como una solución a las dificultades de distribución de la clave de los algoritmos simétricos. En este caso, cada usuario del sistema posee dos claves que están matemáticamente relacionadas: una de ellas es pública y la otra debe mantenerse en secreto. El mensaje será encriptado por una de las claves y desencriptado con la otra. Agregar un nuevo usuario al sistema, ya sea un nuevo prescriptor o una nueva farmacia, requiere la generación de solo un par de claves y la eliminación de un usuario, por ejemplo, cuando cesa el contrato con un profesional o una farmacia, se realiza por un mecanismo de revocación de claves. De esta manera no es necesario intercambiar claves secretas previamente para que un usuario pueda enviar o recibir datos encriptados de las prescripciones.

Los algoritmos de encriptación asimétrica son mucho más lentos que los simétricos. En una prueba realizada con el comando *openssl* en la computadora del autor, se compararon las velocidades de encriptación del algoritmo simétrico AES-128 en modo CBC[7] y del

[7] Chipher Block Chaining. Un modo de funcionamiento de los algoritmos de encriptación en el cual si se encripta el mismo texto de entrada en forma repetida se obtiene un mensaje cifrado diferente. Esto se obtiene al realizar la operación lógica OR exclusivo entre cada bloque del mensaje y el bloque cifrado anterior. [34, p. 183]

algoritmo asimétrico RSA. El primero procesó más de 100 millones de bytes por segundo en bloques de 1024 bytes, mientras que el segundo logró realizar 548 firmas por segundo.

```
openssl speed aes-128-cbc
openssl speed rsa2048
```

Figura 4 Comandos openssl para verificar las velocidades de los algoritmos de encriptación

Algoritmo	16 bytes	64 bytes	256 bytes	1024 bytes	8192 bytes
aes-128-cbc	94977.07	104234.13	105074.21	107323.05	104854.87

Tabla 2 Velocidad de encriptación de un algoritmo simétrico para distintos tamaños de bloques. Los valores están expresados en miles de bytes por segundo

Algoritmo	Firmar	Verificar	Firmas/s	Verificaciones/s
RSA 2048 bits	0.001825s	0.000056s	548.0	17859.6

Tabla 3 Velocidad de encriptación de un algoritmo asimétrico

Es por esto que los algoritmos asimétricos no son utilizados para encriptar los datos, sino que para el diseño de este sistema se empleará un esquema híbrido para encriptar el contenido de las prescripciones electrónicas que serán enviadas al servicio. Primero, el cliente generará una clave simétrica secreta llamada “clave de sesión”. Luego, el cliente encriptará esta clave por medio de un algoritmo de encriptación asimétrico con la clave pública del servicio, que podrá descargar desde el servidor del financiador. La clave de sesión encriptada será enviada al servidor como parte de la llamada al sistema. Solo el servicio podrá desencriptar la clave de sesión con su clave privada. Luego, el cliente encriptará el contenido de la prescripción médica con la clave de sesión y la enviará en el contenido de una llamada al servicio. Por último, el servicio podrá desencriptar la información de la prescripción con la misma clave de sesión. Finalizada la transacción, la clave de sesión se descarta.

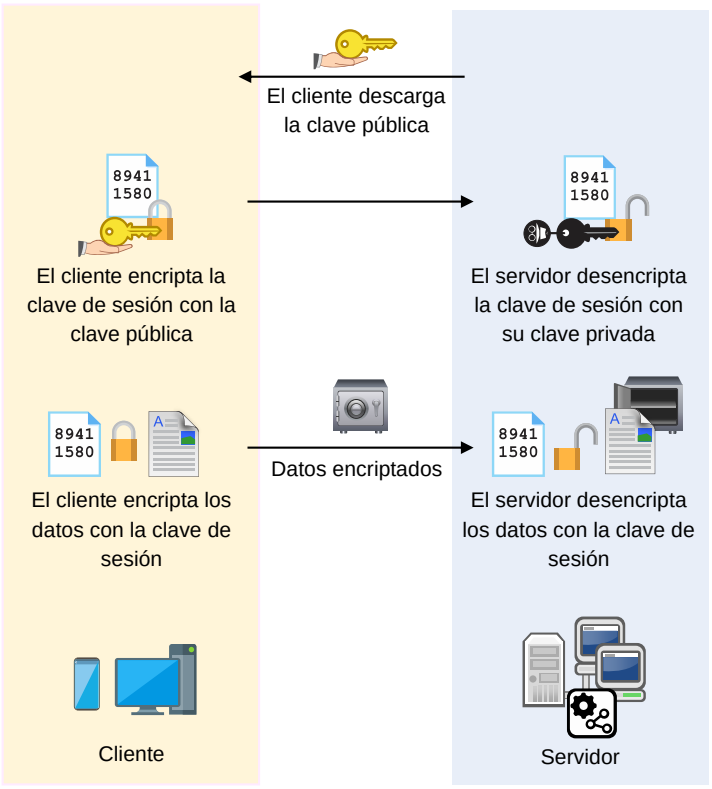

Figura 5 Encriptación y desencriptación de datos con una clave de sesión compartida

Para la implementación se utilizarán las librerías provistas por el lenguaje de programación elegido. Por ejemplo, en *Javascript* se puede usar *Web Crypto API* que es una interfaz que permite utilizar primitivas criptográficas y está implementada por los navegadores. Las aplicaciones web podrán realizar operaciones criptográficas, como firma digital, encriptación y desencriptación. Actualmente es una recomendación de la W3C[8] [36].

```
async function encriptarMensaje(clave, mensaje) {
    let enc = new TextEncoder();
    let encodedMessage = enc.encode(mensaje);

    let textoCrifrado = await window.crypto.subtle.encrypt(
        {
            name: "RSA-OAEP"
```

[8] *World Wide Web Consortium*

```
            },
            clave,
            encodedMessage
      );

      let buffer = new Uint8Array(textoCrifrado);
      return buffer;
}

async function desencriptarMensaje(clave, textoCrifado) {
      let textoPlano = await window.crypto.subtle.decrypt(
            {
                  name: "RSA-OAEP"
            },
            clave,
            textoCrifado
      );

      let dec = new TextDecoder();
      let mensaje = dec.decode(textoPlano);
      return mensaje;
}
```

Figura 6 Ejemplo de funciones para encriptar y desencriptar mensajes

Este ejemplo hace uso de las funciones *encrypt* y *decrypt* [37]. Para la primera se utiliza la clave pública mientras que para la segunda, la clave privada; ambas son objetos de tipo *CryptoKey*. El siguiente es el ejemplo de invocación a estos métodos:

```
let cifrado = await encriptar (publicKey, mensaje);

let decifrado = await desencriptar (privateKey, cifrado);
```

Figura 7 Ejemplo de llamada a los métodos encriptar y desencriptar

Identificación y firma digital

Como se vio anteriormente, la criptografía de clave pública permite a dos usuarios que no se conocen de antemano comunicarse de forma segura sin necesidad de contar previamente con una clave secreta compartida. Sin embargo, cada usuario no tiene forma de conocer la identidad del otro usuario; solo puede conocer su clave pública. No hay ninguna asociación entre esta clave pública y la identidad del usuario. Para asegurarse que la clave pública de un usuario es genuina y no ha sido reemplazada por las de un atacante,

estas se publican en un documento llamado “certificado digital” [38]. Cada certificado almacena, además del par de claves de un usuario, datos de identificación del propietario de las claves, el período de validez del certificado y los datos de la entidad que lo emitió.

Varios servicios de seguridad serán provistos por una infraestructura de clave pública (PKI[9]). El glosario de seguridad de internet (RFC 4949) define a la infraestructura de clave pública como “el conjunto de hardware, software, personas, políticas y procedimientos que son necesarios para crear, administrar, almacenar, distribuir y revocar los certificados digitales basados en criptografía asimétrica.” [39].

Para validar la identidad de prescriptores y farmacias se requiere el uso de una autoridad certificante (CA[10]) que emitirá los certificados digitales. El financiador será quien implementará la CA debido a que tiene todos los medios para producir la identificación de los prescriptores: para que un prestador sea autorizado para trabajar para el financiador previamente se celebra un contrato de prestación de servicios. Como parte de los requisitos para ser contratado como prestador, el profesional debe suministrar la documentación necesaria para corroborar su identidad, título profesional habilitante, título de especialización, certificado de matriculación, inscripción fiscal y seguro de mala praxis entre otros. Esta documentación brinda al financiador la posibilidad de asegurar que el profesional está habilitado para realizar una prescripción médica y además cuenta con la potestad de revocar esta autorización en caso de rescisión del contrato de servicios o de incumplimientos. Por estos motivos será quien emita los certificados digitales a los prescriptores y quien podrá revocarlos en caso de ser necesario.

[9] Public Key Infraestructure
[10] Certificate Authority

El financiador implementará la generación y distribución segura de certificados digitales para validar la identidad de los prescriptores. El mismo prescriptor podrá generar su propio certificado en la plataforma de servicios y podrá descargarlo a su computadora. A continuación, deberá instalarlo en el almacén de certificados de su sistema protegido por un PIN[11] o, aquellos que lo posean, en un dispositivo criptográfico portátil o *smart card*. Cada vez que sea necesario acceder a la clave privada del certificado digital, el prescriptor deberá escribir el PIN.

Autenticación

Para poder utilizar el sistema de prescripción médica electrónica, tanto los profesionales como los dispensadores deberán autenticarse para que así se pueda establecer la identidad del usuario y realizar el control de acceso. El RFC 4949 define a la autenticación de usuarios como el proceso de verificar una identidad pretendida por una entidad del sistema [39]. La autenticación de los usuarios es una operación crítica de seguridad que, si no está implementada de forma segura, presenta riesgos que pueden permitir suplantación de identidad y accesos fraudulentos.

En primer lugar, el financiador de servicios de salud proveerá de cuentas de usuario a los prescriptores como también a los proveedores de medicamentos, previa validación de su identidad y de la validez del contrato de servicios. La cuenta de usuario será el identificador digital único de cada uno de ellos.

Para aumentar la seguridad del proceso de autenticación se requerirá el uso de dos factores de autenticación. El primero será una clave memorizada por el usuario y el segundo estará basado en la posesión un elemento de autenticación. La clave del usuario deberá tener cierta complejidad que haga que adivinarla sea impráctico para

[11] Número de identificación personal

un atacante. Siguiendo las recomendaciones del Instituto Nacional de Estándares y Tecnología de Estados Unidos, la clave deberá tener un mínimo de 8 caracteres y un máximo de 64, y se deberán aceptar caracteres ASCII, incluido el espacio y caracteres especiales [40]. Esta clave será generada por el usuario, pero deberá superar un control de complejidad. Por ejemplo, se podrá evitar que el usuario utilice caracteres repetidos o en secuencia, o claves similares al nombre de usuario. También se podrá comparar la clave propuesta con listas de claves conocidas o que hayan sido comprometidas [41]. Del lado del servidor se almacenarán los nombres de usuarios y un hash de las claves. Se utilizará además un valor de *salt* aleatorio para agregar complejidad al hash y evitar posibles ataques [42].

Comentado [LO1]: ¿Hace falta describir qué es el salt?

El segundo factor de autenticación será provisto por un algoritmo generador de claves únicas basadas en tiempo (TOTP[12]). Este algoritmo se basa en una clave simétrica conocida solo por el sistema y el usuario, y un contador de tiempo que se calcula de la siguiente manera:

$$T = (\text{Hora actual} - T_0) \ / \ X$$

Donde:

T_0 es un contador inicial de tiempo,

X es el intervalo de tiempo, en segundos, que indica la frecuencia de generación de claves,

T es un valor entero de 64 bits que indica la cantidad de intervalos de X segundos que transcurrieron desde el valor T_0 inicial.

Los valores de T_0 y X están predefinidos.

[12] Time-based One-time Password Algorithm

Al resultado del cálculo se le aplica la función *Floor*[13].

Luego se calcula un hash del contador de tiempo con T como clave –la clave T varía cada X segundos– de la siguiente manera:

```
TOTP(K, T) = Truncar(HMAC-SHA1(K, T))
```

Donde:

K es la clave simétrica secreta compartida entre el servicio y el usuario,

T es el contador de tiempo calculado anteriormente,

HMAC-SHA1 es el algoritmo SHA1 utilizado para el cálculo del hash, definido en el RFC 2104 [43],

Truncar es una función que convierte el valor dado en un valor de 6 dígitos que el usuario pueda utilizar que consiste en un truncado dinámico y una reducción para poder extraer un valor de 32 bits a partir del resultado del hash que tiene 160 bits. Esta función está definida en el RFC 4226 [44, p. Sección 5.3]. Básicamente consiste en realizar la división módulo 1000000 –para obtener valores de hasta 6 dígitos como máximo– de una porción de 32 bits del hash.

La clave obtenida será utilizada por el usuario para completar su autenticación luego de ingresar su nombre de usuario y su clave secreta.

El proceso comienza con la registración del usuario. Este deberá utilizar su dispositivo móvil para generar las claves dinámicas a través de una aplicación de autenticación de segundo factor provista por el financiador u otra disponible. Algunos ejemplos de estas son *Google Authenticator*, *Microsoft Authenticator*, *Authy*, *Duo Mobile* y

[13] Función que devuelve el mayor valor entero menor o igual al valor real de la entrada.

FreeOTP. El portal de servicios generará una clave simétrica compartida que será utilizada por la aplicación para generar las claves de un solo uso. Para facilitar el ingreso de esta clave, se representará en un código QR que será leído por la aplicación del dispositivo.

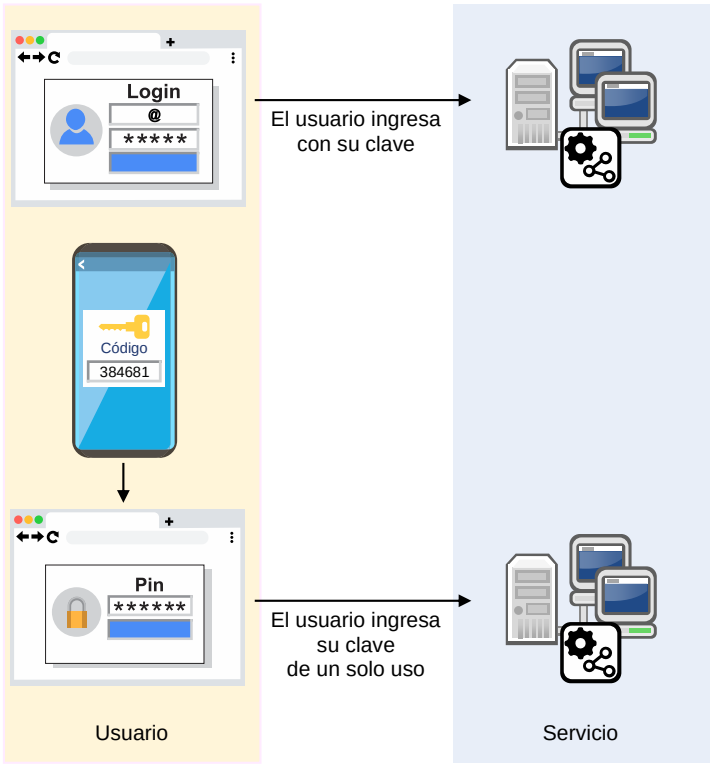

Figura 8 Esquema del inicio de sesión con un segundo factor de autenticación

Figura 9 Configuración de la aplicación de autenticación

A partir de ese momento, la aplicación de autenticación de segundo factor comenzará a generar códigos de seis dígitos que cambiarán cada 30 segundos.

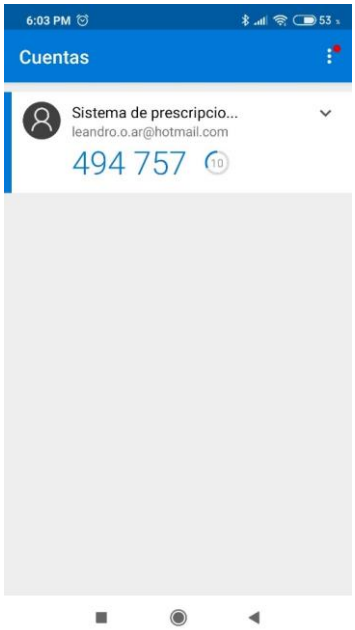

Figura 10 Código generado por la aplicación de autenticación de segundo factor

Por último, el código generado será ingresado en el navegador por el usuario para poder acceder a la plataforma de servicios para realizar prescripciones médicas. El proveedor de servicio validará el código ingresado y realizará el mismo cálculo con la hora actual y la clave secreta compartida con el usuario como entrada.

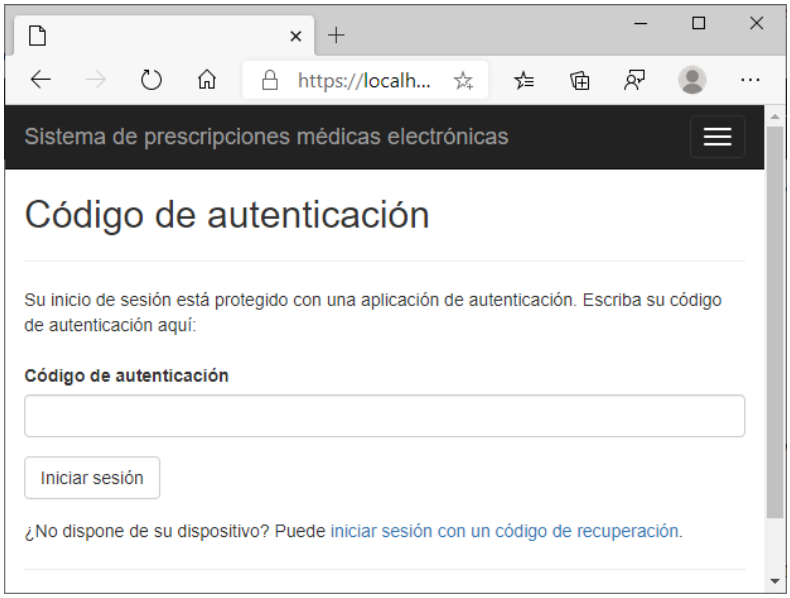

Figura 11 Inicio de sesión con código de autenticación

La ventaja principal es la mejora en la seguridad del inicio de sesión. No se envía ninguna información entre la aplicación que genera los códigos de autenticación y el servicio; es decir que no se necesita conectividad para generar los códigos de segundo factor de autenticación. La clave compartida con el usuario está almacenada en el dispositivo y nunca sale de allí.

El éxito del proceso de generación de claves de segundo factor depende del hecho que los relojes del sistema y del dispositivo del usuario estén sincronizados. Dado que el reloj del servidor estará sincronizado con una fuente externa segura de tiempo y que el reloj del dispositivo del usuario estará sincronizado con la red celular se minimizarán las diferencias. De todas maneras, el proceso de validación del código de autenticación del lado del servidor tomará en cuenta posibles discrepancias entre los relojes y dará como válidos los códigos de autenticación generados 30 segundos antes y 30 segundos después.

El método de generación de claves por TOTP es más seguro que el uso de mensajes SMS como segundo factor de autenticación [45] debido a las vulnerabilidades de la compañía y de la red celular.

Comunicaciones seguras

Otro requisito es la seguridad en las comunicaciones entre un usuario y el portal de servicios. Esto se logrará con el uso del protocolo HTTPS[14] [46]: es el protocolo HTTP por sobre el protocolo TLS[15].

El protocolo garantiza la confidencialidad de la información. Por medio de la utilización de una clave secreta compartida se provee encriptación de la comunicación. Además, el protocolo brinda integridad de los mensajes ya que utiliza un código de autenticación de mensajes (MAC[16]). Por último, también se realiza la autenticación del servidor. Esto significa que el usuario, cuando se conecta al servicio, tendrá la seguridad de que está conectado al servidor real y no a uno falso: los atacantes no pueden suplantar el servicio.

El financiador deberá adquirir un certificado digital comercial en un proveedor reconocido y deberá instalarlo en el servidor web. Se aconseja el uso de un certificado TLS de 2048 bits.

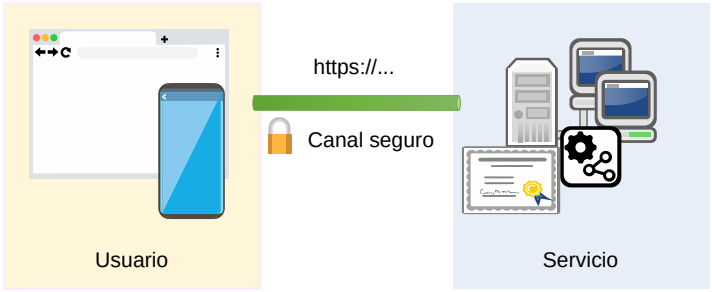

Figura 12 Acceso a un servicio web a través de un canal seguro https

[14] Hypertext Transfer Protocol Secure
[15] Transport Layer Security
[16] Message Authentication Code

Permisos de acceso y autorización

El sistema de prescripciones médicas propuesto implementará la asignación de permisos y privilegios de los usuarios mediante el patrón “control de accesos basado en roles”. Este consiste en asignar a los usuarios los permisos y derechos de acceso al sistema según sus roles o funciones. De esta forma, se vinculan los permisos a los roles y estos son asignados a los usuarios según su función [47].

Se asimila un rol a una función que tiene ciertas atribuciones y puede visualizarse como la relación entre los usuarios y los permisos. Se puede dar uno o varios roles a cada usuario, y este usuario recibe así los permisos definidos en esos roles. Los permisos constituyen las operaciones que se autorizan realizar sobre un objeto. Por cada función que ejecute, el servicio verificará que el usuario que ha iniciado la sesión posea al menos uno de los roles que tienen permiso para ejecutar dicha función.

Figura 13 Esquema relacional del modelo de permisos

La asignación de privilegios por medio de este patrón permite que solo las personas autorizadas puedan acceder a la información sensible del paciente. El administrador del sistema define los roles, los permisos y se asignarán a los usuarios basados en una política de privilegios que define qué usuarios pueden desempeñar esos roles. El sistema de prescripciones contendrá la lógica para aplicar la política definida en función del usuario que inicia sesión.

Por cada llamada a las funciones *API* el sistema determinará si el usuario tiene el privilegio necesario según las reglas establecidas para realizar la acción. Por ejemplo, se definirá el rol “médico” con el permiso de “prescribir medicamento”. Cualquier usuario que posea ese rol podrá realizar la acción de prescripción [48].

En la siguiente tabla se enumeran algunos permisos posibles:

Permiso	Descripción
Prescribir	Prescribir un medicamento.
Modificar prescripción	Alterar una receta ya realizada.
Cancelar prescripción	Anular una prescripción ya emitida.
Prescribir sustancias controladas	Prescribir drogas que tienen un régimen especial por su acción farmacológica, como psicofármacos, ansiolíticos, etc.
Prescribir drogas de alto costo	Prescribir drogas que tienen un régimen especial por su costo, como drogas para trasplantes, HIV, oncológicas, etc.
Autorizar	Autorizar una prescripción.
Rechazar	No autorizar una prescripción.
Cancelar autorización	Revertir el estado de autorización de una prescripción
Autorizar recetas expiradas	Autorizar una prescripción cuando ya ha superado el período de validez.
Anular prescripción	Cancelar una prescripción.
Cambiar nombre comercial	Modificar una prescripción. Cambia el nombre comercial de un producto que tenga el mismo principio activo.
Escribir observaciones	Escribir una leyenda que se adjunta a la prescripción.
Modificar observaciones	Modificar la leyenda.
Enviar prescripción	Poner una prescripción a disposición de cualquier proveedor o farmacia a elección del paciente.
Ver prescripciones pendientes	Visualizar prescripciones realizadas a pacientes.
Asignar prioridad	Cambiar la prioridad de una prescripción.
Asignar a usuario	Para realizar el tratamiento administrativo de la prescripción, asignándola a un usuario particular.
Asignar proveedor	Poner una prescripción a disposición de un único proveedor o farmacia.
Modificar proveedor	Cambiar el proveedor ya asignado a una prescripción.
Dispensar	Proveer o vender un medicamento recetado.
Facturar	Marcar una prescripción como lista para su cobro.

Tabla 4 Permisos más importantes

En la siguiente tabla se enumeran algunos roles posibles:

Nombre	Descripción
Médico	Puede prescribir medicamentos, enviar prescripciones al financiador o al proveedor. Se pueden definir roles más específicos según la necesidad del financiador, como Especialistas, Diabetólogo, Oncólogo, etc., que puedan tener permisos para prescribir un subconjunto más específico de medicamentos.
Dispensador	Asignado a farmacias, droguerías, etc. que están autorizadas a entregar medicamentos.
Médico auditor	Personal del financiador u obra social que se encarga de revisar las prescripciones y autorizarlas (o rechazarlas) según su criterio médico. Puede además modificarlas en caso de ser necesario, o anular prescripciones. Podrá asignar el proveedor toda vez que por cuestiones administrativas o de costo se desee direccionar la dispensa, ya sea a proveedores especializados o aquellos con los que se tenga algún convenio específico.
Personal administrativo	Rol asignado al personal administrativo del sector de auditoría médica. Podrán tener acceso a las prescripciones, asignar prioridad, escribir alguna observación o redirigirlas a algún médico auditor específico.
Administrador	Podrá asignar roles a los usuarios. Definirá los permisos en el sistema de acuerdo con una política de seguridad predefinida.

Tabla 5 Roles posibles

Almacenamiento encriptado

Los datos personales y datos médicos que se encuentren almacenados en cualquier medio deberán asegurarse por medio de métodos de encriptación. Por este motivo será necesaria la utilización de la técnica llamada “encriptación de datos en reposo”.

Los datos en reposo son aquellos que no están en proceso ni en tránsito y que ya han sido grabados en algún almacenamiento persistente [49]. Protegerlos se torna necesario en este sistema para evitar los ataques o el robo de la información que se almacena en texto plano. Incluso puede haber datos replicados, copias de seguridad de las bases de datos y archivos que son copiados a sistemas inseguros que también deben ser protegidos. Hay que tener

especial cuidado también con cualquier tipo de información sensible que pueda estar almacenada en dispositivos de almacenamiento que sean descartados por fallas, por reemplazos o por devolución al fabricante en caso de garantías o reparación.

La encriptación de datos en reposo puede mitigar todos estos riesgos. Incluye aquellos que están almacenados en distintos dispositivos en uso en el financiador, proveedores y en cualquier entidad que pueda tener acceso de alguna manera a la información sensible. Se puede implementar mediante la encriptación total de discos o dispositivos, a nivel de archivos, de aplicación, de bases de datos y de los sistemas de almacenamiento.

Encriptación total de discos

Encriptar todo el almacenamiento protege la información contenida en caso de compromiso del dispositivo o de los sistemas de almacenamiento. Consiste en encriptar todos los datos para que no puedan ser accedidos al montar el disco o dispositivo en otro sistema. Una vez que el usuario se identifica, se puede acceder de forma transparente a los datos como si no estuvieran encriptados. Generalmente se incluye también el disco de arranque del sistema y el sistema operativo [50].

El extravío o robo de computadoras portátiles o unidades USB con información sensible que no está encriptada es una forma frecuente de pérdida de la confidencialidad. En 2019, el Centro Médico de la Universidad de Rochester, en Estados Unidos, acordó pagar una multa de 3 millones de dólares a la oficina de Derechos Civiles de Estados Unidos luego de que sea descubierta la pérdida de una unidad *flash* sin cifrar y el robo de una computadora portátil sin cifrar que contenían información médica confidencial [51].

En sistemas Windows, el producto utilizado es BitLocker. La versión BitLocker To Go también permite encriptar dispositivos removibles [52].

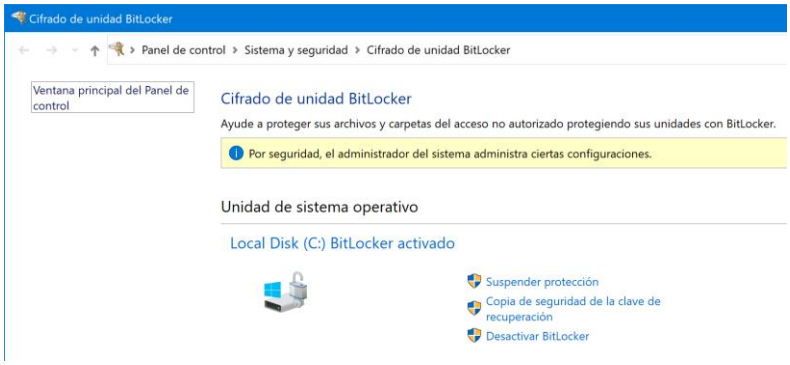

Figura 14 Configuración de la utilidad BitLocker en Windows 10 para encriptar un disco local

Para garantizar la seguridad de los datos contenidos en este sistema de prescripción médica electrónica el administrador debería utilizar alguna solución de encriptación de disco para cualquier dispositivo, servidor o computadora que almacene información sensible de las personas. Es también de vital importancia aplicar encriptación completa de unidades de almacenamiento removibles que puedan contener información sensible de pacientes y prescripciones médicas.

Encriptación a nivel de aplicación

La encriptación a nivel de capa de transporte para asegurar el medio de comunicación, brindada por el protocolo TLS, no es suficiente para asegurar la privacidad de la información que se envía y recibe. Cualquier configuración incorrecta del protocolo o problema con los certificados puede poner en riesgo la seguridad de la información transferida, además de que probablemente los datos estén protegidos solo hasta el punto de terminación HTTPS, dejándolos en texto plano en parte de la red del servidor.

Tampoco se puede confiar ciento por ciento en la seguridad de la capa de transporte ya que las bases de datos, los *backups* o *logs* pueden contener la información en texto plano si no son protegidos o diseñados correctamente.

La encriptación a nivel de la aplicación permite mitigar el riesgo de fugas de información ya que los datos se cifran dentro de la aplicación y así no se dependerá exclusivamente de la seguridad de la capa de transporte. De esta forma se protegen los datos en las capas inferiores. El sistema de prescripciones deberá utilizar la técnica de encriptación del lado del cliente y se podrán cifrar ciertos campos que se consideren sensibles y así enviarlos encriptados al servicio.

El agregado de esta otra capa de seguridad en el sistema de recetas médicas permite aplicar un enfoque de defensa en profundidad: si la protección de la capa de transporte falla o se produce algún compromiso del servidor o de la base de datos, los datos sensibles continuarán protegidos. Si además se combinan con las otras técnicas descriptas en esta sección, se podrá reducir de forma considerable la superficie de ataque a los datos sensibles.

En una aplicación cliente se pueden realizar operaciones criptográficas utilizando por ejemplo la interfaz *Web Crypto API* para encriptar campos con información sensible que luego se enviarán como solicitud al servicio web de la aplicación de prescripción médica. Del lado servidor, se pueden utilizar las librerías de criptografía de *.NET Framework* o el módulo *crypto* de *Node.JS*.

El siguiente código en JavaScript crea una clave de sesión aleatoria, luego la utiliza para encriptar un texto plano que podría corresponder al contenido de una receta por ejemplo o cualquier otro campo con información sensible. La clave de sesión es exportada y encriptada con la clave pública del destinatario (el servicio web). Por último, la función devuelve la clave de sesión y el texto, ambos cifrados (adaptado de [53]).

```
async function encrypt(textoPlano, clavePublica) {
   var claveSesion, datosCifrados;
   const clave = await window.crypto.subtle.generateKey(
      {
         name: "AES-CBC",
         length: 128,
      },
      true,
      ["encrypt", "decrypt"] // Usos posibles de la nueva clave
   );

   // Guardar la clave de sesión en una variable
   claveSesion = clave;
   const claveSes = clave;

   // Vector de inicialización
   var iv = window.crypto.getRandomValues(new Uint8Array(16));
   // Encriptar el texto plano con la clave simétrica
   const ciphertext = await window.crypto.subtle.encrypt(
      {
         name: "AES-CBC",
         iv: iv, // Vector de inicialización
      },
      claveSes,
      textoPlano // Texto plano a encriptar
   );
   const ivMasTextoCrifrado = await [iv, new Uint8Array(cipher
text)];
   // Guardar el objeto devuelto anteriormente en una variable
   datosCifrados = ivMasTextoCrifrado;
   // Exportar la clave de sesión
   const claveExportada = await window.crypto.subtle.exportKey
   (
      "raw",
      claveSesion
   );
   // Encriptar la clave de sesión con la clave pública
   const claveEncriptada = await window.crypto.subtle.encrypt(
      { name: "RSA-OAEP" },
      clavePublica,
      claveExportada
   );
   // Crear y devolver un objeto con los datos encriptados
   var largo = new Uint16Array([claveEncriptada.byteLength]);
   return new Blob(
      [
         largo,
         claveEncriptada,
         datosCifrados[0],
         datosCifrados[1], // Texto crifrado
      ],
      { type: "application/octet-stream" }
   );
}
```

Figura 15 Ejemplo de una función en el cliente que encripta un texto plano con una clave de sesión obtenida a partir de una clave pública

Encriptación de base de datos

Los datos de las prescripciones médicas, de los pacientes que las reciben y en general de todo tipo de información médica sensible relacionada serán almacenados en una o más bases de datos relacionales. La información en reposo será protegida por el motor de bases de datos mediante la aplicación de reglas de control de acceso. Sin embargo, si el administrador de la base de datos o incluso un atacante lograra acceder a los datos en crudo de la base de datos, a los archivos físicos o a las copias de seguridad, podría saltearse las políticas de acceso.

Es por ello que la encriptación de la base de datos del sistema constituye otra capa más de seguridad en el esquema de "defensa en profundidad". Consiste en utilizar algún método de cifrado para encriptar el texto plano de una base de datos [54]. De esta forma solo los usuarios o sistemas autorizados que tengan acceso a la clave podrán leer los datos. También se protegen los *backups* en caso de robos o accesos indebidos.

Dependiendo del motor de base de datos utilizado, se podrá implementar alguna tecnología de encriptación soportada. *Transparent data encryption* (TDE) permite encriptar los datos almacenados en una base de datos. Las páginas de la base de datos se encriptan antes de escribirse y se desencriptan cuando son leídas. Cuando un usuario autorizado accede a la información, el motor de base de datos se encarga de desencriptarla de forma transparente. La principal ventaja es que no se requiere realizar modificaciones en la estructura de las tablas ni en las aplicaciones. TDE está disponible en productos de base de datos de Microsoft, IBM, Oracle y en algunas versiones comerciales de MySQL.

Por ejemplo, Microsoft SQL Server utiliza una clave maestra única por cada servidor que se utiliza para cifrar las claves maestras de cada una de las bases de datos. A su vez, estas se utilizan para encriptar las claves privadas de los certificados de cada base de datos.

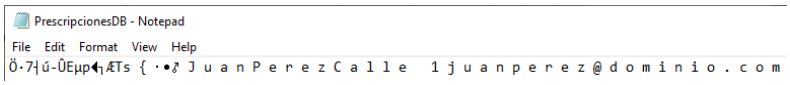

Figura 16 Contenido de una base de datos Microsoft SQL en texto plano, visualizado en un editor de textos

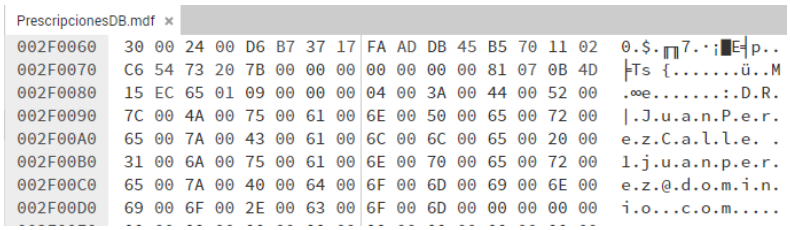

Figura 17 Contenido de la base de datos Microsoft SQL en texto plano, visualizado en un editor binario

Los siguientes comandos SQL muestran cómo activar *Transparent Data Encryption* en una base de datos. Primeramente, se crea la clave maestra con una contraseña. Luego se crea el certificado con el que se encriptará la clave de la base de datos. A continuación, se crea la clave de encriptación de la base de datos con el certificado anterior y por último se activa TDE en la base de datos.

```
USE master;
GO

--Crear una clave maestra con una contraseña compleja.
CREATE MASTER KEY ENCRYPTION BY PASSWORD = 'L7%$#c_/P)á_r2K5f1';
GO

--Crear un certificado. Se especifica un nombre.
CREATE CERTIFICATE TransparentDataEncryptionCert
   WITH SUBJECT = 'Transparent Data Encryption Certificate';
GO

USE PrescripcionesDB;
GO

--Crear una clave de encriptación de una base de datos. Se
especifica el algoritmo y el certificado a utilizar.
CREATE DATABASE ENCRYPTION KEY
```

```
   WITH ALGORITHM = AES_128
   ENCRYPTION BY SERVER CERTIFICATE TransparentDataEncryptionCert;
GO

--Se activa la encriptación de la base de datos.
ALTER DATABASE PrescripcionesDB SET ENCRYPTION ON;
```

Figura 18 Comandos para activar Transparent Data Encryption en una base de datos

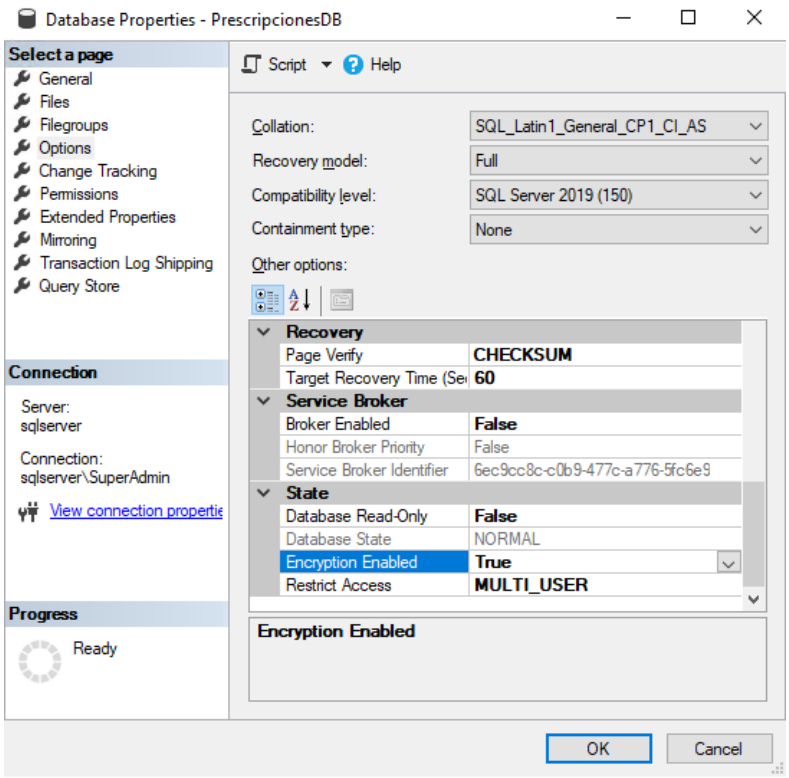

Figura 19 Las propiedades de la base de datos muestran que la encriptación está activada

Una vez activada la encriptación de la base de datos y siempre y cuando las claves y los certificados estén disponibles, se pueden realizar consultas SQL de la misma manera que se hacía antes de activarla. No es necesario modificar las aplicaciones ni los procedimientos almacenados.

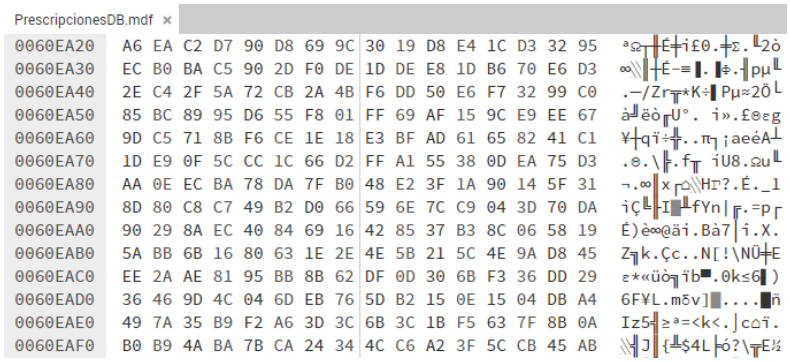

Figura 20 Contenido encriptado de la base de datos Microsoft SQL, visualizado en un editor binario. El espacio vacío también está cifrado.

Aplicación móvil

El financiador de servicios de salud proveerá una aplicación móvil para los usuarios y para sus afiliados que les brindará acceso a los datos de las prescripciones de medicamentos que estén realizadas a su nombre. El usuario utilizará la aplicación para visualizar los datos de las recetas y para realizar la compra de los medicamentos en el proveedor elegido.

Primeramente, la aplicación deberá permitir al usuario generar su nombre de usuario y contraseña para poder acceder. El usuario comenzará el proceso al escribir su número de afiliado o cliente y su número de documento de identidad. Luego de validar estos datos, la aplicación presentará un conjunto de preguntas de seguridad con varias opciones de respuesta, que el usuario deberá contestar correctamente para validar su identidad. Su domicilio particular, número de teléfono, cantidad de miembros en su grupo familiar o fecha de nacimiento son algunos ejemplos de preguntas.

Seguidamente, el usuario procederá a generar su clave de acceso y la aplicación impondrá un criterio de complejidad mínima que deberá tener la clave seleccionada.

La función principal de la aplicación será mostrar un listado de prescripciones médicas activas que el usuario haya recibido por parte de algún profesional de salud. Para poder retirar la medicación recetada el usuario mostrará a su proveedor de confianza un código QR que generará la aplicación. Este contendrá el número de identificación de la receta que será utilizado por el agente de dispensa para acceder a los datos de la receta que el usuario desea retirar.

Figura 21 Ejemplo de código QR generado para una receta electrónica

Otros elementos de seguridad

La seguridad del sistema puede ser ampliada con otros elementos para evitar o mitigar ataques. El financiador de servicios podrá reducir la superficie de ataque con la utilización de infraestructura de red segura y segmentación de la red. Deberá diseñar políticas de protección contra *malware*, actualizaciones de sistemas operativos, software y antivirus, copias de seguridad de bases de datos y documentos, manejo seguro de contraseñas, monitoreo de actividad a través de registros de eventos y *logs*. El equipo de desarrollo deberá estar capacitado en desarrollo de código seguro. Tampoco deberá descuidar la concientización de su personal

en aspectos relacionados a amenazas informáticas, las políticas implementadas y mejores prácticas de seguridad informática.

Conclusiones

Por medio de la adopción de un sistema de prescripciones electrónicas, el financiador de servicios de salud buscará optimizar los procesos de provisión de medicamentos, auditoría y liquidación a los proveedores. Como se describió, este sistema podría reducir el volumen de trabajo administrativo, acelerar los tiempos de facturación de las farmacias, mejorar la seguridad del paciente y facilitarle la obtención de sus medicamentos.

En este trabajo se han enumerado las ventajas principales de un sistema de recetas electrónicas y se han contribuido ideas sobre su diseño y sus potenciales beneficios. También se han analizado los riesgos de la seguridad de la información con sus posibles acciones de mitigación. Es evidente que, con un correcto diseño, las ventajas sobrepasan los riesgos. Estas serán incluso mayores si este sistema se pudiera integrar con aquellos que administran los datos de salud de las personas, sus prácticas diagnósticas y sus historias clínicas. De esta forma la información de prescripciones se podrá relacionar con la de salud, ambiente, historial médico y prestacional.

Los costos en tiempo y monetarios que podrían demandar el diseño y programación de un sistema como el descripto aquí podrán rendir sus frutos al brindar un beneficio para los pacientes, los profesionales médicos, las farmacias y la obra social o prepaga.

Como resultado de este análisis se puede determinar que el diseño de este sistema y su implementación requieren que se consideren todos los aspectos enumerados relacionados a la seguridad de la información altamente sensible que se administra. Seguramente se enfrenten dificultades en su implementación. El tiempo y costo de desarrollo, pruebas y de capacitación a personas no técnicas puede ser muy alto y es posible que se produzcan considerables resistencias.

La amplitud geográfica del país podría ser una barrera. Aquellos profesionales y farmacias ubicados en zonas no favorecidas o que manejen un bajo volumen de prescripciones podrían decidir no utilizar este sistema y preferir continuar con el sistema tradicional.

Las instituciones de salud muy grandes como centros médicos, sanatorios con muchas especialidades u hospitales de alta complejidad podrían encontrar dificultades en capacitar a todo su personal en el uso de un sistema de recetas digitales. El financiador podría brindar a los prestadores interesados algún estímulo económico, o menores plazos de pago para facilitar su adopción.

Por el contrario, aquellos profesionales independientes o que trabajan en pequeños centros o instituciones de salud quizás no cuenten con asesoramiento técnico adecuado. Por lo tanto, el financiador de servicios que desee implementar este sistema deberá brindar a estos asistencia y capacitaciones.

Asimismo, las distintas capacidades técnicas de los usuarios podrían atentar contra la adopción del sistema. A pesar de que el enfoque dado en este trabajo apunta hacia un sistema accesible a través de páginas web, el uso de certificados digitales que deben ser instalados en el sistema de los usuarios puede introducir dificultades técnicas que requieran del soporte de personal idóneo. La gestión de los certificados, los riesgos que se producen en caso de pérdidas o accesos no autorizados, el trabajo administrativo que supone su reemplazo y el desconocimiento de la importancia de mantenerlos seguros son importantes retos a la seguridad.

Si además se requiere el uso de dispositivos criptográficos para almacenar los certificados digitales, el costo de implementación aumentará. Si este costo debe ser asumido por los profesionales, estos podrían negarse a su adopción. Si, en cambio, la provisión de los dispositivos corre por cuenta del financiador, el costo del sistema

podría tornarlo no viable, sobre todo cuando la cantidad de usuarios sea alta.

Si bien el enfoque ha sido tomado desde el punto de vista de un financiador privado de servicios de salud, este trabajo tiene aplicaciones prácticas para instituciones de salud, otros proveedores de software y el Estado. Para la aplicación en el ámbito público o a nivel provincial o nacional es necesario ampliar el enfoque ya que deberán intervenir los organismos públicos pertinentes y la autoridad certificante deberá ser una entidad de mayor nivel, pero el universo de beneficiarios será mucho mayor.

Quedarán algunos desafíos que no han sido analizados y que escapan a un trabajo con enfoque en la seguridad de la información, como por ejemplo la interoperabilidad con otros prestadores de salud o el uso de sistemas terminológicos estándares para codificar alergias, problemas médicos, antecedentes de salud y otros.

En un futuro muy cercano, con el advenimiento de la telemedicina, el paciente tendrá la posibilidad de realizar consultas médicas por medios virtuales. Incluso, ya hay varias empresas de medicina prepaga que brindan atención médica básica a través de aplicaciones móviles. Sin embargo, si se continúa utilizando el sistema tradicional de recetas médicas en papel, el paciente aún necesita obtenerlas directamente desde el profesional de salud en papel y, por lo tanto, se ve obligado a concurrir personalmente. De esta forma se anulan los beneficios de la atención médica a distancia. Es hora entonces de que los interesados piensen no sí, sino cuándo han de implementar su nuevo sistema de prescripciones médicas electrónicas.

Bibliografía

[1] D. S. Bell, S. Cretin, R. Marken y A. B. Landman, «A Conceptual Framework for Evaluating Outpatient Electronic Prescribing Systems Based on Their Functional Capabilities,» *Journal of the American Medical Informatics Association,* vol. 11, nº 1, p. 60–70, 2004.

[2] Asociación Española de Medicamentos Genéricos, «En Genérico,» 29 mayo 2015. [En línea]. Available: https://www.engenerico.com/como-funciona-una-receta-electronica/. [Último acceso: 1 febrero 2020].

[3] Senado y Cámara de Diputados de la Nación Argentina, *Ley N° 23.660 - Obras Sociales. Régimen de aplicación,* Buenos Aires, 1988.

[4] D. Luna, M. Gomez, M. Martínez von Scheid y L. Garfi, «Sistemas de Prescripción Electrónica,» de *InfoSUIS*, 2001.

[5] Editorial Alfa Beta, «Manual Farmacéutico,» 2019. [En línea]. Available: www.alfabeta.net. [Último acceso: 16 octubre 2019].

[6] Kairos Argentina, «k@iros,» 2019. [En línea]. Available: ar.kairosweb.com. [Último acceso: 16 octubre 2019].

[7] D. Luna, A. Gómez, M. Martínez von Scheidt y L. Garfi, «Sistemas de Prescripción Electrónica,» de *InfoSUIS*, 2001.

[8] Sanatorio Sagrado Corazón, «Seguridad en el uso de medicamentos,» Buenos Aires, 2016.

[9] Organización Mundial de la Salud. Ministerio de Sanidad y Política Social de España, «Estudio IBEAS: Prevalencia de efectos adversos en hospitales de Latinoamérica. Informe de resultados Argentina,» 2007.

[10] V. Ocaña, G. Sánchez Domenech y C. Sánchez, «Errores en el proceso de medicación de pacientes internados en el Hospital Público Materno Infantil de Salta,» *Revista Argentina de Salud Pública,* vol. 8, nº 31, pp. 19-26, 2017.

[11] World Health Organization, «10 verdades sobre la seguridad del paciente,» agosto 2019. [En línea]. Available: https://www.who.int/features/factfiles/patient_safety/en/. [Último acceso: 7 enero 2020].

[12] M. Aitken y L. Gorokhovich, «Advancing the Responsible Use of Medicines: Applying Levers for Change,» 2013.

[13] L. Pastó-Cardona, C. Masuet-Aumatell, B. Bara-Oliván y I. Castro-Cels, «Estudio de incidencia de los errores de medicación en los procesosde

utilización del medicamento: prescripción, transcripción, validación, preparación, dispensación y administración en el ámbito hospitalario,» *Farmacia Hospitalaria,* vol. 33, nº 5, pp. 257-268, 2009.

[14] CareCloud, «14 benefits of e-prescribing,» [En línea]. Available: https://www.carecloud.com/continuum/14-benefits-of-e-prescribing/. [Último acceso: 20 noviembre 2019].

[15] BBC News Mundo, «La mujer que acabó en el hospital por la confusa letra de su médico,» 2019. [En línea]. Available: https://www.bbc.com/mundo/noticias-46824189. [Último acceso: 19 diciembre 2019].

[16] M. Confalone Gregorián, L. Bugna, G. Calle, M. Fontana y G. González Capdevila, «Detección, análisis y prevención en el uso de medicamentos con similitud fonética, ortográfica o de envasado en Argentina,» de *Sesión Pública Ordinaria*, 2009.

[17] D. P. Mundy y D. W. Chadwick, «A System For Secure Electronic Prescription Handling,» de *Second International Conference On The Management Of Healthcare And Medical Technology*, Chicago, Illinois, 2002.

[18] O. Lavieri, «Denunciaron que una farmacia estafó al PAMI por más de $60 millones,» *Infobae,* 7 octubre 2019.

[19] H. Alonso, «Millonario fraude al Ipross: farmacias denunciadas quedan fuera del sistema,» *Diario Río Negro,* 4 junio 2019.

[20] Senado y Cámara de Diputados de la Nación Argentina, *Ley de Derechos del Paciente en su Relación con los Profesionales e Instituciones de la Salud Nº 26529,* 209.

[21] Poder Ejecutivo Nacional, *Ley 17132 - Arte de curar. Texto actualizado,* Buenos Aires, 1967.

[22] Senado y Cámara de Diputados de la Nación Argentina, *Ley 25506 - Firma Digital. Texto actualizado,* Buenos Aires, 2001.

[23] Presidenta de la Nación Argentina, *Decreto Reglamentario de la ley 26529 sobre derechos del paciente en su relación con los profesionales e instituciones de salud.,* Buenos Aires, 2012.

[24] M. Yao, «Your Electronic Medical Records Could Be Worth $1000 To Hackers,» 14 abril 2017. [En línea]. Available: https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/#34f68caf50cf. [Último acceso: 11 febrero 2020].

[25] H. Figge, «Cyber Security Primer for Pharmacists,» *US Pharmacist,* vol. 41, nº 2, pp. 26-28, 17 febrero 2016.

[26] Infosec Institute, «Top Cyber Security Risks In Healthcare,» 2000. [En línea]. Available: https://resources.infosecinstitute.com/category/healthcare-information-security/healthcare-cyber-threat-landscape/top-cyber-security-risks-in-healthcare/. [Último acceso: 16 febrero 2020].

[27] Health Care Industry Cybersecurity Task Force. Public Health Emergency. U.S. Department of Health & Human Services., «Report on Improving Cybersecurity in the Health Care Industry,» 2017.

[28] R. Farley, «Fake Clinton Medical Records,» 16 agosto 2016. [En línea]. Available: https://www.factcheck.org/2016/08/fake-clinton-medical-records/. [Último acceso: 22 febrero 2020].

[29] G. Saldana, «Kaspersky Lab: APT de habla china es sorprendido espiando a organizaciones farmacéuticas,» 23 marzo 2018. [En línea]. Available: https://latam.kaspersky.com/blog/kaspersky-lab-apt-de-habla-china-es-sorprendido-espiando-a-organizaciones-farmaceuticas/12648/. [Último acceso: 9 noviembre 2019].

[30] N. Izrael, «Prognosis For Health Care IoT: Six Predictions For 2019,» 1 marzo 2019. [En línea]. Available: https://www.forbes.com/sites/forbestechcouncil/2019/03/01/prognosis-for-health-care-iot-six-predictions-for-2019/?sh=18e0bc27fddd. [Último acceso: 22 noviembre 2019].

[31] U.S. Department of Health and Human Services, «Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information,» [En línea]. Available: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. [Último acceso: 14 marzo 2021].

[32] Consolidated Technologies, Inc, «Security Threats in HealthCare Systems,» 18 marzo 2019. [En línea]. Available: https://consoltech.com/blog/security-threats-healthcare-systems/. [Último acceso: 14 octubre 2020].

[33] Senado y Cámara de Diputados de la Nación Argentina, *Ley de Protección de Datos Personales Nº 25.326,* Buenos Aires, 2000.

[34] W. Stallings, Cryptography and Network Security, Sexta ed., Pearson Education, Inc, 2014.

[35] W. Diffie y M. E. Hellman, «Privacy and authentication: An introduction to cryptography,» *Proceedings of the IEEE,* vol. 67, nº 3, pp. 397 - 427, marzo 1979.

[36] World Wide Web Consortium, «Web Cryptography API,» 26 enero 2017. [En línea]. Available: https://www.w3.org/TR/WebCryptoAPI/. [Último acceso: 3 marzo 2020].

[37] Mozilla, «Web Crypto API,» 18 marzo 2019. [En línea]. Available: https://developer.mozilla.org/en-US/docs/Web/API/Web_Crypto_API. [Último acceso: 12 marzo 2020].

[38] ISO/ITU-T X.509, «Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,» 2019.

[39] R. Shirey, «Request for Comments 4949 - Internet Security Glossary, Version 2,» 2007.

[40] P. A. Grassi, R. Perlner, E. M. Newton, A. Regenscheid, W. E. Burr, J. P. Richer, N. B. Lefkovitz, J. M. Danker y M. F. Theofanos, «Digital Identity Guidelines: Authentication and Lifecycle Management,» 2017.

[41] D. Miessler, «SecLists,» [En línea]. Available: https://github.com/danielmiessler/SecLists/tree/master/Passwords. [Último acceso: 27 enero 2020].

[42] OWASP Foundation, «Password Storage Cheat Sheet,» [En línea]. Available: https://owasp.org/www-project-cheat-sheets/cheatsheets/Password_Storage_Cheat_Sheet. [Último acceso: 20 enero 2020].

[43] H. Krawczyk, M. Bellare y R. Canetti, «Request for Comments 2104 - HMAC: Keyed-Hashing for Message Authentication,» 1997.

[44] D. M'Raihi, S. Machani, M. Pei y J. Rydell, «Request for Comments 6238 - TOTP: Time-Based One-Time Password Algorithm».

[45] National Institute of Standards and Technology, «Cybersecurity Insights - A NIST blog,» 2016. [En línea]. Available: https://www.nist.gov/blogs/cybersecurity-insights/questionsand-buzz-surrounding-draft-nist-special-publication-800-63-3. [Último acceso: 28 enero 2020].

[46] E. Rescorla, «Request for Comments 2818 - HTTP Over TLS,» 2000.

[47] K. Dae-Kyoo, M. Pooja y G. Priya, «Describing Access Control Models as Design Patterns Using Roles,» de *Proceedings of the 2006 conference on Pattern languages of programs*, Portland, Oregon, USA, 2006.

[48] National Health Service, «RBAC Implementation Mapping for the Electronic Prescription Service Release 2,» Londres, 2010.

[49] R. Ross, V. Pillitteri y K. Dempsey, «NIST Special Publication 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,» 2020.

[50] K. Scarfone, M. Souppaya y M. Sexton, «NIST Special Publication 800-11: Guide to Storage Encryption Guide to Storage Encryption Devices,» 2007.

[51] Oficina de Derechos Civiles (Estados Unidos), «Failure to Encrypt Mobile Devices Leads to $3 Million HIPAA Settlement,» 5 noviembre 2019. [En línea]. Available: https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/urmc/index.html. [Último acceso: 26 noviembre 2019].

[52] Microsoft, «BitLocker,» 26 enero 2018. [En línea]. Available: https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview. [Último acceso: 16 noviembre 2019].

[53] C. Engelke, «Public Key Cryptography in the Browser,» 23 agosto 2014. [En línea]. Available: https://blog.engelke.com/2014/08/23/public-key-cryptography-in-the-browser/. [Último acceso: 28 octubre 2020].

[54] L. Bouganim y Y. Guo, «Database encryption,» *Encyclopedia of Cryptography and Security, Springer,* vol. 978, nº 1-4419-5905-8, pp. 1-9, 2009.

[55] R. A. Sansone y L. A. Sansone, «Doctor shopping: a phenomenon of many themes,» *Innovations in clinical neuroscience,* vol. 9, nº 11-12, pp. 42-46, 2012.

[56] Health Care Industry Cybersecurity Task Force, «Report on improving cybersecurity in the health care industry,» U.S. Department of Health and Human Services, 2017.