LA HISTORIA CLINICA ELECTRÓNICA NACIONAL (HCEN) COMO INFRAESTRUCTURA CRÍTICA

Dra. Esc. María José Viega Rodríguez (*)

1. Introducción

La Agencia para el desarrollo del gobierno de gestión electrónica la sociedad de la información y el conocimiento (AGESIC) entendió prioritario abordar el área de la Salud –como uno de los desafíos del gobierno electrónico- con el fin de aportar una fuerza propulsora para la modernización de los procesos, avanzar en la aplicación de las políticas de gobierno en el área y viabilizar mejoras en la calidad de las prestaciones de salud recibidas por los ciudadanos[1].

(*) **Doctora en Derecho y Ciencias Sociales y Escribana Pública por la Universidad Mayor de la República Oriental del Uruguay (UDELAR). Profesora de Informática Jurídica, de Derecho Informático y de Derecho Telemático en la UDELAR. Gerente de la División Derecho Informático en AGESIC (2017 a la fecha)**. Profesora de Derecho Informático en el Máster de Seguridad de la Información de la Facultad de Ingeniería (UDELAR). Profesora de Ética y Legislación en ORT. Directora de la Dirección de Derechos Ciudadanos de la Agencia para el Desarrollo del Gobierno de Gestión Electrónica y la Sociedad de la Información y el Conocimiento (2009-2015). Asesora en Derecho Informático de la Dirección Ejecutiva (2015 a 2017) (AGESIC) – Presidencia de la República. Directora del Instituto de Derecho Informático de la Facultad de Derecho de la Universidad de la República (agosto 2010- marzo 2013). Coordinadora del Grupo del Jurisprudencia del Instituto de Derecho Informático de la UDELAR (2002 – 2014). Coordinadora y profesora de la Especialización en Derecho Informático (CADE). Coordinadora del Grupo de Jurisprudencia en Derecho y Altas Tecnologías (2015 a la fecha). Posgrado de Derecho Informático: Contratos Informáticos, Contratos Telemáticos y Outsourcing en la Universidad de Buenos Aires. Experta Universitaria en Protección de Datos, UNED (ESPAÑA). Experta Universitaria en Administración electrónica, Universidad Operta de Cataluña (España). Ex - Profesora del curso en línea Derecho del Ciberespacio en la UDELAR. Ex - Profesora de Derecho de las Telecomunicaciones en la Universidad de la Empresa. Ex - Profesora en la Oficina Nacional de Servicio Civil (Presidencia de la República) del Curso Derecho de Internet. Ex - Profesora de los cursos de e-learning “Introducción al Derecho de las TICs”, “Documento y firma electrónica”, “Protección de datos” y “Contratos Informáticos” en Viega & Asociados. Directora del Estudio Jurídico Viega & Asociados (1992-2012). Miembro Honorario de la Asociación Paraguaya de Derecho Informático y Tecnológico (APADIT). Miembro Fundador del Instituto de Derecho Informático (UDELAR) y de FIADI Capítulo Uruguay. Autora del libro “Contratos sobre bienes y servicios informáticos”. Amalio Fernández, junio 2008 y del e-book “Marketing Comportamental en línea. El desafío de las cookies”. 2012 (publicado en www.viegasociados.com). “Derecho Informático e Informática Jurídica I” FCU, octubre 2017. Co-autora de los Libros: Lecciones de Derecho Telemático Tomo I y II (FCU, abril 2004 y mayo 2009); e-book “Documento Electrónico y Firma Digital. Cuestiones de Seguridad en las Nuevas Formas Documentales (junio 2005); “Marco normativo del Derecho Informático” (julio 2011); “Documento y firma. Equivalentes funcionales en el mundo electrónico”. (2012). “Privacidad y tecnología en equilibrio” (2012). “Los derechos ciudadanos en el gobierno electrónico” (2013). “Disrupción, economía compartida y Derecho” (2016). “Derecho Informático e informática Jurídica II” (FCU, 2018). Es autora de múltiples trabajos de su especialidad y conferencista a nivel nacional e internacional.

[1] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/politicas-y-gestion/programas/es-saluduy Página visitada: 5 de marzo de 2021.

El Decreto N° 405/011[2] de 23 de noviembre de 2011, aprobó la Agenda Digital Uruguay 2011-2015, entre cuyos objetivos se encontraba la creación de redes avanzadas para la salud y la HCE integrada a nivel nacional, en el entendido que las Tecnologías de la Información y Comunicaciones tienen un gran potencial para la mejora de la gestión de los servicios de salud.

En el año 2012 se firmó un convenio para llevar adelante la estrategia, entre el Ministerio de Salud Pública (MSP), el Ministerio de Economía y Finanzas (MEF) y la AGESIC, creándose el Programa Salud.uy, cuyo Comité de Dirección comenzó a funcionar el 8 de marzo de 2013.

Por Decreto N° 459/016 de 30 de diciembre de 2016[3], se aprobó la Agenda Uruguay Digital 2020 estableciendo en la Meta N° 8 del Objetivo II la innovación para el bienestar social: "*Alcanzar al 100% de los prestadores integrales de salud con la HCEN incorporada en al menos 3 áreas (emergencia, ambulatorio, internación, quirúrgico u otras), el 100% de los servicios oncológicos públicos y privados con HCE oncológica implementada y disponer de los instrumentos normativos y técnicos que habiliten la prescripción médica electrónica*".

2. Descripción de la infraestructura

El Sistema de Historia Clínica Electrónica Nacional (HCEN) se trata de una herramienta que permite el almacenamiento, transferencia y consulta de información sobre la prestación de servicios de salud y datos clínicos del usuario.

Entre sus cometidos se encuentra promover la continuidad de la atención sanitaria y la calidad del registro a través de la normalización de las estructuras clínicas, así como generar una base sustantiva de información clínica que permita complementar los servicios asistenciales y su prestación a distancia.

Uno de sus principales objetivos es garantizar que la información clínica vital del paciente o usuario esté disponible y accesible para el profesional de la salud, de forma oportuna, segura y en línea.

Durante el año 2015 se puso en marcha el Plan de Adopción, que consistió en la transferencia de los lineamientos y estándares definidos por el programa hacia los equipos técnicos de los prestadores de servicios de salud, así como de los componentes de software para la HCEN.

---

[2] https://www.impo.com.uy/bases/decretos/405-2011
[3] https://www.impo.com.uy/bases/decretos/459-2016

Frente al sistema de HCEN, en la cual la HCE funciona como un sistema federado entre los distintos prestadores de salud, el intercambio de información clínica se convierte en el principal desafío, desde dos puntos de vista: técnico y jurídico. Desde el punto de vista técnico se creó la Red Salud y la Plataforma de Salud, como infraestructura segura que permitiera la conexión de los distintos prestadores, tanto públicos como privados, a los efectos de permitir subir la información y habilitar los accesos. A diferencia de la plataforma de gobierno electrónico, en la cual interactúan solo organismos públicos, la plataforma de salud debería construirse de forma tal que habilitara el ingreso de las instituciones públicas y privadas del área.

Cada prestador de salud tiene su propio repositorio, base de datos o sistema de HCE. La plataforma de salud tiene dos componentes: el registro de personas y el registro nacional de eventos. Cada vez que nosotros consultamos un médico se genera un registro en eventos, independientemente del prestador en el que me atiendo, quedando solo el registro de la consulta, como si fuera el índice de un libro. Todo el contenido de la hoja clínica queda en el sistema de la institución y cualquier médico, en instancia de consulta, puede verla en ese sistema. Un aspecto importante a destacar es que no se está compartiendo información clínica. Cuando se habla de intercambio de información entre prestadores, en realidad la terminología no es correcta, sino que cada prestador pone a disposición la información y lo que se habilita es el acceso a ésta. El acceso ha sido objeto de preocupación y uno los desafíos en relación al sistema, siendo el consentimiento del usuario la regla habilitante, pero existen excepciones legales a éste. Un tema desafiante es la responsabilidad de los prestadores como custodios de la HCE. El sistema se ha concebido para que la información pueda ser visualizada, que el médico la tenga disponible para acceder a ella, pero no está previsto que se descargue. Sin embargo, podría reproducirla de muchas formas, como por ejemplo hacer una captura de pantalla.

En el ámbito jurídico, se aprobaron diversas normas a los efectos de dar soporte legal al sistema. El art. 466 de la Ley N° 19.355 de 30 de diciembre de 2015[4], el Decreto N° 242/017 de 31 de agosto de 2017[5], regulando en forma separada la HCE del Sistema de HCEN. En el artículo 2° literal C) se encuentra definida la Plataforma HCEN como la infraestructura tecnológica y de servicios que permite la conectividad

[4] https://www.impo.com.uy/bases/leyes/19355-2015
[5] https://www.impo.com.uy/bases/decretos/242-2017

de los diferentes sistemas de información del conjunto de Instituciones con competencias legales en materia de salud, públicas y privadas, con el objetivo de intercambiar información clínica. En el literal D) se establece que la Red Salud: "*es una red privada para la conexión de Instituciones con competencias legales en materia de salud, públicas y privadas, a través de la Plataforma HCEN, que permite el intercambio seguro de información de los usuarios del sistema de salud*". En los literales E) y F) se definen los Registros de Personas y Eventos respectivamente. El Registro de personas es el índice de pacientes o usuarios con la finalidad de ser identificados unívocamente dentro de la Plataforma de HCEN. El Registro de eventos es el índice de los documentos clínicos electrónicos generados y almacenados en las Instituciones con competencias legales en materia de salud, públicas y privadas.

En HCEN la garantía de seguridad y confidencialidad está dada porque la información sale del prestador utilizando firma electrónica avanzada de persona jurídica, de la institución. Respecto a la seguridad de las HCE el artículo 12 establece que será responsabilidad de cada Institución dotar de los mecanismos y procedimientos de administración e identificación electrónica a quienes accedan a la HCE. Todo acceso a la HCE debe quedar debidamente registrado y disponible. La información no podrá ser alterada o eliminada sin que quede registrada la modificación de que se trate.

Cada prestador es responsable de la gestión de la seguridad de su información. Por tanto, cada prestador va a gerenciar sus accesos. Es importante que la información sea confidencial, pero también que la información sea íntegra y que esté disponible cuando se necesite.

El artículo 18 establece cuestiones relativas a la gestión de acceso, estableciendo que a los efectos de conectar a la Plataforma y a la Red Salud deberán estar debidamente identificadas electrónicamente, garantizando la autenticación de las personas, así como la privacidad y la integridad de la información clínica intercambiada, de forma que no sea revelada ni manipulada por terceros.

La Ley N° 19.670 de 15 de octubre de 2018, en el art. 194 reitera, con mayor claridad el funcionamiento de la HCEN, el que va a ser reglamentado por el Decreto N° 122/019[6] de 29 de abril de 2019, que permite la gestión de los accesos por parte

[6] https://www.impo.com.uy/bases/decretos/122-2019

de las personas. El artículo 2° regula la seguridad en los procesos y hace remisión a la Ley N° 18.600, de 21 setiembre de 2009[7].

3. ¿Por qué se trata de una infraestructura crítica?

Considero que se trata de una infraestructura crítica -en un sentido amplio- porque refiere a un servicio público esencial, considerándose esenciales aquellos que, si se interrumpe el servicio ponen en riesgo la vida, la seguridad o la salud de la población. La criticidad va a estar dada por el impacto público y social, la cantidad de población afectada y el impacto económico.

En el documento Aportes para una Estrategia de desarrollo 2050, en el Cap. 5 Transformación social, refiere al ámbito de la salud (página 209) y específicamente a la HCEN (página 215) [8].

El sector salud se encuentra contemplado en las Agendas Digitales país, como se hizo mención y también en la nueva agenda 2025, en el área Sociedad Digital inclusiva, Objetivo II, Punto 7) establece: "Profundizar la adopción digital de los servicios de salud, desarrollando prescripciones ambulatorias con receta digital, integrando el resumen de paciente a la HCE y modernizando los procesos de comunicación de la autoridad sanitaria con los profesionales de salud", aprobada por Decreto N° 134/021 de 4 de mayo de 2021[9].

Por otra parte, los datos de salud como activos son muy valiosos, mientras los datos crediticios cambian, cambio la tarjeta de crédito, por ejemplo, los cambios en salud o no se producen o son menores. Esto llevó a que en 2020 el aumento de las fugas de datos de salud en Estados Unidos fuera de un 55%[10].

4. ¿Cómo podría detenerse o interrumpirse la infraestructura a consecuencia de un ciberataque?

Los ciberataques podrían darse de diferente forma, podría atacarse la HCEN para interrumpir el servicio, o podría utilizarse como una herramienta para acceder a las HCE de una determinada institución o de un usuario concreto.

---

[7] https://www.impo.com.uy/bases/leyes/18600-2009

[8] https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/Estrategia_Desarrollo_2050.pdf Página visitada el 3 de agosto de 2021.

[9] https://www.impo.com.uy/bases/decretos/134-2021

[10] Conferencia del Ing. Santiago Paz el 20 de mayo de 2021, disponible en http://itsalud.usuaria.org.ar

a) Accesos no autorizados: el peligro no es que se ingrese a la HCEN, sino que se utilice ésta para ingresar a cualquier institución de salud, desde un lugar que pueda tener una protección débil, como puede ser una policlínica en el interior del país y desde allí puedo acceder a cualquier institución. Por eso, el plan de adopción fue estableciendo niveles, para garantizar la seguridad de los sistemas. Se afecta la confidencialidad de la información y podría afectar también la integridad. Si al acceder se cambia información en una HCE podría incluso producir la muerte de una persona, o sea que el efecto podría no ser solo virtual, sino también físico.
b) Randsomware: afecta la disponibilidad de la información. Podría producirse tanto a nivel de la Plataforma, afectando el Registro de eventos, el de personas o ambos, y también podría ingresarse a través de la HCEN para bloquear HCE.
c) Denegación de servicios: este ataque se puede realizar a través de la contratación de botnets y dejar inoperante la HCEN, de forma tal que sea imposible realizar los accesos a las HCE de los diferentes prestadores. Afectaría la disponibilidad de la información.
d) Fraude de identidad: la suplantación de identidad afectaría la confidencialidad de la información. Aquí el ataque sería contra un prestador de salud, que permitiría el ingreso a su sistema, habilitando por tanto el ingreso a la HCEN y a través de ésta a los otros prestadores.
e) Robo de información: afecta la confidencialidad de la información y puede afectar la disponibilidad de ésta. En este caso pueden plantearse dos situaciones: que me lleve la información, desapoderando a la institución de salud (sería de aplicación el art. 340 del C. Penal que tipifica el hurto) o que realice una copia de la información, en cuyo caso no aplica el art. 340. También podría aplicarse a los registros de personas y eventos de la HCEN.
f) Espionaje: puede ser de utilidad conocer el estado de salud de altos funcionarios del Estado, de los candidatos en las elecciones o de personas públicas, afectando por tanto la confidencialidad.

5. Efecto que tendrían estos ataques en el contexto nacional

Mientras que desconocer quién accedía a mi HC en papel no era una preocupación de la ciudadanía, la posibilidad de acceder a información clínica a través de la HCEN produjo varias movilizaciones, al punto que debió aprobarse el art. 194 de la Ley N° 19.670 y el Decreto N° 122/019, estableciendo la obligatoriedad de las instituciones

de subir la información al registro de personas y al registro de eventos, pero a su vez otorgando el derecho a los usuarios a negarse a que se realicen accesos a través de la HCEN. Por otra parte, se garantizó el acceso a los usuarios al historial de accesos. Si esta desconfianza en el sistema, en el prestador y en los médicos, sucede en un ámbito de normalidad, podría convertirse en una situación compleja cualquiera de las violaciones a la confidencialidad referenciadas en el punto anterior.
Por otra parte, la exposición de determinados datos de salud puede ser altamente dañoso para quienes sufren determinadas enfermedades. No podemos dejar de mencionar que los datos de salud son datos considerados sensibles por la Ley N° 18.331 de 11 de agosto de 2008[11], de Protección de datos personales.
Además, la indisponibilidad de la información afectaría la continuidad asistencial que es el objetivo de la HCEN. Y la violación a la integridad puede causar graves perjuicios a la salud de las personas, incluso la muerte.

6. Rol que la inteligencia y contrainteligencia podría desempeñar para prevenir o evitar la ocurrencia del ciberataque

La protección de una infraestructura crítica implica la detección y alerta temprana, la detención, la reacción y el manejo de crisis. En este sentido, podemos entender que se ha estado trabajado acertadamente para proteger la plataforma HCEN.
Durante el año 2018 se realizaron varias actividades con la finalidad de potenciar los aspectos de seguridad de los distintos componentes de Salud.uy, trabajando en conjunto con el área de Seguridad de la Información de Agesic. Se realizaron acciones puntuales sobre algunas aplicaciones (hackeos éticos) auditorías y se trabajó en el cumplimiento de objetivos estratégicos. Desde el punto de vista más específico y técnico, se realizaron revisiones de seguridad a través de hackeos éticos (Ethical Hacking) de cinco aplicaciones de diferentes portes utilizadas o implementadas por Salud.uy: Historia Clínica Electrónica Oncológica (HCEO), Red Integrada de Diagnóstico por Imagen (RIDI), Programa de Salud Bucal Escolar de Presidencia de la República (PSBE), Pentaho (utilizado para Bussiness Inteligence en Salud.uy) y Owncloud (Servicio de alojamiento de archivos). Las revisiones sirvieron para detectar posibles brechas de seguridad en las aplicaciones o infraestructura, de modo de poder corregirlas en tiempo y forma. Por otro lado, se

[11] https://www.impo.com.uy/bases/leyes/18331-2008

inició un proceso de instalación de varios Web Application Firewall (WAF) en las aplicaciones desplegadas bajo el control de Salud.uy[12].

Agesic ha trabajado también en varios documentos: el Marco de Ciberseguridad, la guía de implementación del Marco de Ciberseguridad, la Lista de verificación y la Guía de auditoría[13]. Tanto las actividades que se han venido realizando como las recomendaciones de la Guía de implementación del Marco[14], en la cual se hace especial referencia al sector salud, aplican a las actividades de inteligencia (recolección y análisis de la información) y contrainteligencia, trabajando en la ciberseguridad del sistema y desconozco si se ha utilizado algún sistema señuelo con el objeto de engañar, que es otro de los aspectos de ésta.

Tomando como referencia la Guía de implementación me ha parecido relevante destacar los siguientes aspectos:

Gestión de riesgos: evaluar los posibles riesgos y vulnerabilidades a la confidencialidad, integridad y disponibilidad de la HCE, así como con relación a la conectividad de dispositivos médicos.

Organización y gobernanza: a) ante incidentes de seguridad que afecten o puedan afectar la infraestructura de HCEN o sus sistemas circundantes (por ejemplo, servidores DNS, Firewalls, Correo, etc.), deben reportarse siempre al CERTuy o equipo de respuesta que corresponda.

b) Todo proyecto que incluya dispositivos médicos con conectividad debe tener una evaluación de riesgos específica y definirse una política sobre la utilización de dispositivos móviles.

c) Contar con controles tendientes a mitigar el riesgo relacionado al acceso remoto de los proveedores de equipamiento médico que requieren acceder por temas de mantenimiento.

d) Se debe prestar especial cuidado en el intercambio transfronterizo de datos, cumpliendo con lo establecido en el artículo 23 de la Ley N° 18.331.

---

[12] Informe ejecutivo de las actividades de Salud.uy 2018. https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/informes-ejecutivos-saluduy Página visitada el 27 de julio de 2021.

[13] https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/marco-ciberseguridad Página visitada el 3 de agosto de 2021.

[14] Guía de implementación del Marco de Seguridad de la Información Versión 4.1, Noviembre 2019. https://archivos.agesic.gub.uy/nextcloud/index.php/s/qmAqzYpqJN2F35r Página visitada el 27 de julio de 2021.

Gestión humana: a) es recomendable que los roles y responsabilidades del personal que tenga acceso a datos personales y de salud, se encuentren debidamente documentados, indicando en cada caso el tipo de información al que puede acceder.
b) Es necesario que se cuente con esfuerzos específicos de capacitación y concientización en temas vinculados a seguridad de la información para el equipo de salud.
Gestión de activos: a) es recomendable identificar especialmente los activos de información que procesan y/o almacenan información de los usuarios (sistemas de historias clínicas, equipamiento médico, etc.).
b) Es deseable que se identifique al responsable de la gestión del activo y al responsable técnico.
c) Es necesario que todo aquel equipamiento que procese o almacene información de salud se ubique en el centro de datos.
d) Las instituciones de salud pública, deben clasificar la información de acuerdo a la Ley N° 18.381. En el ámbito privado, se recomienda clasificar la información de salud como confidencial.
d) Resulta imprescindible contar con mecanismos de eliminación segura de la información de los medios de almacenamiento, ya que no gestionar adecuadamente los procesos de destrucción de información podría generar una brecha de confidencialidad.
Control de acceso: a) control de los accesos lógicos a dispositivos médicos, trazas o logs, identificación y autenticación, altas y bajas de usuarios, contando con un doble factor de autenticación para acceso a la HCE.
b) A nivel de XDS (intercambio de datos entre empresas), se puede utilizar el campo HASH, (Hash de los elementos del documento) para que, al recibir el documento se verifique la integridad.
c) Para intercambiar información de salud deberán utilizar protocolo HTTPS y los respaldos deben estar cifrados.
d) Se debe utilizar firma electrónica avanzada de la Institución (persona jurídica) para los siguientes casos: almacenar los documentos clínicos, intercambiar documentos clínicos, al recibir un CDA, validar la firma electrónica avanzada. Los documentos clínicos deben almacenarse al menos, con firma electrónica común del médico y firma electrónica avanzada de la Institución. El simple logueo al sistema no

alcanza como método de firma, por lo que se recomienda que cada médico utilice la firma electrónica avanzada de persona física para firmar los documentos clínicos.

Seguridad física y del ambiente: a) implementar controles de acceso físico a las instalaciones y equipos ubicados en el centro de datos y áreas relacionadas.

b) Contar con un sistema de gestión y monitoreo centralizado capaz de alertar fallas sobre el equipamiento y establecer el mantenimiento de los componentes críticos.

Seguridad de las operaciones: a) al planificar los respaldos se debe contemplar lo indicado en la Ley N° 18.331, teniendo especial cuidado con la ubicación de los servidores (nube), en virtud de las disposiciones referentes a transferencias internacionales de datos personales.

b) Se debe establecer al menos algún mecanismo de contingencia en caso de indisponibilidad de los sistemas de HCE propios para lograr la consulta a la historia clínica de los usuarios.

c) Se debe considerar la revisión regular de los sistemas que sean críticos para la atención clínica (por ejemplo, HCE, LIS, RIS, PACS, equipos biomédicos, entre otros) y aquellos que afecten o puedan afectar a la infraestructura de HCEN o sus sistemas circundantes.

Seguridad de las comunicaciones: a) considerar las transferencias internacionales de datos, como ya se hizo referencia.

b) Se debe evaluar la necesidad de utilizar segregación para los diferentes servicios, por ejemplo: laboratorio clínico, imagen médica, CTI, entre otros. Se debe considerar especialmente la segregación de la red que contenga componentes que gestionen información y/o intervengan en la prestación de servicios de salud.

c) Se recomienda contar con un procedimiento de reporte mensual al CERTuy o equipo de respuesta que corresponda, sobre estadísticas de la actividad detectada en el WAF.

7. Reflexión final

Si bien es probable que la HCEN no figure como activo crítico en el Decreto reservado en materia de seguridad nacional, entendemos que podemos considerarla como tal, por las razones expuestas.

Como surge del análisis realizado, son varias las Instituciones involucradas: el Ministerio de Salud, Agesic (Salud.uy y Cert.uy) y las instituciones de salud públicas y privadas.

Sería relevante la creación de un Csirt de Salud, que se centre en las características específicas de la infraestructura y que, por tanto, proteja en forma particular este activo.

Para finalizar, y a los efectos de desmitificar la típica frase de que “en Uruguay nunca pasa nada”, mencionar que, en nuestro país, además del conocido caso del ataque del ransomware al Círculo Católico[15], en mayo de este año (2021) el director general del MSP, Miguel Asqueta, informó a través de sus redes sociales que su cuenta de correo electrónico había sido hackeada[16].

[15] “Datos de los usuarios de la salud están expuestos a las manos de hackers”. 23 de setiembre de 2017. https://www.elobservador.com.uy/nota/datos-de-los-usuarios-de-la-salud-estan-expuestos-a-las-manos-de-hackers-2017923500 Página visitada el 27 de julio de 2021.

[16] Unidad del Ministerio de Salud Pública es blanco de ciberataques. https://www.republica.com.uy/unidad-del-ministerio-de-salud-publica-es-blanco-de-ciberataques-id830901/ Página visitada el 27 de julio de 2021.