

# XI INFORME SEIS

## Las TIC y la seguridad de los pacientes

**Primum non nocere**

### **COORDINADORES:**

*Javier Carnicero Giménez de Azcárate*

*David Rojas de la Escalera*

*Raúl Martínez Santiago*







# XI INFORME SEIS

Las TIC y la seguridad de  
los pacientes

**Primum non nocere**

---

## ***Coordinadores***

*Javier Carnicero Giménez de Azcárate*

*David Rojas de la Escalera*

*Raúl Martínez Santiago*

## ***Comité Editorial***

*Javier Carnicero Giménez de Azcárate*

*Selene Indarte Galli*

*Raúl Martínez Santiago*

*Xavier Pastor i Durán*

*Antonio Poncel Falcó*

*Fernán González Bernaldo de Quirós*

*David Rojas de la Escalera*

Queda rigurosamente prohibida, sin la autorización escrita de los titulares del “Copyright”, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de esta obra por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático y la distribución de ejemplares de ella mediante alquiler o préstamo públicos.

ISBN: 978-84-617-4024-6

Copyright © SEIS, Sociedad Española de Informática de la Salud, 2016  
<http://www.seis.es>

Secretaría Técnica: CEFIC

C/ Enrique Larreta, 5 - bajo izda. 28036 - Madrid

Tel: 34 91 388 94 78 Fax: 34 91 388 94 79

[cefic@cefic.co](mailto:cefic@cefic.co)

*Este trabajo está dedicado a D. Emilio Aced Fález,  
inolvidable compañero y amigo de la Junta Directiva de la SEIS*



<b>Prólogo</b> .....	9
<b>Resumen ejecutivo</b> .....	11
<b>La seguridad del paciente y las TIC en el marco del sistema de salud</b> .....	19
<b>Capítulo I</b> Conceptos básicos de seguridad de los pacientes <i>Pedro Parra Hidalgo</i> .....	29
<b>Capítulo II</b> Principales fuentes de riesgo: Aportaciones de las tecnologías de la información y la comunicación <i>Fernán González Bernaldo de Quirós, Carlos Otero y Daniel Luna</i> .....	47
<b>Capítulo III</b> La utilización de las TIC como un factor de riesgo para la seguridad de los pacientes <i>David Rojas de la Escalera y Javier Carnicero Giménez de Azcárate</i> .....	67
<b>Capítulo IV</b> TIC aplicadas a la seguridad del paciente dentro del laboratorio de análisis clínicos <i>Miguel Angel De Cristóforo, Matías G. Dombald y Nereo N. Candenas</i> .....	91
<b>Capítulo V</b> El riesgo en el Bloque Quirúrgico: Aportaciones de las TIC <i>Carlos Emparán García de Salazar</i> .....	121
<b>Capítulo VI</b> Unidad de Cuidados Intensivos: Aportaciones de las Tecnologías de la Información y Comunicación <i>Daniel Luna, Selene Indarte, Humberto Mandirola y Sonia Benítez</i> .....	143
<b>Capítulo VII</b> La seguridad transfusional y las tecnologías de la información y la comunicación <i>Arturo Pereira Saavedra</i> .....	171
<b>Capítulo VIII</b> La seguridad de la información desde la perspectiva de la seguridad del paciente <i>Raúl Martínez Santiago</i> .....	187
<b>Los autores</b> .....	209



## Prólogo



Los Informes SEIS nacen en 1998 con el objetivo de estudiar asuntos de interés para los socios, profesionales del Sistema Sanitario, estudiantes y público en general, relacionados con las tecnologías de la información y de las comunicaciones y la salud.

Estos Informes se enmarcan en la misión de nuestra sociedad científica, que no es otra que promover la investigación, desarrollo e innovación, implantación y buen uso de las TIC en el ámbito de la salud, en beneficio de la sociedad y con pleno respeto a los derechos individuales, y en particular en una de sus líneas estratégicas: la de elaborar estudios e informes que analicen y promuevan la implantación de las tecnologías de la información y de las comunicaciones en el sector de la salud.

Hoy el sector salud está inmerso en una transformación digital, con multitud de diversos proyectos en marcha, y por ello pretendemos trasladarle una visión profesional de los temas más trascendentales, siempre desde la perspectiva de su relación con las TIC, que consideramos que afectan, interesan y preocupan tanto al sector sanitario como a los ciudadanos.

Es una realidad que los Informes SEIS se han constituido como un referente internacional de prestigio en el sector, gracias a la independencia y rigor con los que son elaborados y, sobre todo, a los autores y editores que desinteresadamente participan en su elaboración, aportando su

conocimiento y experiencia para compartirlos con los profesionales del sector sanitario y el público en general. La SEIS expresa una vez más nuestro más sincero agradecimiento por su trabajo y colaboración.

En este nuevo Informe SEIS, titulado “Las TIC y la seguridad de los pacientes: *Primum non nocere*”, se ofrece una revisión crítica de los aspectos más destacados que afectan a la seguridad de los pacientes, y de cómo las TIC pueden contribuir a la solución de las necesidades existentes, aportando además un valor añadido. No menos importante es identificar y evaluar los nuevos riesgos que, como consecuencia del desarrollo de los proyectos TIC, pueden aparecer en relación con la seguridad de los pacientes.

Es necesario también que todos los proyectos contemplen la seguridad de los pacientes entre sus principales objetivos y requisitos funcionales, y no sólo como un valor añadido para el paciente, sino también por el elevado impacto que supone en la eficiencia y actividad de la asistencia sanitaria. A modo de ejemplo, un estudio reciente estimó que en España, durante el período 2008-2010, un 6,8% de los episodios asistenciales se vieron afectados por algún evento adverso relacionado con la seguridad del paciente, lo que supuso un coste económico de unos 90 millones de euros, además de las consecuencias para la calidad de vida de los pacientes afectados.

En este nuevo Informe SEIS se revisan los conceptos básicos de seguridad de los pacientes, las principales fuentes de riesgo, las propias TIC como un factor de riesgo y la visión específica de diferentes escenarios concretos. Confiamos en que este nuevo volumen resulte una vez más de interés y utilidad como fuente de conocimiento para los profesionales del sistema de salud.

**Luciano Sáez Ayerra**

Presidente de la Sociedad Española de Informática de la Salud

## Resumen ejecutivo



El sistema de salud, concebido como el conjunto de “todas las organizaciones, personas y acciones cuyo objetivo primario es promover, mejorar o mantener la salud”, asume las funciones de provisión asistencial, creación y gestión de recursos, administración del propio sistema y financiación de toda la actividad.

El Sistema Nacional de Salud (SNS) español, de carácter público, es un ejemplo de evolución desde un sistema de seguridad social y gestión centralizada hacia un sistema financiado mediante impuestos y cuyas competencias de provisión asistencial corresponden en la actualidad a los gobiernos de las comunidades autónomas, que constituyen el nivel regional de las administraciones públicas. Su esquema de funcionamiento actual es el producto de varias acciones y reformas estratégicas que han venido produciéndose durante décadas.

Las últimas medidas emprendidas son consecuencia del contexto de crisis económica, que ha llevado incluso a poner en tela de juicio la sostenibilidad del actual modelo del SNS. Esta situación se ve agravada por una situación en la que se combinan el envejecimiento de la población, con el consiguiente aumento de enfermedades crónicas y degenerativas, y el progreso de la medicina, que permite ofrecer nuevas técnicas diagnósticas y terapéuticas, lo que supone una mayor demanda por parte de la población y la necesidad de incurrir en nuevos costes.

Por lo tanto, existe una necesidad manifiesta de conciliar la contención del gasto con el mantenimiento de la calidad de los servicios y en particular con la garantía de la seguridad de los pacientes, lo que obliga a las instituciones y organizaciones a buscar soluciones de compromiso que permitan guardar el mejor equilibrio posible entre ambos extremos. La aplicación de las Tecnologías de la Información y la Comunicación (TIC) a la asistencia sanitaria es una de las oportunidades más claras en este aspecto.

## Conceptos básicos de seguridad de los pacientes

La calidad de la asistencia sanitaria es un concepto complejo que combina diversas dimensiones como la efectividad, la eficiencia, la accesibilidad, la personalización, la satisfacción, y la seguridad del paciente. Esta última se define como “la ausencia de daño innecesario, real o potencial, asociado a la atención sanitaria”, y obedece al interés de los sistemas sanitarios por no causar daños evitables como consecuencia de la prestación asistencial.

A partir de esta definición, la seguridad del paciente obliga a establecer varios conceptos relacionados, como riesgo, daño asociado a la atención sanitaria, incidente relacionado con la seguridad del paciente, incidente sin daños, incidente con daños (evento adverso), reacción adversa, efecto secundario, o error. Este último se define como “el hecho de no llevar a cabo una acción planeada o de aplicar un plan incorrecto”.

La importancia de la seguridad del paciente puede estimarse a partir de las cifras contempladas en diversos estudios, que cuantifican los efectos negativos de los eventos adversos en problemas de salud evitables, costes económicos e incluso fallecimientos. Por lo tanto, no es de extrañar que durante los últimos años se hayan promovido a escala mundial diversas estrategias para la mejora de la seguridad del paciente, auspiciadas por organismos como la Organización Mundial de la Salud, la Organización para la Cooperación y el Desarrollo Económicos, la Agencia para la Investigación y Calidad de la Asistencia estadounidense (AHRQ) y la Unión Europea.

Fruto de estas estrategias son medidas y acciones para la gestión de la calidad y seguridad de la asistencia, como los análisis de causas-raíz, los análisis modales de fallos y efectos, los sistemas de notificación, el impulso

de una cultura corporativa de la seguridad, o la monitorización de la seguridad del paciente. En el ámbito de esta última se han desarrollado varios indicadores de resultados que miden la incidencia de complicaciones y efectos adversos. Como resultado de todo ello, se han definido varias recomendaciones y buenas prácticas encaminadas a garantizar la máxima seguridad posible durante el cuidado del paciente.

## Principales fuentes de riesgo

Los errores en medicina representan un grave problema de salud pública y constituyen una seria amenaza para la seguridad del paciente. En los últimos años, a partir de una creciente revisión de los procesos de cuidado, las instituciones de salud han tratado de hacer foco en cómo identificar y prevenir o al menos mitigar esos “errores”, sin embargo ninguna iniciativa ha sido totalmente efectiva.

Asociadas a otras iniciativas, las Tecnologías de la Información y la Comunicación (TIC) están siendo utilizadas como una herramienta para reducir los errores y mejorar la seguridad (por ejemplo, mediante el uso de prescripción electrónica asistida y sistemas de soporte a la toma de decisión). Sin embargo, si no son implementadas con cuidado, estas tecnologías no logran ser efectivas y peor aún pueden introducir nuevos errores.

En este capítulo se describe el concepto de error en medicina, el rol de las TIC en la seguridad del paciente y los cuidados que hay que tener al aplicarlas, se enumeran las principales fuentes de riesgo y cómo abordarlas con las TIC y las estrategias para analizar los riesgos y mitigarlos.

## La utilización de las TIC como un factor de riesgo para la seguridad de los pacientes

La incorporación de las Tecnologías de la Información y la Comunicación (TIC) a la atención sanitaria es un hecho consolidado desde hace mucho tiempo, y se ha llevado a cabo con el objetivo de mejorar la eficacia, eficiencia y efectividad del sistema de salud. Sin embargo, y a pesar de su potencial, las TIC pueden suponer también la introducción de riesgos para la seguridad del paciente. La gestión de estos riesgos debe comenzar con un análisis pormenorizado de los

mismos, para definir sus principales parámetros, evaluar sus posibles consecuencias y, finalmente, decidir la estrategia más adecuada para afrontarlos.

El estudio del sistema de información de salud muestra los principales puntos de vulnerabilidad para la seguridad del paciente. Teniendo en cuenta que el objetivo de registrar la información clínica es garantizar que el proceso asistencial quede debidamente caracterizado y se pueda conocer con exactitud en posteriores consultas, un primer riesgo claro es la posibilidad de que se comentan errores en la identificación de las personas, elementos y acciones clave que intervengan en el proceso. Este riesgo se reduce con la creación, adopción, buen uso y evolución de estándares para la codificación de toda esta información, teniendo en cuenta todas las fases y posibles variaciones del proceso asistencial.

A este riesgo fundamental hay que añadir los correspondientes a cada etapa del ciclo de vida de un sistema TIC: diseño, desarrollo, implantación, utilización, mantenimiento y evolución. En este sentido, se trata de riesgos relacionados con el uso de las TIC e independientes en su mayor parte del ámbito profesional de la salud: requisitos funcionales mal definidos, diseños incorrectamente aplicados, infraestructuras erróneamente dimensionadas, formación insuficiente de los usuarios, carencias en los servicios de soporte y mantenimiento, etc.

Para reducir estos riesgos es necesario incorporar la seguridad del paciente a los objetivos de todo proyecto de desarrollo de un sistema TIC sanitario, y tenerla en cuenta en todos los procedimientos de trabajo y de gestión del proyecto. Existen algunas recomendaciones y buenas prácticas que pueden ser de ayuda para este tipo de actuaciones, como por ejemplo las guías SAFER.

### La seguridad del paciente dentro del laboratorio de análisis clínicos

Muchas son las instancias en las que la tecnología puede intervenir para lograr una mejora continua de la calidad y sobre todo influir positivamente sobre la seguridad del paciente durante el proceso de atención en el ámbito del laboratorio de análisis clínicos.

Para encarar en forma sistemática todo el proceso diagnóstico del laboratorio, se acepta dividirlo en distintas etapas denominadas comúnmente como “Pre-analítica”, “Analítica” y “Post-analítica”, las que se describirán en los diferentes apartados de este capítulo.

El empleo de las tecnologías de la información y la comunicación (TIC) forman parte importante, si no ineludible, en el manejo de este proceso, al punto tal que no se puede concebir un laboratorio moderno sin sistema de información. Sin embargo, es importante tomar en cuenta que este aporte genera potencialmente nuevas posibilidades de error, que indefectiblemente deben ser consideradas y controladas.

## El riesgo en el Bloque Quirúrgico

Junto con las Unidades de Cuidados Intensivos es en el quirófano el lugar donde mayor riesgo de complicaciones puede tener un paciente hospitalizado. Las buenas prácticas en términos de seguridad del paciente requieren una organización para la gestión de la seguridad. Los centros sanitarios deben desarrollar sistemas eficaces para asegurar, a través de la dirección clínica, una asistencia segura y aprender lecciones de su propia práctica y de la de otros.

La introducción de los sistemas de historia clínica electrónica, sistemas de recogida de datos intraoperatorios, o de imágenes digitalizadas de la intervención quirúrgica nos abre un campo de mejora en la seguridad del paciente que se puede enfocar en cuatro puntos: Primero, el uso de TIC y sistemas de HCE en el propio quirófano. Segundo, en el control y estandarización de procesos perioperatorios, desde la consulta hasta el alta del paciente. Tercero, el uso de archivos digitalizados quirúrgicos que sirvan de “cajas negras” quirúrgicas. Y cuarto, la creación de modelos de trabajo que, aunque estén basados en los ordenadores tradicionales, evolucionen a equipos portátiles de todo tipo en los que se puedan integrar flujos de proceso clínico, gestión de alertas de riesgo, introducción de algoritmos de riesgo quirúrgico, y sistemas de volcado de datos a grandes bases de datos en los que se puedan realizar grandes análisis multivariantes desde procedimientos quirúrgicos comunes hasta procedimientos muy especializados o infrecuentes.

## Unidad de Cuidados Intensivos

El proceso de atención de pacientes en unidades de cuidados intensivos o *intensive care units* (UCI) es complejo y requiere un rápido acceso a información clínica del paciente. Entre otras características los

pacientes muchas veces están inconscientes, intubados, polimedidados, con múltiples transductores y la mayoría de las veces sin la familia presente. Los pacientes tienen mayor exposición a sufrir errores médicos y los profesionales a cometer esos errores debido a que se encuentran inmersos en este escenario. Las tecnologías de la información y comunicación (TIC) desempeñan un rol fundamental para dichos procesos y tienen el potencial para, en muchos casos, prevenir dichos fallos, aunque su introducción también puede determinar la aparición de nuevas equivocaciones. Las TIC sin duda son una ayuda para tomar decisiones pero también pueden inducir a errores si no están adecuadamente diseñadas.

El propósito de este capítulo será desarrollar los tópicos arriba mencionados realizando una revisión narrativa de las fuentes de información disponibles. En primer lugar, se hará una breve referencia a características de los pacientes en UCI, procesos asistenciales y fuentes de riesgo para la seguridad del paciente en dichos procesos. En segundo lugar, se expondrán los componentes de un Sistema de Información Clínico en UCI, así como los fundamentos sobre la clasificación de los sistemas basados en TIC en estas unidades asistenciales. En tercer lugar, se describe a las TIC como estrategia para la mejora en la seguridad del paciente, así como la integración de la Información en este nivel de atención. Finalmente, se otorgará especial atención a los nuevos errores que genera el uso de TIC en este escenario, así como los sistemas de reportes de errores en UCI.

## La seguridad transfusional

Al hablar de seguridad transfusional debe distinguirse entre la seguridad del producto sanguíneo (calidad y esterilidad) y la seguridad del proceso de la transfusión, tal como se lleva a cabo en los hospitales. Este último es muy sensible al error humano debido a la necesidad de realizar múltiples transcripciones de datos críticos, como la identidad del paciente, a la ausencia de control centralizado, a la coexistencia de procesos paralelos destinados a pacientes diferentes y a los lapsus inevitables del personal sanitario que pueden acabar en la transfusión incompatible de consecuencias graves.

El proceso de la transfusión se ha beneficiado poco de las tecnologías de la información y la comunicación (TIC) pues la única

aportación destacable ha sido la incorporación de códigos de barras en la identificación del paciente y de los productos sanguíneos. Estos sistemas basados en códigos gráficos tienen numerosas limitaciones pues su capacidad para almacenar y renovar la información es baja, no eliminan la necesidad de acciones manuales y son poco útiles en algunos ambientes, como el quirúrgico, donde puede faltar la necesaria línea de visión directa entre el código y el lector.

Las tecnologías basadas en radiofrecuencia (RFID) superan esas limitaciones y es de esperar que contribuyan de un modo decisivo a la seguridad de la transfusión. Es importante que la implantación de sistemas RFID contemple todos los procesos hospitalarios que requieren la identificación del paciente y no sólo el de la transfusión.

### La seguridad de la información desde la perspectiva de la seguridad del paciente

Seguridad es sinónimo de confianza y se debe hacer todo lo posible para evitar que ésta se rompa o al menos, si se rompe, recuperarla lo antes posible. Esto es extensible tanto a la seguridad clínica como a la seguridad de la información, que deben garantizarse al máximo.

La seguridad de la información, tanto en su vertiente técnica como normativa, debe ser siempre un elemento de suma y no de resta en la seguridad clínica. Como algunos aspectos de la seguridad de la información pueden ser contrarios a la seguridad de los pacientes, siempre se deben ponderar los distintos aspectos que intervienen en su ejecución, para lograr un equilibrio que por un lado asegure la seguridad de la información y por otro no ponga en peligro la seguridad de los pacientes. Por ejemplo, proteger con controles excesivos el acceso a la información clínica (confidencialidad, un componente de la seguridad de la información) puede ser perjudicial para la seguridad del paciente, si se dificulta tanto ese acceso que los clínicos desisten de consultar información que puede ser trascendental para la asistencia.

La seguridad de la información debe aportar calidad, tecnología y organización en la parte técnica, y garantías y adaptación a las necesidades en la parte normativa, para ser de utilidad a la práctica clínica. Los incidentes de seguridad se deben registrar para analizar y detectar las causas, resolver los problemas y tomar medidas para que no vuelvan a ocurrir.



## La seguridad del paciente y las TIC en el marco del sistema de salud

*Javier Carnicero Giménez de Azcárate*

*David Rojas de la Escalera*



### El sistema de salud

La Organización Mundial de la Salud (OMS) define el sistema de salud como el conjunto de “todas las organizaciones, personas y acciones cuyo objetivo primario es promover, mejorar o mantener la salud”<sup>1</sup>. En la Conferencia Ministerial Europea organizada por la OMS y celebrada en Tallin (Estonia) en el año 2008, se establecieron las siguientes funciones básicas de un sistema de salud<sup>2</sup>:

- La provisión de servicios de salud a individuos y poblaciones, prestando la mejor asistencia posible para prevenir o resolver sus problemas de salud.
- La creación y gestión de recursos, concepto que engloba los profesionales, las infraestructuras, las tecnologías y el conocimiento del sistema de salud. Esto requiere planificación y visión a largo plazo, utilización efectiva y ética de los recursos del sistema, formación y actualización de profesionales, y evaluación rigurosa de las tecnologías sanitarias, en especial de las innovaciones resultantes de los proyectos de investigación.

---

<sup>1</sup> Organización Mundial de la Salud (OMS). Everybody’s business: Strengthening health systems to improve health outcomes. WHO’s framework for action, 2007.

<sup>2</sup> Organización Mundial de la Salud (OMS). The Tallinn Charter: Health Systems for Health and Wealth. Conferencia Ministerial Europea de la OMS sobre Sistemas de Salud, 25-27 junio. Tallin (Estonia), 2008.

- La administración del sistema, que comprende la definición de un marco legal específico, el diseño de políticas y estrategias de salud, el registro y análisis de información para la gestión sanitaria—incluyendo factores sociales, económicos y ambientales—, la incorporación de la perspectiva de salud en todas las políticas gubernamentales, y la monitorización y evaluación del funcionamiento del sistema.
- La financiación del propio sistema, basada en la asignación —y redistribución, en caso necesario— de los recursos en función de las necesidades de la población y del desempeño en cada área; en la reducción de las barreras financieras para el acceso y utilización del sistema; en la incentivación de la eficiencia en la organización y en la provisión de la asistencia; y en la promoción de la transparencia del propio proceso de financiación. Aunque el sistema de salud debe proporcionar unos servicios que respondan a las necesidades sanitarias de la población, también debe velar por su propia sostenibilidad financiera.

En resumen, el objetivo principal de un sistema de salud es la atención de salud, ya sea individual —pacientes— o colectiva —población—, y tanto para atender problemas de salud como para prevenirlos. En torno a esta función primaria se articulan otras que son de carácter instrumental, pero que sin embargo resultan imprescindibles para garantizar la prestación, la continuidad y la mejora de dicha asistencia. Estas funciones son comunes a todos los sistemas de salud, independientemente de algunas de sus características fundamentales, como su dimensión o su condición pública o privada.

### El Sistema Nacional de Salud de España: Situación y tendencias

El Sistema Nacional de Salud (SNS) en España tiene sus orígenes en el sistema de seguridad social que estuvo vigente hasta la aprobación de la Ley General de Sanidad de 1986. Esta norma creó un sistema de cobertura universal, financiado mediante impuestos y con la gestión de la provisión asistencial encomendada a las Comunidades Autónomas tras un proceso gradual de descentralización de competencias. En 2012, con motivo de la crisis económica, se introdujeron algunos cambios en el acceso al sistema y en la financiación de algunas prestaciones<sup>3</sup>, cuyo impacto, todavía por evaluar, se atisba con alguno de los datos que se muestran más adelante.

---

<sup>3</sup> Real Decreto-ley 16/2012, de 20 de abril, de medidas urgentes para garantizar la sostenibilidad del Sistema Nacional de Salud y mejorar la calidad y seguridad de sus prestaciones.

Algunos de los desafíos a los que debe hacer frente el SNS son los ya bien conocidos del envejecimiento de la población, que trae consigo una mayor prevalencia de enfermedades crónicas y degenerativas, y las restricciones presupuestarias consecuencia de la crisis económica, y las mayores demandas de los pacientes. A esto se unen la continua incorporación de nuevas tecnologías sanitarias, más costosas. El mejor ejemplo de esto último son los nuevos medicamentos, por ejemplo los destinados al tratamiento de la hepatitis C. Estos retos son comunes a la mayor parte de los países occidentales. Por otra parte, desde hace más de 10 años el Sistema Nacional de Salud ha llevado a cabo un esfuerzo considerable para incorporar las tecnologías de la información y de la comunicación (TIC) al núcleo de la actividad asistencial mediante proyectos de historia clínica electrónica, imagen médica digital y receta electrónica, buscando una mayor eficiencia y calidad.

La población española ha crecido de manera notable en el periodo 2001-2011, principalmente debido a un aumento muy importante del número de ciudadanos extranjeros. Sin embargo, esta población envejece, lo que unido al descenso de la natalidad podría llegar a provocar un descenso en el número de habitantes en los próximos años. El porcentaje de mayores de 65 años en España es ya del 17,38% y la tendencia es creciente. Aunque la natalidad repuntó en los primeros años del siglo XXI, se aprecia un nuevo descenso a partir de 2009, coincidente con el inicio de la actual crisis económica. Muy relacionada con el envejecimiento de la población está la tasa de dependencia de población mayor de 64 años, que relaciona la población mayor de esta edad con la comprendida entre los 16 y los 64 años. Este indicador, a pesar de la oscilación que coincide con el repunte de la natalidad en los primeros años de este siglo, muestra una tendencia creciente. Así, en 2003 era del 25,05% y en 2013 del 26,14%<sup>4</sup>.

El gasto sanitario público ha experimentado un crecimiento continuado, tanto en términos absolutos como en porcentaje del PIB, hasta el año 2009. Sin embargo, con motivo de la crisis económica y las medidas implantadas a partir de ese año se observa una reducción. El gasto sanitario público en España ha pasado de 1.510 euros por habitante, y un 6,5% del PIB en 2009, a 1.309 y 5,9% respectivamente en el año

---

<sup>4</sup> Instituto Nacional de Estadística (INE). Tasa de dependencia (%) =  $100 \cdot \text{Población mayor de 64 años} / \text{Población entre 16 y 64 años}$ .

2013. Aunque el gasto sanitario total medido por su porcentaje sobre el PIB también desciende a partir del año 2011, el porcentaje de gasto sanitario público sobre el total de gasto ha pasado del 74,6% en el año 2009 al 71,7 % en 2011 (véase Tabla 0.I).

<b>Tabla 0.I. Volumen y estructura del gasto sanitario en España (2009-2013).</b>					
	<b>2009</b>	<b>2010</b>	<b>2011</b>	<b>2012</b>	<b>2013</b>
Gasto sanitario público (M€)	70.579,00	69.417,00	68.050,00	64.153,00	61.710,00
Gasto sanitario público (% PIB)	6,50	6,40	6,30	6,10	5,90
Gasto sanitario público/habitante (€)	1.510,00	1.475,00	1.442,00	1.357,00	1.309,00
Gasto sanitario total (% PIB)	9,10	9,10	9,00	8,90	8,80
Gasto sanitario público (% sobre el total)	74,60	74,00	73,30	71,70	71,59
Gasto farmacéutico (% sobre el total)	18,70	18,80	17,90	16,70	18,80

Fuentes: Ministerio de Sanidad, Servicios Sociales e igualdad (MSSSI) de España, y Organización para la Cooperación y el Desarrollo Económicos (OCDE).

Según el Barómetro Sanitario que publica el Ministerio de Sanidad, la valoración de las personas que utilizaron los servicios sanitarios públicos es positiva, tanto en atención primaria como en especializada y en urgencias. Se identifican como aspectos susceptibles de mejora los relacionados con los tiempos de acceso a los servicios: la obtención de cita el mismo día que se solicita, si así se desea, en Atención Primaria (38%), las demoras para las consultas de atención especializada y para la hospitalización programada (que se considera que no han mejorado), y los tiempos de permanencia en sala de espera para entrar en consulta (el 31% espera más de 1 hora).

Debe resaltarse que según este estudio una clara mayoría de los ciudadanos prefiere para su atención los centros públicos: 68,4% para ser atendidos en A. Primaria; 53,9% en el caso de consultas a especialistas; 63,7% para la hospitalización; y un 63% para la atención en urgencias. Esta preferencia ha aumentado en todos los casos en más de 3 puntos desde 2012. A pesar de esta valoración en general positiva, se identifica un cierto pesimismo en cuanto a la evolución de los servicios sanitarios. La apreciación más frecuente es que han mejorado o siguen funcionando igual: así piensa el 65% en el caso de la A. Primaria; el 74% para los hospitales; el 53% para las consultas de especialistas y –el más bajo– el 47% para las urgencias. Sin embargo, ha aumentado el porcentaje de personas que piensan que los servicios han empeorado en los 5 últimos años, que en el caso de la asistencia especializada ambulatoria se sitúa en un 37,3% y en el de las urgencias alcanza el 43,1%. La satisfacción con el sistema sanitario público se

califica con 6,31 puntos sobre 10, valoración ligeramente inferior al año anterior (6,41). La ya larga serie disponible (2002-2014) muestra que este indicador se mueve en un intervalo entre 5,94 y 6,59 puntos<sup>5</sup>.

La crisis y las restricciones económicas han conducido, como ya se indicó antes, a una contracción del gasto público en salud, que coincide con una disminución de la actividad asistencial. Como ejemplo puede citarse la evolución de la lista de espera quirúrgica. Según los datos publicados por el Ministerio de Sanidad, a 31 de diciembre de 2009 el número de pacientes en lista de espera quirúrgica estructural ascendía a 372.468, con una espera media de 67 días. En 2014 las cifras son de 511.923 y 87 días<sup>6</sup>. Sin embargo, la diferencia en la lista de espera de consultas en atención especializada entre esos años ha aumentado solo ligeramente, de una espera media de 59 días en 2009 a 65 días en 2014.

<b>Tabla 0.II. Algunos indicadores del SNS español.</b>							
	<b>2009</b>	<b>2010</b>	<b>2011</b>	<b>2012</b>	<b>2013</b>	<b>2014</b>	<b>2015</b>
Lista de espera quirúrgica							
Número de pacientes	372.468	392.072	459.885	571.395	583.612	511.923	549.424
Tiempo medio de espera (días)	67	65	73	100	101	87	89
Lista espera consultas externas							
(pendientes/1000 habitantes)	40,24	33,00	36,10	42,16	39,94	39,43	43,35
Tiempo medio espera (días)	59	53	58	59	54	65	58
Fuente: Ministerio de Sanidad, Servicios Sociales e igualdad (MSSSI) de España. Sistema de Información de Listas de Espera.							

Las TIC se han incorporado de forma desigual al Sistema Nacional de Salud. Más del 90% de los médicos de atención primaria cuentan con sistemas de historia clínica electrónica y la receta electrónica es una realidad en la mayoría de las comunidades autónomas, aunque el grado de cobertura del servicio varía de unas a otras. La incorporación de la historia clínica electrónica en los centros hospitalarios ha sido más desigual. Con carácter general, los nuevos hospitales tienen una implantación completa, mientras en los hospitales con años de funcionamiento esta labor ha sido más dificultosa. Las comunidades autónomas no publican informes de resultados de los proyectos ni del impacto en la mejora de la calidad de la atención [1].

<sup>5</sup> Barómetro Sanitario 2014. Disponible en: <http://www.msssi.gob.es/estadEstudios/estadisticas/inforRecopilaciones/barometro/home.htm>

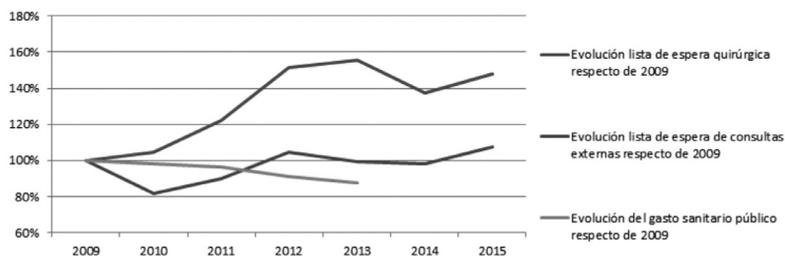
<sup>6</sup> Ministerio de Sanidad, Servicios Sociales e igualdad (MSSSI) de España. Sistema de Información de Listas de Espera.

Precisamente la incorporación de las TIC a los sistemas de salud se ha considerado una estrategia fundamental para afrontar los retos mencionados antes. Sin embargo, las TIC son instrumento, aunque imprescindible solo instrumento y no un fin, para mejorar la calidad del sistema de salud.

Cuando parece que la situación económica comienza a mostrar signos de recuperación es el momento de afrontar los desafíos pendientes del sistema sanitario. Para ello es necesaria una estrategia de mejora de la calidad, de la efectividad y de la eficiencia. Estos conceptos no son incompatibles y como se analiza en este libro, efectividad y eficiencia son atributos de la calidad de la asistencia sanitaria.

## Las TIC en el contexto de la seguridad de los pacientes

En el actual contexto de restricciones presupuestarias, con la consiguiente contención y en algunos casos reducción interanual del gasto sanitario, es fácil suponer que durante los últimos años se ha producido inevitablemente una merma de la calidad asistencial. El descenso en la contratación de personal, tanto fijo como temporal, la paralización de inversiones en infraestructuras sanitarias, tanto en la apertura de nuevos centros como en la remodelación de los ya existentes, y la búsqueda de fórmulas de contratación que potencian la externalización de servicios, entre otras medidas, se asocian tradicionalmente con el recorte de gastos, que a su vez conduce a asumir una disminución de la calidad del servicio prestado.



**Figura 0.1.** Evolución porcentual del gasto sanitario público y del número de pacientes en lista de espera quirúrgica y de consultas externas desde el año 2009.

En la Figura 0.1 se compara la evolución de las listas de espera, tanto de consultas externas como quirúrgica, con la del gasto sanitario público durante los últimos años. El número de pacientes en lista de espera quirúrgica crece de forma llamativa a la par que se reduce el gasto durante la serie 2009-2013, para después experimentar un descenso importante en el año 2014 aunque aumenta el 2015. La lista de espera quirúrgica en 2013 supera en un 55% la de 2009 mientras la de consultas externas es prácticamente la misma. Sin embargo, el gasto sanitario público en 2013 es el 87% del gasto de 2009. Aunque los datos de gasto de 2014 y 2015 no están aún disponibles en el momento de la elaboración de este Informe SEIS, no parece probable que se haya producido durante ese año un incremento, a la vista del crecimiento de la lista de espera que se observa en 2015. Por lo tanto, parece razonable asumir que el gasto sanitario es un factor importante en la evolución de las listas de espera (especialmente de la quirúrgica, al corresponder a una actividad asistencial con un coste mucho mayor que el de la atención ambulatoria), pero desde luego no se trata del único factor a tener en cuenta.

Al margen del fundamento que pueda tener esta postura, es un hecho contrastado que el descenso en la calidad de la asistencia también tiene un coste. En el caso concreto de la seguridad de los pacientes, un estudio realizado sobre datos del período 2008-2010, coincidiendo con los primeros años de la actual crisis económica (pero antes de que se introdujeran los primeros recortes importantes en materia de gasto sanitario), afirma que, sobre una muestra de 245.320 episodios, aproximadamente 17.000 (un 6,8%) sufrieron algún evento adverso. El coste asociado a estos episodios se estima en unos 1.300 millones de euros, y el coste derivado de los eventos adversos correspondientes se calcula en casi 90 millones de euros, un 6,74% del coste total [2].

Por otro lado, el sistema público de salud se financia mediante los ingresos procedentes de los impuestos, de modo que también parece acertado suponer que en un contexto de crisis económica sería necesario un aumento de la presión fiscal para mantener la calidad de la asistencia. Ambas estrategias son impopulares, puesto que sus consecuencias son indeseadas por parte de pacientes, profesionales y gestores. Por lo tanto, es prioritario para las administraciones públicas buscar un equilibrio entre la reducción del gasto y el incremento de la recaudación tributaria, lo que nos lleva a buscar fórmulas que permitan maximizar la eficiencia de las inversiones y reducir los tiempos de retorno de las mismas.

La incorporación de las TIC a la actividad asistencial es una de las iniciativas que se pone habitualmente como ejemplo en estos casos. El presente Informe SEIS pone el foco sobre las posibles contribuciones de las TIC a una actividad asistencial que debe compaginar una mayor complejidad y especialización, derivada del progreso de la medicina y de la aparición de nuevas técnicas diagnósticas y terapéuticas, con un mayor aprovechamiento de los recursos existentes que permita minimizar el impacto del contexto socioeconómico actual en la calidad de la asistencia. Todos ellos pueden representar factores de riesgo para la seguridad del paciente, y deben ser tenidos en cuenta a la hora de valorar las posibles aportaciones de las TIC.

En el Capítulo I se establecen varios conceptos básicos, entre los que destacan el de calidad asistencial y el de la seguridad del paciente propiamente dicha, siendo la segunda un componente importante de la primera. Se ofrecen además algunas cifras ilustrativas del impacto de la seguridad del paciente (o de su ausencia) en la calidad asistencial, y se analizan las estrategias y actividades más comunes para su gestión en el entorno de las instituciones y servicios de salud.

El Capítulo II complementa al anterior mediante el análisis detallado de las principales fuentes de riesgo para la seguridad del paciente, clasificadas en diversas categorías relacionadas con los distintos procesos que se derivan de la actividad asistencial: atención clínica, prescripción de medicamentos, procedimientos, gestión de sangre y hemoderivados, gestión administrativa y documental, infecciones nosocomiales, nutrición, oxigenoterapia y uso de otros gases, comportamiento de los profesionales sanitarios, accidentes de los pacientes, infraestructura y organización. El capítulo se completa con nociones sobre la evaluación de errores y con la exposición de las posibles aportaciones de las TIC para mejorar la gestión de la seguridad del paciente, sin olvidar que su utilización también supone por sí misma una fuente de riesgo.

Esta idea es la base del Capítulo III, en el que se estudian los riesgos que la utilización de las TIC supone para la seguridad del paciente. Partiendo del concepto de sistema de información de salud como entorno en el que la información del paciente se registra de forma incremental y estructurada, y después se emplea para diversos usos además del puramente asistencial, se identifican varios puntos críticos para garantizar la seguridad del paciente en la traslación de los procesos al ámbito TIC. Asimismo, se identifican y analizan los distintos

riesgos durante la ejecución de los proyectos orientados a la creación de un sistema TIC. Por último, se enumeran varias recomendaciones y buenas prácticas, con mención especial de las guías SAFER a modo de ejemplo.

Una vez establecidos estos fundamentos, se da paso a una serie de capítulos enfocados al estudio de entornos específicos. El Capítulo IV versa sobre las mejoras que el uso de las TIC puede significar para los laboratorios clínicos, revisando cada etapa del proceso desde la solicitud de un análisis hasta la entrega de los resultados obtenidos, y teniendo en cuenta algunos aspectos particulares de ambientes concretos, como por ejemplo la identificación de pacientes que precisan atención urgente.

El uso de TIC permite además calcular varios indicadores de gestión del laboratorio, ayudando así a mantener una dinámica de mejora continua del servicio.

El Capítulo V se centra en uno de los ámbitos que, por su naturaleza, mayores riesgos entraña para la seguridad del paciente: el bloque quirúrgico. Tras una revisión general de los procedimientos habituales para la organización y gestión de su actividad, se analizan los puntos esenciales para la seguridad del paciente y se presentan las metodologías de prevención más extendidas en la actualidad. Finalmente, se detallan las aportaciones de las TIC en las distintas fases y aspectos del proceso quirúrgico: control de instrumental, digitalización de procedimientos, integración con la historia clínica electrónica, análisis de eventos adversos, alertas, riesgo quirúrgico, etc.

En el Capítulo VI se analiza la unidad de cuidados intensivos, otro entorno que tradicionalmente supone mayores riesgos en materia de seguridad del paciente. Este capítulo comienza definiendo el perfil del paciente crítico, e identificando en consecuencia las principales fuentes de riesgos para su seguridad en el ámbito de la UCI. Posteriormente se revisan los sistemas de información clínica más importantes (historia clínica electrónica, órdenes médicas y prescripción de medicamentos entre otros), identificando las necesidades existentes desde la perspectiva de los cuidados intensivos, complementando esta exposición con la integración de los dispositivos de monitorización del paciente, uno de los rasgos más característicos de estos ambientes. Se trata también la importancia de los sistemas de apoyo a la toma de decisiones, una de las

líneas de actuación más importantes de los últimos años, y se explican las aportaciones de las TIC para la mejora de la seguridad del paciente crítico, sin olvidar los riesgos específicamente provocados por el uso de estas nuevas herramientas dentro de la UCI.

El Capítulo VII pone el foco en la gestión de la seguridad transfusional, uno de los procesos en los que se da una mayor prevalencia de errores humanos como causa de eventos adversos. Tras establecer una separación entre la seguridad del producto y la seguridad del proceso, se explican las distintas etapas de este último y se enumeran los errores más comunes, ofreciendo además datos sobre la frecuencia con la que se producen. Esto permite identificar los principales riesgos y cuantificar su impacto en la seguridad del paciente, definiendo en consecuencia las prioridades a la hora de adoptar precauciones y orientando las mejoras que las TIC pueden aportar en este ámbito.

Finalmente, el Capítulo VIII trata la seguridad de la información, un concepto totalmente distinto del de seguridad del paciente, aunque en algunas ocasiones se han llegado a confundir. En este capítulo se estudia la primera desde la perspectiva de la segunda, utilizando la tradicional división en las componentes de confidencialidad, integridad y disponibilidad para identificar posibles riesgos para la seguridad del paciente, así como las posibles soluciones que ofrecen las TIC. Se realiza también un repaso de la legislación relacionada actualmente vigente en España (que incluye las directivas aprobadas por la Unión Europea), para después pasar a estudiar el conflicto perenne entre protección de datos y seguridad clínica. Llegados a este punto se dan situaciones en las que entran en colisión varias normativas, hasta el punto de requerir la intervención de las autoridades competentes.

## Bibliografía

- [1] Carnicero J. y Rojas D. Lessons learned from implementation of information and communication technologies in Spain's healthcare services: issues and opportunities. *Appl Clin Inform* 2010; 1(4):363-76.
- [2] Allué N., Chiarello P., Bernal Delgado E., Castells X., Giraldo P., Martínez N. Sarsanedas E., Cots F. Impacto económico de los eventos adversos en los hospitales españoles a partir del Conjunto Mínimo Básico de Datos. *Gac Sanit.* 2014; 28(1):48-54.

## Capítulo I

# Conceptos básicos de seguridad de los pacientes

*Pedro Parra Hidalgo*



### Resumen

La calidad de la asistencia sanitaria es un concepto complejo que combina diversas dimensiones como la efectividad, la eficiencia, la accesibilidad, la personalización, la satisfacción, y la seguridad del paciente. Esta última se define como “la ausencia de daño innecesario, real o potencial, asociado a la atención sanitaria”, y obedece al interés de los sistemas sanitarios por no causar daños evitables como consecuencia de la prestación asistencial.

A partir de esta definición, la seguridad del paciente obliga a establecer varios conceptos relacionados, como riesgo, daño asociado a la atención sanitaria, incidente relacionado con la seguridad del paciente, incidente sin daños, incidente con daños (evento adverso), reacción adversa, efecto secundario, o error. Este último se define como “el hecho de no llevar a cabo una acción planeada o de aplicar un plan incorrecto”.

La importancia de la seguridad del paciente puede estimarse a partir de las cifras contempladas en diversos estudios, que cuantifican los efectos negativos de los eventos adversos en problemas de salud evitables, costes económicos e incluso fallecimientos. Por lo tanto, no es de extrañar que

durante los últimos años se hayan promovido a escala mundial diversas estrategias para la mejora de la seguridad del paciente, auspiciadas por organismos como la Organización Mundial de la Salud, la Organización para la Cooperación y el Desarrollo Económicos, la Agencia para la Investigación y Calidad de la Asistencia estadounidense (AHRQ) y la Unión Europea.

Fruto de estas estrategias son medidas y acciones para la gestión de la calidad y seguridad de la asistencia, como los análisis de causas-raíz, los análisis modales de fallos y efectos, los sistemas de notificación, el impulso de una cultura corporativa de la seguridad, o la monitorización de la seguridad del paciente. En el ámbito de esta última se han desarrollado varios indicadores de resultados que miden la ocurrencia de complicaciones y efectos adversos. Como resultado de todo ello, se han definido varias recomendaciones y buenas prácticas encaminadas a garantizar la máxima seguridad posible durante el cuidado del paciente.

## Concepto de calidad asistencial. Dimensiones de la calidad.

Según el diccionario de la lengua española, calidad es la propiedad o conjunto de propiedades inherentes a algo, que permiten juzgar su valor. En los diferentes sectores de actividad se ha ido desarrollando un cuerpo de conocimientos y unas metodologías para medir la calidad de sus productos o servicios, de modo que permitan apreciarlos como igual, mejor o peor que los restantes de su misma especie. Así, la calidad de la atención sanitaria va a ser el conjunto de propiedades que son inherentes a los servicios de salud y que permiten establecer una comparación entre el desempeño de una organización y el de otras similares o entre el desempeño de la misma organización en momentos diferentes del tiempo.

El desarrollo de este cuerpo de conocimientos ha estado ligado a la transformación de los modelos tradicionales de prestación de servicios sanitarios orientados por profesionales en modelos empresariales de producción de servicios centrado en los clientes [1].

Los trabajos de Codman en 1914 fueron la base que llevó a la asociación de cirujanos norteamericana, American College of Surgeons

(ACS) a la creación en 1918, del programa de estandarización de hospitales que incluía como requisitos para prestar una asistencia de calidad la cualificación del personal, la calidad y uso de la documentación clínica, el tratamiento y la revisión de la asistencia por colegas (peer review).

En 1952 el ACS junto con otras organizaciones crearon la Joint Commission on Accreditation of Hospitals (JCAH) con el objetivo de dar continuidad al programa de estandarización. La JCAH como entidad acreditadora de las instituciones sanitarias que reciben fondos de los programas federales ha desempeñado un papel fundamental en el desarrollo de los programas de gestión de la calidad. La publicación de “La evaluación de la calidad de la atención médica” [2] con la formulación de la estrategia sobre la evaluación de la calidad asistencial basada en la estructura, proceso y los resultados, supuso un hito en la historia de la gestión de la calidad.

En 1972 se crea en Estados Unidos la Professional Standards Review Organization (PSRO) con el objetivo de revisar la calidad de la atención que prestaban los hospitales concertados con los programas Medicare y Medicaid. El propósito del programa era asegurar que los servicios ofrecidos eran necesarios desde el punto de vista médico, de calidad según estándares profesionales y lo más económicos posibles.

En los países europeos la gestión de la calidad en los sistemas sanitarios no se impulsa hasta la década de 1980. En este año la OMS señalaba en el documento “Salud para todos en el año 2000” que “De aquí a 1990, todos los estados miembros deberán de haber creado unas comisiones eficaces que aseguren la calidad de las atenciones a los enfermos en el marco de sus sistemas de prestaciones sanitarias...”.

En 1990 la JCAH revisa su estrategia e incorpora la orientación a resultados, la mejora continua de la calidad y la necesidad de implicar a los profesionales en los proyectos de mejora de la calidad, transformándose en la Joint Commission on Accreditation of Health Organizations (JCHAO). La evolución de este enfoque ha permitido el desarrollo de conjuntos de indicadores de calidad sobre los procesos y los resultados de las organizaciones sanitarias.

## Definiciones de calidad asistencial

No hay una definición universal del concepto de calidad de la atención sanitaria. Las definiciones existentes responden a distintas interpretaciones del significado de atender las necesidades de atención sanitaria. Algunas de las más conocidas son:

- Donabedian (1980): Calidad asistencial es el tipo de asistencia esperado para maximizar el nivel de bienestar del paciente, una vez tenido en cuenta el balance entre beneficios y pérdidas esperadas en todas las fases del proceso de atención.
- Oficina Regional Europea de la OMS (1985): La calidad de la atención sanitaria consiste en asegurar que cada paciente recibe el conjunto de servicios diagnósticos y terapéuticos más adecuados para conseguir una atención sanitaria óptima, teniendo en cuenta todos los factores y los conocimientos del paciente y del servicio médico, y lograr el mejor resultado con el mínimo riesgo de efectos iatrogénicos y la máxima satisfacción del paciente con el proceso.
- Ministerio de Sanidad del Reino Unido (1997): Calidad asistencial es hacer las cosas adecuadas, a las personas adecuadas, en el momento preciso y hacer las cosas bien a la primera.
- Instituto de Medicina de Estados Unidos (2001): La calidad de atención es el grado en el cual los servicios de salud prestados a personas y poblaciones aumentan la probabilidad de obtener los resultados deseados de salud y son coherentes con los conocimientos profesionales del momento.

La calidad de la atención es un concepto complejo en el que se identifican distintos componentes de la calidad que pueden ser medidos y se conocen como las dimensiones de la calidad asistencial. Vamos a revisar las más citadas y sobre las que hay un mayor consenso:

- La efectividad y la eficiencia son dos dimensiones que están incluidas en todas las definiciones de calidad asistencial. La efectividad es la medida en que una determinada práctica o atención sanitaria mejora el estado de salud de población que la recibe, es decir, el beneficio que se obtiene tras una intervención en condiciones de aplicabilidad reales.
- La eficiencia se define en términos de relación entre coste y resultado, Es el grado en el que se consigue el más alto nivel de calidad con los recursos disponibles. Relaciona los resultados obtenidos, medidos por la efectividad, con los costes que genera el servicio prestado.

- La accesibilidad consiste en la facilidad con que puede obtenerse la atención sanitaria en relación con limitaciones económicas, organizativas, geográficas o culturales. Algunos autores incluyen en ella el concepto de equidad como la medida en que los cuidados apropiados son recibidos por la población de forma equitativa, es decir, si la atención sanitaria llega a quien la necesita y cuando la necesita.
- La atención centrada en el paciente, aunque no tiene una definición globalmente aceptada, se refiere al grado en que son tenidos en cuenta en el proceso de atención los valores y las preferencias de los pacientes, mientras que la satisfacción es la medida en que la atención sanitaria cumple con las expectativas de los usuarios.

Como hemos podido comprobar, la seguridad, referida a la reducción del riesgo, es un componente importante de las definiciones que hemos revisado de calidad asistencial, y se consideraba tradicionalmente que estaba incluida en la calidad científico-técnica de la atención.

## La seguridad del paciente como dimensión de la calidad asistencial

Los sistemas sanitarios son organizaciones con una compleja interacción entre relaciones humanas, recursos tecnológicos, conocimientos científicos y condiciones de los pacientes que con frecuencia producen daños innecesarios a los pacientes.

El interés por no producir daños innecesarios a los pacientes ha formado parte históricamente de las preocupaciones de los profesionales sanitarios. En la década de los 50 del siglo XX se publican trabajos sobre los efectos indeseables de la atención sanitaria y se relacionan con el progreso de los métodos diagnósticos y terapéuticos en la medicina. Es en la década de los ochenta cuando la Sociedad Americana de Anestesiología lanza el término Patient Safety con la creación en 1985 de la Anesthesia Patient Safety Foundation.

La publicación del informe “To err is human” en 1999 por el Instituto de Medicina de Estados Unidos [3] puso de manifiesto que la octava causa de mortalidad en EEUU está relacionada con los errores en la atención sanitaria y supuso una inflexión que ha convertido la seguridad del paciente en una prioridad en los sistemas de salud de todo el mundo que han desarrollado estrategias para el control de los daños evitable en la atención sanitaria.

La seguridad ha aflorado como una de las dimensiones de la calidad asistencial y la OMS la define como “la ausencia de daño innecesario, real o potencial, asociado a la atención sanitaria” [4]. A diferencia de las otras dimensiones de la calidad que ponen el foco en conseguir los máximos niveles posibles de beneficio en salud y de satisfacción para el paciente, la seguridad se enfoca en reducir un efecto indeseado como es el daño o riesgo de daño producido por la propia asistencia sanitaria.

Como se ha señalado, la extensión de la conceptualización de la seguridad no solo al daño real, sino también a aquellos fallos de la atención que potencialmente podrían causar daño, hace que se solape con otras dimensiones de la calidad y, en especial, con la efectividad. Este solapamiento refuerza la indisolubilidad de la seguridad como una dimensión de la calidad, y la necesidad de integrar su gestión con la gestión y mejora de la calidad [5].

El Programa de Seguridad del Paciente de la OMS ha definido el Marco Conceptual de la Clasificación Internacional para la Seguridad del Paciente con el fin de elaborar términos aceptables a escala internacional para recopilar, codificar y clasificar los acontecimientos en relación a la seguridad del paciente. [4]. En la Tabla I.1 se relacionan los principales conceptos de esta Clasificación.

<b>Tabla I.1. Conceptos Clave para la Seguridad del Paciente.</b>	
<b>Término</b>	<b>Definición</b>
Seguridad del Paciente	Reducción del riesgo de daño innecesario asociado a la atención sanitaria hasta un mínimo aceptable
Riesgo	Probabilidad de que se produzca un incidente
Daño asociado a la atención sanitaria	Daño derivado de planes o medidas adoptados durante la prestación de asistencia sanitaria o asociado a ellos, no el debido a una enfermedad o lesión subyacente.
Incidente relacionado con la seguridad del paciente	Evento o circunstancia que ha ocasionado o podría haber ocasionado un daño innecesario a un paciente.
Incidente sin daños	Incidente que alcanza al paciente, pero no causa ningún daño apreciable
Incidente con daños (evento adverso)	Incidente que produce daño a un paciente
Reacción adversa	Daño imprevisto derivado de un acto justificado, realizado durante la aplicación del procedimiento correcto en el contexto en que se produjo el evento.
Efecto secundario	Efecto conocido, distinto del deseado primordialmente, relacionado con las propiedades farmacológicas de un medicamento.
Error	El hecho de no llevar a cabo una acción prevista según se pretendía o de aplicar un plan incorrecto.
Fuente: <a href="http://www.who.int/patientsafety/implementation/icps/icps_full_report_es.pdf">http://www.who.int/patientsafety/implementation/icps/icps_full_report_es.pdf</a>	

## El error en la atención sanitaria

Los modelos explicativos de los problemas de seguridad del paciente pretenden comprender las razones por las que pueden producirse los problemas de seguridad y averiguar de qué forma se puede intervenir para su prevención.

El modelo del queso suizo de Reason [6] es utilizado para analizar la causalidad de los accidentes. Según este modelo las defensas o barreras de una organización para evitar los fallos (formación de los profesionales, tecnología disponible, organización,...) se pueden representar como las rebanadas de un queso suizo. Los agujeros en las rebanadas son los fallos que pueden aparecer aleatoriamente en cada una de las barreras. El sistema produce fallos cuando los agujeros de cada rebanada se alinean y permiten que un peligro pase a través de todos ellos y provoque el fallo. El problema no es que aparezca un fallo o error en el sistema, sino que concurren varios a la vez.

Se define el error como el hecho de no llevar a cabo una acción planeada o de aplicar un plan incorrecto. Los errores pueden ser de comisión, si se hace algo erróneo; o de omisión, que se produce por no haber hecho lo correcto.

A la hora de analizar errores es importante diferenciar entre fallo humano y fallo del sistema. Al error humano se le conoce como fallo activo y son los cometidos por los profesionales que están en contacto directo con el paciente. Son fáciles de identificar y casi siempre implican a alguien situado en la primera línea asistencial. Dentro de esta categoría entran los despistes, lapsus u olvidos, equivocaciones o incumplimiento de normas establecidas.

Los fallos del sistema se conocen como fallos latentes y están referidos a circunstancias o fallos relacionados con la gestión y la organización, como diseños inadecuados del proceso, problemas relativos al equipamiento o a la cantidad, cualidad y organización del personal.

Los dos tipos de fallos son importantes para entender las causas de la producción de incidentes de seguridad, aunque ningún incidente de seguridad será correctamente entendido si no se han averiguado cuales han sido las circunstancias del sistema que lo han hecho posible.

Centrar las actuaciones en culpar a los profesionales cuando se produce un error conduce a ocultar los fallos, impedir el aprendizaje y a la repetición del incidente, mientras que centrarse en los fallos del sistema permite encontrar soluciones y rediseñar los procesos para impedir que el error humano pueda producirse o que, en caso de que se produzca, el sistema haya incorporado mecanismos para detectarlo y solucionarlo antes de que afecte al paciente.

## Magnitud e importancia de la seguridad del paciente

El informe “To err is human” del Instituto de Medicina de Estados Unidos estimaba que anualmente fallecían entre 44.000 y 98.000 norteamericanos debido a fallos y errores cometidos en el sistema sanitario de los Estados Unidos [3]. La base de las estimaciones realizadas por el IOM fue el estudio de Brennan publicado en 1991, conocido como estudio Harvard, sobre una cohorte de 30.000 pacientes hospitalizados en 51 hospitales de agudos del estado de Nueva York. En este estudio se estimaban 3,8 eventos adversos por cada 100 pacientes atendidos de los cuales los investigadores consideraban evitables casi la tercera parte [7].

Otros estudios retrospectivos han sido llevados a cabo con posterioridad en otros países (Australia, Dinamarca, Reino Unido, Nueva Zelanda, Francia, Canadá y España). Aunque las metodologías utilizadas han sido diferentes, en general, los resultados señalan que aproximadamente un 10% de los pacientes hospitalizados sufre un evento adverso como consecuencia de la atención hospitalaria, con un intervalo entre 4% y 17%. Se considera que alrededor de un 50% de estos eventos podrían haberse prevenido aplicando prácticas seguras. Los eventos adversos más frecuentes están relacionados con el uso de medicamentos y con la infección nosocomial.

En España se realizó en 2005 el estudio ENEAS [8], un estudio retrospectivo con una muestra de 5.624 pacientes en 24 hospitales con una metodología de revisión de historias clínicas. La incidencia de efectos adversos relacionados con la asistencia sanitaria fue de 9,3%. El 37% de estos efectos adversos estaba relacionado con la medicación, el 25% con las infecciones nosocomiales y otro 25% con problemas técnicos durante un procedimiento. El 42,8% de los efectos fueron considerados evitables.

Los estudios realizados en Atención Primaria ofrecen resultados dispares. En España el estudio APEAS encontró una prevalencia de 18,6 sucesos adversos por 1.000 consultas de los cuales el 70% fueron considerados evitables. El 55% de los eventos adversos estuvieron relacionados con la medicación prescrita [9].

También en España se ha realizado el estudio SYREC en 79 unidades de cuidados intensivos. Es un estudio de cohortes prospectivo basado en la notificación de incidentes por los profesionales de las unidades. Se estimó en 73% el riesgo de sufrir un incidente sin daño y de un 40% para sufrir un evento adverso. Los eventos adversos más frecuentes estaban relacionados con los cuidados y las infecciones y el 60% fueron clasificados como evitables o potencialmente evitables [10].

Los eventos adversos tienen consecuencias sobre la salud y sobre el consumo de recursos. En el estudio ENEAS el 31,4% de los pacientes con eventos adversos tuvo un incremento de 6,1 estancias adicionales. Se ha realizado una estimación del impacto económico de los eventos adversos en los hospitales españoles a partir del Conjunto Mínimo Básico de Datos para el período 2008-2010. Los eventos adversos añaden un coste incremental medio entre 5.260€ y 11.905€. En conjunto, los autores estiman el coste incremental total en más de 88 millones de euros, un 6,7% del total del gasto sanitario [11].

## Las estrategias de seguridad del paciente en el ámbito internacional

La OMS aprobó en 2002 la resolución WHA55.18 en la que se instaba a los estados miembros a priorizar la seguridad de los pacientes y a establecer todo tipo de mejoras que dispongan de suficiente base científica.

En 2004 la OMS pone en marcha la Alianza Internacional para la Seguridad del Paciente cuyas iniciativa y actividades están suponiendo un liderazgo internacional [12]. La Alianza ha ido desarrollando líneas de actuación en temas específicos y, en la actualidad tiene en marcha las siguientes trece áreas de actuación:

1. Retos Mundiales para la Seguridad del Paciente que incluyen:

- “Una atención limpia es una atención más segura” para disminuir las infecciones asociadas a la atención sanitaria y con especial énfasis en la higiene de las manos, y
  - “La cirugía segura salva vidas” que tiene como foco principal la implementación de la lista de verificación de la seguridad en cirugía.
2. Pacientes por la seguridad del paciente: para la construcción de una red global de pacientes y organizaciones de pacientes para participar en la mejora de la seguridad.
  3. Investigación para la Seguridad del Paciente: que promueve estudios para mejorar los instrumentos y los métodos para los estudios de prevalencia y otras herramientas de medición.
  4. Clasificación Internacional para la Seguridad del Paciente: para armonizar a nivel internacional las normas para recoger, codificar y analizar los factores relevantes para la seguridad del paciente.
  5. Notificación y aprendizaje: con el objetivo de desarrollar instrumentos y guías para la implementación y mejora de los sistemas de notificación.
  6. Soluciones para la Seguridad del Paciente: que difunde intervenciones y acciones que han probado su efectividad para prevenir y reducir los riesgos para los pacientes.
  7. “High 5s”: es un proyecto colaborativo entre un grupo de países que tiene como objetivo facilitar la implementación y evaluación de medidas de seguridad dentro de una comunidad de aprendizaje. Han lanzado proyectos de conciliación de la medicación, cirugía en el sitio correcto y gestión segura de medicamentos inyectables.
  8. Tecnología para la Seguridad del Paciente: dirigida a generar oportunidades para la contribución de las nuevas tecnologías a la seguridad del paciente.
  9. Gestión del Conocimiento: trabaja con los estados miembros y otros socios para recopilar y compartir el conocimiento sobre seguridad del paciente.
  10. Eliminación de las infecciones asociadas a catéter venoso central: que pretende replicar los resultados obtenidos en Michigan para disminuir estas infecciones, especialmente en pacientes de unidades de cuidados intensivos.
  11. Educación para una atención sanitaria más segura: desarrolla una guía curricular para estudiantes de medicina y otras profesiones sanitarias.

12. Premio de Seguridad: es un reconocimiento internacional a la excelencia en la mejora de la seguridad del paciente.
13. Listas de verificación: aprovechando el éxito de la lista de verificación en cirugía se pretende elaborar listas de verificación en otras áreas.

La Organización para la Cooperación y el Desarrollo Económico puso en marcha en el año 2001 el proyecto de Indicadores de Calidad Asistencial de la OCDE (OECD Health Care Quality Indicators Project) que tiene como objetivo medir la calidad asistencial con indicadores de proceso y resultado. El proyecto ha incorporado indicadores para la monitorización de la seguridad del paciente teniendo en cuenta especialmente los propuestos por la Agencia para la Investigación y Calidad de los Cuidados de Salud de Estados Unidos (AHRQ).

La Comisión Europea creó en 2004 el High Level Group on Health Services and Medical Care que cuenta con un grupo de trabajo en seguridad del paciente denominado Working Patient Safety Group (WPSG). Tiene como misión establecer recomendaciones para el desarrollo e implementación de estrategias en seguridad del paciente en el marco nacional e internacional y está impulsando una red para promover el intercambio de buenas prácticas entre los países miembros.

### **Actividades para la gestión de la calidad y la seguridad**

Los principios y métodos de la gestión de la calidad son aplicables también a la mejora de la seguridad. Por tanto, las actividades para la gestión de la calidad y la seguridad serán una combinación de actividades dirigidas a planificar o diseñar la calidad, actividades de monitorización para asegurarse que no hay problemas de calidad y que se actúa según lo planificado, y la puesta en marcha de ciclos de mejora cuando a través de la monitorización se identifiquen problemas de calidad.

En el caso de la seguridad del paciente, como en otras dimensiones de la calidad asistencial y dentro del marco común metodológico, se han desarrollado algunas herramientas específicas como los sistemas de notificación de incidentes y la promoción de la cultura de seguridad, y por otro lado, se han adaptado al sector sanitario dos herramientas procedentes de la industria de probada utilidad para el análisis de

riesgos, el Análisis Causa-Raíz (ACR) y el Análisis Modal de Fallos y Efectos (AMFE). Vamos a revisarlos sucintamente.

### Sistemas de notificación

Los sistemas de notificación son considerados una herramienta para la identificación de incidentes con el objetivo de mejorar la seguridad aprendiendo de los errores. Existe un amplio consenso sobre su importancia y sobre su carácter no punitivo y una amplia variabilidad acerca de su forma de implementación. Son útiles para identificar oportunidades de mejora, pero no son válidos para hacer estimaciones de la frecuencia y de la tendencia de los incidentes de seguridad.

Las principales características que deben tener estos sistemas son:

- Voluntariedad. Fomentando la participación en organizaciones donde haya una cultura de seguridad.
- Confidencialidad. La información relacionada con el incidente no se transfiere a terceras partes.
- El sistema debe ser independiente de cualquier autoridad.
- Los incidentes deben analizarse por profesionales experimentados en el marco de equipos multidisciplinares.
- Retroalimentación con informes y recomendaciones a los interesados.
- No punitivo, de modo que los profesionales que notifican estén libres de represalias como consecuencia de la notificación.

El consenso sobre su importancia y la recomendación de implementarlos no se acompaña de evidencias de su efectividad para la mejora de la seguridad. Un informe de 2012 de una muestra de 189 hospitales de Estados Unidos señala que se notificaron un 14% de los incidentes, se investigaron un 30% de ellos y se realizó alguna intervención en el 12% de los analizados [13].

### La cultura de seguridad

Al igual que sucede con los sistemas de notificación hay un amplio consenso sobre el hecho de que las organizaciones que han desarrollado una cultura de seguridad (aviación, industria nuclear...) consideran que ésta ha sido un elemento clave para alcanzar sus objetivos.

El desarrollo de la cultura de seguridad en las organizaciones sanitarias es propuesto como un requisito estructural para crear las condiciones que permitan aprender de los errores y tratar de que no vuelvan a producirse. Sin embargo, no hay suficientes evidencias del impacto de las intervenciones para impulsar la cultura de seguridad y sobre los resultados obtenidos.

Se han desarrollado diversos instrumentos para medir la cultura de seguridad en las diferentes organizaciones de los servicios de salud. El objetivo de estos cuestionarios es conocer la situación en cada organización e identificar las acciones para mejorarla. Los principales instrumentos han sido elaborados en Estados Unidos: Hospital Survey on Patient Safety Culture, The Safety Attitudes Questionnaire y el Patient Safety Climate in Healthcare Organizations Survey. El primero de estos cuestionarios, elaborado por la AHRQ fue adaptado al contexto español como resultado de una cooperación entre el Ministerio de Sanidad y Consumo y la Universidad de Murcia y aplicado a una muestra representativa de hospitales del Sistema Nacional de Salud [14]. Asimismo, se ha realizado una validación del cuestionario MOSP para medir la cultura de seguridad en atención primaria [15].

#### Análisis de Causas-Raíz (ACR)

El ACR es una herramienta de análisis retrospectivo de los incidentes de seguridad, encaminada a identificar qué, cómo y por qué ocurrieron, con el objetivo de diseñar e implementar las intervenciones oportunas para evitar su recurrencia.

Es una herramienta que se emplea en la industria y que se introduce en los servicios de salud desde 1997, año en el que la Joint Commission empezó a exigir que se empleara para investigar los eventos centinela. Las fases de un ACR son:

- Elección del tema. Se suele utilizar para eventos centinela y eventos graves modificables.
- Formación del equipo. Es un elemento crítico porque los resultados van a depender de la experiencia y de la subjetividad de los miembros del equipo.

- Recogida de la información sobre el paciente, los profesionales implicados, los equipos utilizados y la situación en que se ha producido.
- Análisis de la información a través de técnicas como la lluvia de ideas, técnica de grupo nominal, diagrama de flujo, set de preguntas de cribaje y alerta, reglas para la causalidad y clasificación de las causas.
- Elaboración de informe con la formulación de las medidas correctoras.
- Seguimiento de la implementación y del resultado de las medidas aplicadas.

### Análisis Modal de Fallos y Efectos (AMFE)

El Análisis Modal de Fallos y Efectos es una herramienta que permite identificar, evaluar y diseñar estrategias de mejora de los posibles fallos de un proceso o producto. Es una técnica de análisis proactivo que analiza los posibles riesgos, asignándole prioridad y permitiendo actuar preventivamente.

Las fases para la realización de un AMFE son:

- Definir el tema a analizar a través de la identificación de las situaciones que suponen daños potenciales.
- Formación del equipo de análisis que ha de ser multidisciplinar y con conocimiento de esta metodología.
- Describir todos los pasos del proceso a evaluar a través de un diagrama de flujo.
- Realizar el análisis de riesgos a través de:
  - Listado de posibles fallos.
  - Definir la gravedad y probabilidad.
  - Estimar la prioridad del riesgo.
- Diseñar la intervención y las medidas para comprobar su efectividad.
- Seguimiento de la implementación y del resultado de las medidas aplicadas.

### Monitorización de la seguridad del paciente

La monitorización es una actividad sistemática que tiene como objetivo identificar potenciales oportunidades de mejora que deben ser analizadas y, en su caso, objeto de intervenciones para conseguir su mejora. Se han desarrollado conjuntos de indicadores para detectar problemas de seguridad del paciente y controlar el mantenimiento de las mejoras.

Los conjuntos de indicadores elaborados para eventos centinelas están basados en problemas relevantes de seguridad, son de baja frecuencia y su detección es costosa y dependen de la notificación voluntaria de los profesionales. La presencia de un solo caso debe conducir a un análisis de causas para rediseñar el proceso afectado, pero dada su baja frecuencia no está demostrada su efectividad para su empleo en actividades de monitorización.

El enfoque más generalizado para monitorizar problemas de seguridad del paciente es a través de indicadores de resultado, donde destaca claramente la propuesta de indicadores de la AHRQ que aparecen en la Tabla I.2.

<b>Tabla I.2. Indicadores de Resultado en Seguridad del Paciente a nivel de hospital. Agency for Healthcare Research and Quality.</b>
Mortalidad en GRD de baja mortalidad
Ulcera de decúbito
Cuerpo extraño tras intervención
Neumotórax iatrogénico
Infección sanguínea asociada a catéter venoso central
Fractura de cadera postoperatoria
Hemorragia o hematoma postoperatorio
Trastorno metabólico y fisiológico postoperatorio
Fracaso respiratorio postoperatorio
Embolismo pulmonar o trombosis venosa profunda
Sepsis postoperatoria
Dehiscencia de herida quirúrgica
Punción o laceración accidental
Reacción transfusional
Trauma o lesión perinatal en neonato.
Trauma obstétrico en parto vaginal con instrumentos
Trauma obstétrico en parto vaginal sin instrumentos
Fuente: <a href="http://qualityindicators.ahrq.gov/downloads/modules/psi/v31/psi_guide_v31.pdf">http://qualityindicators.ahrq.gov/downloads/modules/psi/v31/psi_guide_v31.pdf</a>

Estos indicadores miden la presencia de complicaciones y efectos adversos a partir de las bases de datos clínico-administrativas de los centros. Su interpretación requiere de múltiples ajustes. La propia AHRQ ha publicado una evaluación en la que reconoce las dificultades de validez e interpretación de los indicadores [16]. Asimismo, se cuestiona su utilidad para la puesta en marcha de acciones de mejora al

no tener los indicadores relación con procesos específicos. También se cuestiona su utilidad para detectar tendencias y para comparar hospitales debido a la inestabilidad de los resultados por su baja frecuencia.

Por último, hay un enfoque alternativo basado en indicadores elaborados sobre aspectos de estructura o de proceso sobre los que hay evidencia científica de su influencia en la seguridad del paciente.

La AHRQ publicó en 2001 una revisión de la evidencia sobre las intervenciones para mejorar la seguridad del paciente en el informe “Making Health Care Safer: A critical Analysis of Patient Safety Practices” que, aunque fue criticado porque clasificó con un nivel bajo de evidencias algunas intervenciones ampliamente aceptadas, se ha utilizado como base para trabajos posteriores [17]. A partir de la revisión de la AHRQ, el National Quality Forum publicó en 2003 “Safe Practices for Better Health Care” que es un listado de prácticas de alta prioridad para ser implementadas, basadas en la evidencia científica de su efectividad en relación a la seguridad del paciente y a su posible generalización. Este listado ha sido revisado por última vez en 2010 [18]. Tomando como eje estas prácticas se han elaborado listados de indicadores que son más fáciles de interpretar y con menos problemas de validez cuanto mayor sea la evidencia sobre la que se apoyan. Por encargo del Ministerio de Sanidad se realizó una medición en una muestra de hospitales del Sistema Nacional de Salud [19].

La AHRQ ha publicado en 2013 una actualización de la revisión de la evidencia con el informe “Making Health Care Safer II” [20] que incorpora nuevas intervenciones y tiene en cuenta en la valoración además de la evidencia de la efectividad, el potencial de daño, el coste de implementación y la dificultad del proceso de implementación. El Informe de 2013 propone una lista de 10 intervenciones fuertemente recomendadas, y otras 12 recomendadas (véase Tabla I.3).

Tabla I.3. Prácticas recomendadas por la Agency for Healthcare Research and Quality

I) Fuertemente recomendadas	I.1. Checklist pre-quirúrgicos y de anestesia para prevenir eventos durante y después de la cirugía.
	I.2. Conjunto de intervenciones (“bundles”) que incluyen checklists para prevenir infecciones asociadas a catéter venoso central.
	I.3. Intervenciones para reducir el uso de catéteres urinarios, incluyendo recordatorios, órdenes para interrumpir su uso, o protocolos de enfermería para retirarlos.
	I.4 Conjunto de intervenciones (“bundles”) que incluyen elevación de la cabecera, paréntesis sin sedación, cuidado bucal con clorhexidina, y tubos de succión subglótica endotraqueal, para prevenir neumonía asociada a ventilador.
	I.5 Intervenciones para mejorar higiene de manos.
	I.6 Listado de abreviaturas no permitidas.
	I.7 Intervenciones multicomponentes para reducir las úlceras por presión.
	I.8 Barreras para prevenir las infecciones asociadas a los cuidados.
	I.9 Uso de ultrasonografía en tiempo real para la colocación de catéter venoso central
	I.10 Intervenciones para mejorar la profilaxis de tromboembolismo venoso.
II) Recomendadas	Intervenciones multifacéticas para prevenir caídas.
	Uso de fármacos clínicos para prevenir acontecimientos adversos relacionados con medicamentos (ADE)
	Documentación de preferencias del paciente para cuidados terminales
	Consentimiento informado para mejorar comprensión de los riesgos potenciales de los procedimientos
	Entrenamiento para trabajo en equipo
	Conciliación de la medicación
	Reducir la exposición a fluoroscopia y tomografía computerizada
	Uso de indicadores de resultado y “report cards” sobre cirugía
	Sistemas de respuesta rápida para paradas
	Utilización de métodos complementarios para detectar eventos adversos y errores médicos en la monitorización de problemas de seguridad
Prescripción electrónica	
Uso de ejercicios de simulación para la seguridad del paciente	
Fuente: <a href="http://www.ahrq.gov/research/findings/evidence-based-reports/services/quality/ptsafetysum.html">http://www.ahrq.gov/research/findings/evidence-based-reports/services/quality/ptsafetysum.html</a>	

## Bibliografía

- [1] Simón P. Ética de las organizaciones sanitarias. Nuevos modelos de calidad. Madrid: Triacastela; 2005.
- [2] Donabedian A. Evaluating the quality of medical care. *Milbank Memorial Fund Quarterly* 1966; 44:166-206.
- [3] Kohn LT, Corrigan JM, Donaldson MS (Editors). To err is human. Building a safer health system. Institute of Medicine. Washington: National Academy Press; 1999.
- [4] OMS. Marco Conceptual de la Clasificación Internacional para la Seguridad del Paciente. Versión 1.1. Informe Técnico, 2009. Disponible en: [http://www.who.int/patientsafety/implementation/icps/icps\\_full\\_report\\_es.pdf](http://www.who.int/patientsafety/implementation/icps/icps_full_report_es.pdf) (Último acceso septiembre 2015).
- [5] Saturno PJ. Seguridad del paciente. Marco conceptual. Enfoques y actividades. Manual del Master en gestión de la calidad en servicios de salud. Universidad de Murcia 2008.
- [6] Reason J. Human error: models and management. *BMJ* 2000; 320:768-770.
- [7] Brennan TA et al. Incidence of adverse events and negligence in hospitalized patients. Results of the Harvard Medical Practice Study I. *N Eng J Med* 1991;324:370-376.
- [8] Aranaz JM et al. Estudio nacional sobre los efectos adversos ligados a la hospitalización: ENEAS 2005. Madrid: Ministerio de Sanidad y Consumo; 2006.
- [9] Estudio APEAS. Estudio sobre la seguridad de los pacientes en atención primaria de salud. Madrid: Ministerio de Sanidad y Consumo; 2008.
- [10] Incidentes y eventos adversos en medicina intensiva. Seguridad y riesgo en el enfermo crítico. SYREC 2007. Madrid: Ministerio de Sanidad, Política Social e Igualdad; 2010.
- [11] Allué N, Chiarello P, Bernal E, Castells X, Giraldo P, Martínez N et al. Impacto económico de los eventos adversos en los hospitales españoles a partir del Conjunto Mínimo Básico de Datos. *Gac Sanit.* 2014;28(1):48-54.
- [12] World Alliance for Patient Safety Programme. Geneva: WHO, 2004. Disponible en <http://www.who.int/patientsafety/about/programmes/en/> (Acceso en septiembre 2015).
- [13] Levinson DR. Hospital incident reporting systems do not capture most patient harm. Department of Health and Human Services, Office of Inspector General, OEI-06-09-00091, Washington; 2012.
- [14] Saturno PJ et al. Análisis de la cultura sobre seguridad del paciente en el ámbito hospitalario del Sistema Nacional de Salud español. Madrid: Ministerio de Sanidad y Consumo; 2009.
- [15] Traducción, validación y adaptación del cuestionario MOSP para medir la cultura de seguridad del paciente en Atención Primaria. Madrid: Ministerio de Sanidad, Política Social e Igualdad; 2010. Disponible en: <http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/docs/MOSPS.pdf>
- [16] AHRQ. Guide to Patient Safety Indicators. Department of Health and Human Services. Agency for Healthcare Research and Quality. Version 3.1 (march 2007). Washington: AHRQ; 2003. Disponible en: [http://qualityindicators.ahrq.gov/downloads/modules/psi/v31/psi\\_guide\\_v31.pdf](http://qualityindicators.ahrq.gov/downloads/modules/psi/v31/psi_guide_v31.pdf)
- [17] Shojania KG, Duncan BW, McDonald KM, et al., eds. *Making Health Care Safer: A Critical Analysis of Patient Safety Practices*. Evidence Report/Technology Assessment No. 43. AHRQ Publication No. 01-E058. Rockville, MD: Agency for Healthcare Research and Quality. July 2001.
- [18] National Quality Forum (NQF). Safe practices for better healthcare-2010 Update: A consensus report. Washington: NQF; 2010. Disponible en: [https://www.qualityforum.org/Publications/2010/04/Safe\\_Practices\\_for\\_Better\\_Healthcare\\_%E2%80%932010\\_Update.aspx](https://www.qualityforum.org/Publications/2010/04/Safe_Practices_for_Better_Healthcare_%E2%80%932010_Update.aspx)
- [19] Indicadores de buenas prácticas sobre seguridad del paciente. Resultados de su medición en una muestra de hospitales del Sistema Nacional de Salud español. Madrid: Ministerio de Sanidad y Política Social; 2009.
- [20] Shekelle PG et al. Making Health Care Safer II: An updated Critical Analysis of the Evidence for Patient Safety Practices. Comparative Effectiveness Review N° 211. AHRQ Publication n° 13-E001-EF. Rockville: Agency for Healthcare Research and Quality; 2013. Disponible en: <http://www.ahrq.gov/research/findings/evidence-based-reports/services/quality/ptsafetysum.html>

## Capítulo II

# Principales fuentes de riesgo: Aportaciones de las tecnologías de la información y la comunicación

*Fernán González Bernaldo de Quirós*

*Carlos Otero*

*Daniel Luna*



## Resumen

Los errores en medicina representan un grave problema de salud pública y constituyen una seria amenaza para la seguridad del paciente. En los últimos años, a partir de una creciente revisión de los procesos de cuidado, las instituciones de salud han tratado de hacer foco en cómo identificar y prevenir o al menos mitigar esos “errores”, sin embargo ninguna iniciativa ha sido totalmente efectiva.

Asociadas a otras iniciativas, las Tecnologías de la Información y la Comunicación (TIC) están siendo utilizadas como una herramienta para reducir los errores y mejorar la seguridad (por ejemplo, mediante el uso de prescripción electrónica asistida y sistemas de soporte a la toma de decisión). Sin embargo, si no son implementadas con cuidado, estas tecnologías no logran ser efectivas y peor aún pueden introducir nuevos errores.

En este capítulo se describe el concepto de error en medicina, el rol de las TIC en la seguridad del paciente y los cuidados que hay que

tener al aplicarlas, se enumeran las principales fuentes de riesgo y cómo abordarlas con las TIC y las estrategias para analizar los riesgos y mitigarlos.

## Introducción: Error en Medicina

El error en medicina no es un concepto nuevo, todo lo contrario, la medicina como toda práctica humana es falible y vulnerable al error. Con el avance de la práctica médica y la estandarización de los procesos de cuidados, la calidad de la asistencia sanitaria ha mejorado, evidencia de esto es que en todas partes del mundo la esperanza de vida ha ido en aumento. Gran responsabilidad en esta mejora en la calidad de atención y la esperanza de vida, le cabe a los avances científicos y al uso de tecnologías para el cuidado de la salud. Sin embargo, estudios realizados en varios países, han demostrado que esos beneficios generaron también riesgos significativos para la seguridad de los pacientes. Desde su publicación en 1999, el reporte del Instituto de Medicina de los Estados Unidos (IOM) titulado “To Err is Human” impactó fuertemente en el tema, por primera vez se contaba con un estimativo cierto del impacto del error en la salud. En un sistema de salud colapsado por los altos costos, el reporte de la IOM denunciaba millonarias pérdidas económicas asociadas al error médico, y más significativo aún daba cifras de entre 44.000 y 98.000 muertes cada año por errores médicos prevenibles en los Estados Unidos. El error representaba ahora entre la quinta y octava causa de muerte [1][2].

La identificación de las fuentes de riesgo en medicina y la reducción de los errores se ha transformado en una preocupación importante y actual en la mejora de la calidad de la atención de salud y la seguridad de los pacientes. Lograr reducir el error médico a su mínima expresión será quizás uno de los mayores desafíos de la medicina del siglo XXI.

Diversas estrategias han sido utilizadas para combatir el error médico, las más visibles, debido a su efectividad, han sido aquellas que se focalizaron en estandarización de los procedimientos y guías de práctica clínica, educación al equipo de salud en la detección del riesgo y prevención del error; esfuerzos en lograr una comunicación efectiva y trabajos puntuales en el ciclo de la medicación y el empoderamiento de los pacientes [3][4]. Sin embargo ninguna estrategia será verdaderamente efectiva si se implementa en forma aislada, se requiere de un enfoque sistémico que se inicia con estándares y adhesión a las llamadas buenas prácticas pero que de ninguna manera concluye ahí.

## Breve descripción del concepto de seguridad del paciente

Tanto la Organización mundial de la salud (OMS) como el Instituto de Medicina de los Estados Unidos (IOM), definen a la seguridad del paciente como la ausencia de lesiones a causa de la atención sanitaria, que se supone debe ser beneficiosa. Es importante además consignar que el campo de estudio de la seguridad incluye no sólo los incidentes que causan daño sino también los errores de atención que no lo causan, pero que potencialmente podrían causarlo. En el concepto de daño real o potencial, se encuadra también el riesgo que el paciente sufre o puede sufrir por la ausencia de servicios que resultarían beneficiosos. En otras palabras, la no provisión de una práctica beneficiosa también se considera como una fuente de riesgo [1][5][6][7].

Si bien se han publicado numerosos estudios que intentan dilucidar qué genera riesgo para los pacientes, aun no existe consenso unánime en cómo se genera el riesgo. Uno de los modelos más conocidos es quizás el de “queso suizo” de J. Reason [4], que explica que el riesgo, o en muchos casos el error, aparece como resultado de la alineación de defectos o “agujeros” en las medidas de seguridad y control que hubiesen podido evitarlo. Otra forma de explicarlo sería la existencia de fallos estructurales, procesos inadecuados o, fallos debido a la conducta humana. En un modelo más complejo, aún bajo discusión en el seno de la Alianza Mundial para la Seguridad del Paciente de la OMS y teóricamente útil para la clasificación unívoca de los tipos de incidente, se habla de “factores contribuyentes” a los incidentes de seguridad que acuerdan con la definición de seguridad desde la perspectiva denominada socio-técnica, que incluye a la tecnología (software, hardware), las personas (médicos, técnicos, pacientes), los procesos (normas y flujos de trabajo), la organización (estructura, planeamiento, incentivos), y el ambiente externo (regulaciones, opinión pública, etc.). Independientemente del modelo, lo importante es comprender qué es lo que pone en riesgo al paciente, de forma que se pueda intervenir en su prevención [4][8][9].

## El concepto de error en Medicina y en otras disciplinas

Si bien existió siempre, el reconocimiento del error en medicina como un problema endémico necesitó de una extensa bibliografía que lo pusiera en evidencia. Diversos estudios dejaron en manifiesto lo frecuente y variable del error así también como sus consecuencias.

Aquí vemos una marcada diferencia con otras disciplinas. Producto quizás de un reconocimiento inmediato de la fragilidad del acto humano, sectores con una percepción más alta de riesgo, tales como el de la aviación y la energía nucleares, se adhirieron a estándares de seguridad mucho más altos que los servicios de salud. La aviación es quizás el modelo a imitar cuando se habla de seguridad y prevención de errores. Aunque no es menester nuestro determinar que es más riesgoso, el volar o el ser admitido a un hospital, los números se ocupan de borrar lo subjetivo del análisis. Hoy en día hay una probabilidad de 1 en 1.000.000 de sufrir daño por volar en aviones, mientras que, como mencionamos, esta probabilidad es muchísimo mayor cuando accedemos a atención sanitaria. No fue milagroso lo conseguido en la aviación, donde aún hoy la mayoría de los incidentes se dan a causa del Factor Humano, requirió de la inmediata percepción, por parte de todos los actores involucrados, del concepto seguridad como eje en al desarrollo de procesos y la aplicación de tecnología al servicio de esa seguridad. A pesar de los avances tecnológicos son los humanos quienes serán responsables en última medida del éxito y seguridad en la industria. Estas son cosas que tiene que aprender la medicina de otras disciplinas, resulta perentorio un rápido reconocimiento de la existencia del error médico, reconocimiento desnudo de la soberbia que frecuentemente acompaña el quehacer médico. Como en la aviación, si queremos garantizar la calidad en la atención, se requiere de un abordaje comprometido e interdisciplinario del riesgo en salud [10][11].

Ahora bien, el reconocimiento de lo vulnerable y falible del acto médico así también como la necesidad de un esfuerzo sistémico interdisciplinario es un paso enorme en la dirección correcta, pero avanzar dependerá de un esfuerzo de mejora continua. Otras disciplinas han venido trabajando en la identificación de las fuentes de riesgo y su disminución, y tal vez su éxito se deba a una cuestión que debemos considerar fundamental: examinar en detalle los errores ocurridos y considerar la posibilidad futura de error como una instancia siempre posible. Las disciplinas que mejor manejan la ocurrencia y mitigación del error, son aquellas que aceptan que el riesgo siempre existe. El error puede ocurrir, más allá de las competencias de los profesionales involucrados y por lo tanto planean y desarrollan estrategias para el monitoreo del riesgo y del error [12][13][14].

Aplicando las lecciones aprendidas en otros sectores, sabemos que la adopción de tecnologías innovadoras, la educación de los proveedores

y los consumidores, mejorar los sistemas de notificación de error, y el desarrollo de nuevos incentivos económicos, podría mejorar notablemente la calidad de la atención, con el respectivo descenso del riesgo y el error en medicina.

## El rol de las TIC en la mejora de la seguridad del paciente

La agencia Americana para la investigación y calidad en salud “AHRQ”, por sus siglas en inglés, identifica 6 estrategias eficaces para reducir la incidencia de errores, estas van desde cambios en la cultura organizacional y educación, hasta las que nos compete en este libro: la introducción de tecnología para reducir errores y mejorar la seguridad [15]. No es nuevo considerar a las TIC como una estrategia efectiva para la mejora de la seguridad del paciente. Desde el 2006 en adelante, existen reportes que demuestran que el uso de tecnologías podría reducir los efectos adversos asociados al cuidado de la salud, mejorar la calidad de cuidado y reducir los costos [16][17][18][19]. Las tecnologías de la información han demostrado ser una estrategia adecuada para mejorar la seguridad del paciente. Los registros médicos electrónicos, sobre todo aquellos que poseen sistemas de prescripción electrónica integrados, sistemas de soporte a la toma de decisiones (clinical decision support systems CDSS), estrategias de entrenamiento utilizando simuladores y mecanismos a prueba de fallos en las herramientas de diagnóstico o dispositivos médicos, pueden disminuir el riesgo, evitar errores y reducir el daño [20][21][22][23][24][25].

Por otro lado hay que destacar la utilidad de las TIC en la gestión de la información y cómo una buena gestión del conocimiento puede dar apoyo a programas de seguridad. Como mencionamos anteriormente, las fuentes de riesgo para la seguridad del paciente son cambiantes. En el ambiente clínico actual incorporamos no solo nuevas tecnologías, sino también nuevas prácticas y nuevos procesos que pueden generar nuevos riesgos que se suman a los que ya podíamos tener identificados. En este ambiente se vuelve imprescindible contar con una buena gestión del conocimiento. La aplicación de TIC en salud nos permite, a través del relevamiento y monitoreo continuo, conocer la realidad del nuestro medio y nos da el potencial de ponderar esa realidad con toda aquella información que este contenida en la literatura científica, documentos, sitios web, programas gubernamentales, proyectos en curso y otras realidades. Es lógico suponer que no puedo cambiar lo

que no conozco, como enfrentar o superar los riesgos si no los conozco, no sé su incidencia o cómo mi realidad se compara con la de otras prácticas o referencias. En este sentido, la implementación de TIC tendrá un impacto fundamental en la recuperación y uso secundario de ese conocimiento, pero lo positivo del impacto dependerá de la forma en que se implemente, si no queremos generar nuevos errores o potenciar los existentes [4][13][14][26][27][28][29].

### Nuevos errores inducidos por las TIC en salud “e-iatrogenia”

La potencialidad de generar nuevos problemas al implementar TIC no es un detalle menor, existen numerosos reportes que indican cómo las TIC, sobre todo a partir de implementaciones fallidas, pueden transformarse en nuevas fuentes de riesgo. Los errores inducidos por la tecnología, como los generados por las TIC, son tan importantes y frecuentes que se los ha definido como “iatrogenia tecnológica” o “e-iatrogénesis” [30][31].

Estos errores asociados a la aplicación de TIC pueden deberse a varios factores, entre los que encontramos con frecuencia:

- Usuarios dependientes del sistema, que dejan, en ocasiones de lado el criterio personal, aguardando las indicaciones que el sistema ofrece para evitar errores [32]. Muchas veces, no todas las opciones están contenidas en las alertas programadas, y la falsa confianza puede generar errores.
- Accesos directos o por defecto a opciones propuestas por el sistema que pueden modificar el plan terapéutico o diagnóstico recomendables, por ejemplo para los pacientes de edad avanzada o con bajo peso, lo que puede resultar en dosis tóxicas, o procedimientos inadecuados [33][34].
- Advertencias irrelevantes o frecuentes que pueden interrumpir el flujo de trabajo, o peor aún, limitar la acción del médico innecesariamente, privando al paciente del beneficio del acto médico [25][33].
- Errores generados a partir de sistemas de soporte originados en bases de conocimiento inapropiadas o desactualizadas, en bases de datos deficientes o incompletas, tengamos en cuenta que el producto del sistema de información, por caso CDSS, dependerá en particular de que los datos estén completos y correctos.

La identificación y reconocimiento de este fenómeno iatrogénico permitió también que surjan soluciones que buscan reducir el impacto e incluyen: Cambios en el diseño de las interfaces haciendo uso de técnicas de diseño centrado en el usuario y siguiendo normas de usabilidad; anulaciones de los sistemas automáticos o las opciones por defecto, esto implica a veces generar una instancia de validación extra, como podría ser, ante una indicación una confirmación sobre a qué paciente se le está indicando; brindar adecuado entrenamiento y soporte a todos los usuarios; e implementaciones adecuadas de las TIC con control y seguimiento posterior al proceso de implementación [11] [35][36][37].

## Principales fuentes de riesgo

Conociendo la importancia en la prevención del error, y el impacto que la identificación del riesgo tiene en la calidad de atención, es importante identificar las fuentes de riesgo. En este sentido, las fuentes de riesgo son todas las circunstancias que aumentan la probabilidad de que un paciente sufra un error o esté expuesto a un daño potencial ya sea por la mala atención médica o por la omisión del cuidado debido.

Describiremos aquí algunos las principales fuentes de riesgo para la seguridad del paciente según la Clasificación Internacional para la Seguridad del Paciente (CISP) de la OMS, y como las TIC pueden ayudarnos a prevenirlo.

### Errores administrativos y de documentación

En este apartado se hace referencia al daño o potencial daño surgido a partir de fallas en los procesos de identificación de pacientes y muestras, asignación de turnos, etc. Es este quizás el primer ítem a considerar al momento de implementar TIC, para reducir el impacto de estos errores se deben crear sistemas únicos de identificación de pacientes o lugares, es decir, Tablas Maestras, que son la base del sistema de información.

### Atención clínica

En referencia a los potenciales riesgos que el paciente puede sufrir por la atención clínica que reciba, o por la omisión de servicios recomendados. Aquí se destaca el valor que pueden tener los sistemas de soporte a la toma de decisiones que contribuyen a la adhesión a las mejores prácticas clínicas.

## Prácticas y procedimientos

Hace referencia a los daños a los que las personas se pueden ver expuestas frente a la aplicación de prácticas y procedimientos. En este grupo se encuadran los riesgos asociados a la mala aplicación del método o los efectos no deseados de su uso correcto. Este aspecto puede ser cubierto por los sistemas de soporte a la toma de decisiones. Los CDSS son útiles para lograr adhesión a las mejores prácticas. En este sentido se podría mostrar una recomendación en el momento de indicarse un procedimiento, la recomendación puede tener distintas características y nivel de granularidad para asistir al profesional de la salud que va a realizar la práctica.

## Infecciones asociadas a la atención sanitaria

Tiene que ver con los procesos infecciosos surgidos del contacto del paciente con la institución, en situaciones en las cuales no era esperado. Pensar en las TIC como instrumento educador y de monitoreo. La reducción de este tipo de infecciones se logrará conociendo su incidencia e informando estrategias de prevención.

## Prescripción de medicamentos

Son las fallas o potenciales fallas a las que se ve sometido el paciente en el momento de recibir una medicación, incluyendo los procesos asociados al paciente, como su correcta identificación y preparación, como así también al proceso que involucre a los medicamentos. Ellos tienen que ver con la preparación correcta, la administración adecuada, lo concerniente a alergias, interacciones y dosis y el correcto seguimiento del efecto y control de efectos adversos. Para lidiar con estos fenómenos contamos con múltiples estrategias. Sistemas de códigos que nos permiten cerrar el ciclo de la medicación. Logramos con esto una validación al lado del paciente, en el momento de la administración, y nos aseguramos que esté recibiendo la medicación adecuada, en el momento y lugar adecuado, por la vía adecuada. También disponer de la información en forma ubicua, es decir en todos y cualquier lado cuando la necesito y bases de conocimientos de fármacos curadas que nos permiten explotar el conocimiento y dar soporte a los clínicos sobre posibles dosis inadecuadas o interacciones farmacológicas potencialmente nocivas.

## Procesos que involucran sangre y derivados

Es el riesgo resultante del proceso de contacto del paciente y el personal de salud con sangre y sus derivados, ya sea en los procesos de extracción, como en lo referido a transfusiones y prácticas asociadas. Los sistemas de soporte a la decisión tienen por característica principal, lograr una mayor adherencia a guías de práctica clínica. Recomendaciones brindadas por el sistema en momentos claves pueden evitar errores en el proceso de manejo de sangres y sus derivados. Los sistemas de código de barras resultan útiles también para el seguimiento y correcta identificación de estas muestras.

## Nutrición

Esta fuente de riesgo evalúa los errores asociados al proceso de alimentación y preparación de alimentos, como los riesgos derivados del contacto del paciente, como alergias alimentarias, intolerancias, o patologías como enfermedad celiaca, etc. Nuevamente actuará como instrumento de prevención, el contar con la mejor información posible sobre el paciente y el alimento.

## Errores asociados al manejo de oxigenoterapia y otros gases

Es el riesgo que surge del manejo y manipulación de oxígeno y otros gases. Hay ya disponibles sistemas que pueden censar el requerimiento de oxígeno del paciente y alertar cuando debe ajustarse. De mismo modo los sistemas de soporte pueden sugerir valores y advertir cuando se exceden las recomendaciones, evitando riesgos potenciales como en el caso de la retinopatía del prematuro.

## Comportamiento

Es el riesgo derivado de la conducta inapropiada de los profesionales de salud o los pacientes y sus familiares. Las TIC tienen la potencialidad de acercar a los pacientes al cuidado de su salud, elementos como portales de salud, sistemas de mensajería médico paciente empoderan con conocimiento y mejoran también la relación médico paciente. Se ha demostrado en varias publicaciones que el uso de herramientas TIC actúa en forma positiva en la satisfacción de los pacientes con aquellos encargados de su cuidado.

### Accidente de los pacientes

Son los riesgos que surgen de los accidentes que los pacientes pueden sufrir en el proceso de atención, como por ejemplo el riesgo de caídas. La correcta identificación en el sistema de los pacientes con necesidades especiales acompañadas de alertas que informen de estas, pueden contribuir en la prevención de estos accidentes.

### Infraestructura

Son los riesgos derivados de la infraestructura de atención.

### Gestión y organización

Corresponde a los riesgos pertinentes a cuestiones relacionada con el gerenciamiento y la estructura organizacional. Es en este aspecto donde las TIC pueden dar una mayor contribución como medio de aumento de la calidad de atención médica, impactando en el cuidado que recibe el paciente. El éxito en la gestión de una organización de salud dependerá de cómo se maneja el flujo de información.

Como comentamos estos no son las únicas fuentes de riesgo, pero comprenden los principales factores para la aparición del error y la disminución en la seguridad. Como se evidencia, los pacientes están sometidos a varios o casi todas estas fuentes. Lo mismo sucede con el personal de salud, por lo que su análisis debe ser considerado desde la perspectiva del flujo de trabajo asistencial y en una visión integral que evalúe todas las potenciales causas. Es importante consignar que cuanto más compleja es la situación del paciente, y más especializado su cuidado, mayores son los riesgos a los que se ve sometido, sumándose a su mayor vulnerabilidad. Definir claramente los roles y responsabilidades en la detección y control del riesgo y generar un plan integral para el abordaje del riesgo, que involucre el uso de TIC, es primordial para disminuir el riesgo lo máximo posible.

### Evidencia del beneficio de implementación de las TIC

Como fuimos mencionando al describir cada riesgo, tecnologías, bien implementadas, pueden ser útiles en todos los ámbitos del cuidado de la salud, existen algunas intervenciones particulares que han demostrado

ser particularmente efectivas en la disminución del riesgo. Es importante destacar que el beneficio observable por cada intervención solo será completamente efectivo asociado a las otras y no como un esfuerzo solitario. Para simplificar su entendimiento a continuación se mencionan brevemente algunas de estas estrategias son:

### Sistemas para la correcta identificación de los pacientes

El empadronamiento, la identificación de los pacientes y la existencia de duplicados puede ser el talón de Aquiles en los sistemas de información en salud si no se presta cuidadosa atención durante su implementación y seguimiento. Solo podremos garantizar que el paciente que está siendo atendido se corresponde con la historia clínica y es el correcto si respeta un modelo de empadronamiento único para todo el sistema; un set mínimo de datos con identificaciones transitorias que sean monitoreadas y completadas luego y listas que faciliten el ingreso al paciente correcto. Con el uso de la tecnología es factible asegurarnos que un registro no está duplicado, y que sus datos están actualizados, lo que resulta ser un pilar en el proceso de mitigación de riesgos para la atención de los pacientes [38][39][40]. Es importante remarcar que la tecnología por sí sola no puede garantizar la identificación precisa del paciente. El personal de salud y aquellos dedicado al empadronamiento deben recibir entrenamiento adecuado y seguir procedimientos confiables.

### Historia Clínica Electrónica (HCE)

La implementación de la HCE, quizás el núcleo del sistema de información en salud, ha logrado reducir gran cantidad de tipo de errores, como los asociados a la prescripción de medicamentos, los recordatorios para cuidados preventivos y la organización y estructuración para la solicitud de prácticas y procedimientos. Si bien estos puntos se tratan con más detalle más adelante en este libro, es importante mencionar que la HCE, como integrador de las demás estrategias del uso de TIC, es fundamental para la optimización de los beneficios que estas herramientas pueden tener [18][21][41]. Los avances en la informática en salud y la adopción generalizada de HCE, basadas en estándares internacionales, que permitan que sean interoperables, prometen acceso a los registros de un paciente en cualquier sitio de la atención

sanitaria, logrando una continuidad de cuidado que favorece no solo la seguridad del paciente y la disminución de riesgo, sino que mejora la calidad de cuidado. Sin embargo, este beneficio, puede ser riesgoso si los médicos y los usuarios de estos registros no comprenden y trabajan en respetar cuestiones concernientes por ejemplo a la privacidad del paciente y el valor de la información [21][42][43].

### Sistemas de Prescripción Electrónica (Computerized Provider Order Entry - CPOE)

Los errores en la prescripción son la principal fuente de error prevenible identificada en el proceso de identificación de riesgo y error en medicina [44]. Por su capacidad de aumentar la adhesión a guías de atención, los CPOE han demostrado un enorme potencial para aumentar la calidad del cuidado médico, cuando se implementan correctamente al flujo de trabajo de los trabajadores de salud, reduciendo el tiempo entre prescripción y administración o seguimiento de la orden. Pueden reducir significativamente errores comunes como los asociados a la legibilidad y en el caso particular de los medicamentos agregan otros beneficios como el favorecer la completitud de la orden, recomendar posologías y ofrecer procesos de validación por parte de farmacéuticos y enfermeros.

Uno de los mayores beneficios en el manejo computarizado de las órdenes médicas es el acceso a bases de conocimientos, es así que los CPOE asociados a sistemas de soporte a la decisión, set de órdenes y visualización grafica de datos alcanzan su mayor potencial reduciendo la carga cognitiva del médico y evitando errores.

### Sistemas de soporte

La esencia de los sistemas informatizados es el dar soporte a los procesos humanos. Nada refleja más claramente esto que los Computerized Decision Support System (CDSS).

Los CDSS son herramientas de ayuda basadas en una estructura básica que contempla la mayor evidencia científica disponible para la ayuda a la toma de decisiones profesionales en línea, no reemplazan el juicio medico sino que lo complementan. Se ha demostrado su utilidad

en múltiples procesos de atención, como la prescripción, los procesos diagnósticos, la aplicación de prácticas preventivas, etc. Estos sistemas han demostrado ser efectivos en la mejora de la calidad de atención y en la reducción del error [24][25][45]. Esta efectividad se ve en como los CDSS apoyan al médico en sus tareas, reduciendo la carga cognitiva y alertando ante posibles daños. Actúan reduciendo el riesgo de errores con medicaciones, disminuyendo errores en diagnósticos y aumentando el acceso al conocimiento, dando información confiable y consistente.

### Códigos de barras como estrategia para el manejo de errores de identificación de pacientes y muestras

Los lectores de códigos de barras facilitan y aumentan la precisión en el momento de ingresar datos. La estandarización de un sistema de códigos de barras puede ser útil en la prevención del error y la mitigación del riesgo. Los sistemas de códigos de barras son de utilidad para varias tareas como control y seguimiento de inventario y materiales, validación al momento de la administración de medicamentos e identificación de pacientes a lo largo de su estadía hospitalaria, para evitar errores.

Se cree por ejemplo, que el uso de estas tecnologías puede reducir hasta en un 25% los errores asociados al proceso de medicación. Aun cuando su beneficio ha sido probado, su adopción no fue la esperada, sobre todo en los países en vías de desarrollo. Su máximo potencial se evidencia cuando esta tecnología se aplica a sistemas electrónicos de prescripción en el contexto de HCE [39][40][44].

Herramientas de empoderamiento para pacientes. Portales personales de salud, aplicaciones para teléfonos inteligentes, herramientas interactivas, etc.

Una de las estrategias que la Alianza Mundial para la Seguridad del paciente recomienda, es la incorporación de los pacientes en la prevención del error. Por eso los portales personales de salud, sobre todo aquellos integrados a sistemas de salud informatizados que integran toda la información de los pacientes en un ámbito seguro y confiable, tienen la capacidad de impactar en la seguridad del paciente.

Los portales de pacientes, en versiones web o móviles nos acercan la posibilidad de incorporar al paciente, probablemente el mayor interesado en que no se cometan errores en su proceso de cuidado, como

un escriba de su propio cuidado. El paciente o su cuidador puede ahora controlar su medicación, revisar sus problemas y en forma cada vez más difundida, incluso revisar su historial clínico completo en tiempo real [46]. Es así como con las aplicaciones para teléfonos móviles o apps, y las herramientas interactivas para el cuidado de la salud, tienen, y van a tener en el futuro, un rol fundamental en la identificación del riesgo y la prevención del error. Los pacientes, mediante estas tecnologías, podrán, y deberán hacer un seguimiento activo de su seguridad y controlar las potenciales fuentes de riesgo a las que podrían ser sometidos [21][43][47][48][49].

### Herramientas de comunicación para médicos y pacientes

La optimización de la comunicación efectiva entre profesionales es una de las metas que la OMS propone para la prevención del error. Las tecnologías que garanticen la correcta comunicación no solo entre médicos y personal de salud, sino también con los propios pacientes, han tenido un efecto positivo en el control del riesgo y la prevención del daño. Son buenos ejemplos de esto los servicios de telemedicina con mensajería sincrónica o asincrónica, que incluso permiten acercar la atención al paciente, fuera inclusive del sistema sanitario [5][11][19].

### Instancias para la evaluación del error

Una de las principales estrategias para la mitigación del riesgo, es la evaluación del error. El Marco Conceptual de la Clasificación Internacional para la Seguridad del Paciente de la OMS recomienda cuales son los datos a tener en cuenta para el análisis y prevención de riesgos [7].

Marco conceptual para la evaluación del error

1. Tipo de incidente: Un tipo de incidente es una categoría formada por incidentes de naturaleza común que se agrupan por compartir características acordadas, y constituye una categoría «parental» bajo la cual pueden agruparse muchos conceptos. Los tipos de incidentes comprendidos son los: administración clínica, proceso clínico/procedimiento, documentación, infección asociada a la atención sanitaria, medicación/líquidos para administración i.v., sangre/productos sanguíneos, nutrición, oxígeno/gases/vapores, dispositivos/equipos médicos, comportamiento, accidentes del paciente, infraestructuras/locales/instalaciones, y recursos/gestión de la organización.

2. Resultados para el paciente: La clase resultados para el paciente contiene los conceptos relacionados con las repercusiones para el paciente total o parcialmente atribuibles a un incidente. Los resultados para el paciente pueden clasificarse según el tipo de daño, el grado de daño, y el impacto social o económico.
3. Características del paciente: Las características del paciente son atributos seleccionados de un paciente, como sus datos demográficos o el motivo de consulta.
4. Características del incidente: clasifican la información sobre las circunstancias que rodearon el incidente, como en qué momento y lugar del paso del paciente por el sistema de salud tuvo lugar el incidente, quiénes se vieron implicados y quién lo notificó.
5. Factores o peligros contribuyentes: son las circunstancias, acciones o influencias que se cree que han desempeñado un papel en el origen o el desarrollo de un incidente o que elevan el riesgo de que se produzca. Son ejemplos de ello factores humanos tales como el comportamiento, el desempeño o la comunicación; factores del sistema como el entorno de trabajo, y factores externos que escapan al control de la organización, como el medio natural o las políticas legislativas. Es habitual que en un incidente relacionado con la seguridad del paciente intervenga más de un factor contribuyente o un peligro.
6. Resultados para la organización: se refieren a las repercusiones para la organización total o parcialmente atribuibles a un incidente. Abarcan las consecuencias directas para la organización, como el aumento de los recursos asignados a la asistencia del paciente, la atención de los medios de comunicación o las ramificaciones jurídicas. A diferencia de ellas, las consecuencias clínicas o terapéuticas se consideran resultados para el paciente
7. Detección: La detección se define como una acción o circunstancia que permite descubrir un incidente. Por ejemplo, un incidente puede detectarse por un cambio en la situación del paciente o mediante un monitor, una alarma, una auditoría, un examen o una evaluación de riesgos. Los mecanismos de detección pueden estar incorporados al sistema como barreras oficiales o establecerse de forma no estructurada.
8. Factores atenuantes: son acciones o circunstancias que previenen o moderan la progresión de un incidente hacia la producción de un daño al paciente. Se conciben para reducir todo lo posible dicho daño una vez que el error se ha producido y se han puesto

en marcha mecanismos de control del daño. Juntas, la detección y la atenuación pueden impedir que la progresión de un incidente alcance al paciente o lo dañe. Si el incidente causa daño, pueden adoptarse medidas de mejora.

9. Medidas de mejora: son las medidas que se adoptan o las circunstancias que se modifican para mejorar o compensar el daño tras un incidente. Se aplican al paciente (tratamiento clínico de una lesión, presentación de disculpas, etc.) y a la organización (reunión informativa con el personal, cambios de cultura, gestión de reclamaciones, etc.).
10. Medidas adoptadas para reducir el riesgo: se concentran en disposiciones para evitar que se repita el mismo incidente relacionado con la seguridad del paciente o uno similar y en mejoras de la resiliencia del sistema. Son aquellas medidas que reducen, gestionan o controlan el daño o la probabilidad de daño asociado a un incidente. Pueden ir dirigidas al paciente (dispensación de una atención adecuada, apoyo a la toma de decisiones, etc.), al personal (formación, disponibilidad de políticas y protocolos, etc.), a la organización (mejora del liderazgo o la orientación, evaluación proactiva del riesgo, etc.) y a los agentes y equipos terapéuticos (auditorías regulares, funciones forzosas, etc.). La detección, los factores atenuantes y las medidas de mejora influyen en las medidas adoptadas para reducir el riesgo y las orientan.

## Conclusión

La seguridad del paciente es un problema grave de salud pública en todo el mundo. Entender el impacto que el error médico tienen en los pacientes, los factores de riesgo y como mitigarlos resulta indispensable. En este capítulo hemos descripto en forma generalizada el rol que una cuidada implantación de los distintos componentes de las TIC en salud pueden tener para prevenir los errores y aumentar la seguridad de los pacientes y lo importante de pensar en estrategias integrales para abordar el error en medicina. Como el lector podrá ver a lo largo de este libro, las TIC tienen, y tendrán, un rol fundamental en la generación de soluciones para viejos y nuevos problemas que se relacionan con la seguridad. Creemos que conocerlas en detalles y saber cómo usarlas será de gran utilidad para los gestores de salud.

## Bibliografía

- [1] IOM, 1999. *To Err Is Human: Building a Safer Health System*.
- [2] Donaldson L. The challenge of quality and patient safety. *Journal of the Royal Society of Medicine*. 2008; 101(7):338-41. doi:10.1258/jrsm.2008.
- [3] Reason, 2004. Beyond the organisational accident: the need for “error wisdom” on the front-line. *Qual Saf Health Care*.
- [4] Reason, J., 2000. Human error: models and management. *BMJ* 320, 768–770. doi:10.1136/bmj.320.7237.768
- [5] Mitchell, P.H., 2008. Defining Patient Safety and Quality Care, in: Hughes, R.G. (Ed.), *Patient Safety and Quality: An Evidence-Based Handbook for Nurses*, Advances in Patient Safety. Agency for Healthcare Research and Quality (US), Rockville (MD).
- [6] Patient Safety | Joint Commission, 2015. Patient Safety | Joint Commission [WWW Document]. Disponible en: [http://www.jointcommission.org/topics/patient\\_safety.aspx](http://www.jointcommission.org/topics/patient_safety.aspx) (accessed 9.7.15).
- [7] WHO | Patient safety [WWW Document], 2015. WHO. Disponible en: <http://www.who.int/patientsafety/en/> (accessed 9.7.15).
- [8] Battles, J., Lilford, R., 2003. Organizing patient safety research to identify risks and hazards. *Qual. Saf. Health Care* 12, ii2–ii7. doi:10.1136/qhc.12.suppl\_2.ii2
- [9] Van der Schaaf, T.W., 1995. Near miss reporting in the chemical process industry: An overview. *Microelectron. Reliab., Reliability: A Competitive Edge* 35, 1233–1243. doi:10.1016/0026-2714(95)99374-R
- [10] Palmieri, Patricia R. DeLucia, Lori T. Peterson, Tammy E. Ott, Alexia Green, 2008. The anatomy and physiology of error in adverse health care events, in: *Patient Safety and Health Care Management*, Advances in Health Care Management. Emerald Group Publishing Limited, pp. 33–68.
- [11] WHO | World Alliance for Patient Safety [WWW Document], 2004. WHO. Disponible en: <http://www.who.int/patientsafety/worldalliance/en/> (accessed 9.7.15).
- [12] Agrawal, A., 2009. Medication errors: prevention using information technology systems. *Br. J. Clin. Pharmacol.* 67, 681–686. doi:10.1111/j.1365-2125.2009.03427.x
- [13] Sexton, J.B., Thomas, E.J., Helmreich, R.L., 2000. Error, stress, and teamwork in medicine and aviation: cross sectional surveys. *BMJ* 320, 745–749. doi:10.1136/bmj.320.7237.745
- [14] Weingart, N.S., Wilson, R.M., Gibberd, R.W., Harrison, B., 2000. Epidemiology of medical error. *BMJ* 320, 774–777. doi:10.1136/bmj.320.7237.774
- [15] AHRQ’s Patient Safety Initiative: Building Foundations, Reducing Risk. December 2003. Agency for Healthcare Research and Quality, Rockville, MD. Disponible en: <http://archive.ahrq.gov/research/findings/final-reports/pscongrpt/psini2.html>
- [16] Goldzweig, C.L., Towfigh, A., Maglione, M., Shekelle, P.G., 2009. Costs and benefits of health information technology: new trends from the literature. *Health Aff. Proj. Hope* 28, w282–293. doi:10.1377/hlthaff.28.2.w282
- [17] HealthIT.gov, 2014. Health IT and Patient Safety Goals | Policy Researchers & Implementers | HealthIT.gov [WWW Document]. Disponible en: <http://www.healthit.gov/policy-researchers-implementers/health-it-and-safety> (accessed 9.7.15).
- [18] Huckvale, C., Car, J., Akiyama, M., Jaafar, S., Khoja, T., Khalid, A.B., Sheikh, A., Majeed, A., 2010. Information technology for patient safety. *Qual. Saf. Health Care* 19, i25–i33. doi:10.1136/qshc.2009.038497
- [19] Shekelle, P.G., Morton, S.C., Keeler, E.B., 2006. Costs and benefits of health information technology. *Evid. ReportTechnology Assess.* 1–71.
- [20] Bates, D.W., Leape, L.L., Cullen, D.J., Laird, N., Petersen, L.A., Teich, J.M., Burdick, E., Hickey, M., Kleffield, S., Shea, B., Vander Vliet, M., Seger, D.L., 1998. Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. *JAMA* 280, 1311–1316.
- [21] Carter, J.H., 2004. How EMR software can help prevent medical mistakes [WWW Document]. Disponible en: <http://www.acpinternist.org/archives/2004/09/emr.htm> (accessed 9.8.15).

- [22] Hernandez, F., Majoul, E., Montes-Palacios, C., Antignac, M., Cherrier, B., Doursounian, L., Feron, J.-M., Robert, C., Hejblum, G., Fernandez, C., Hindlet, P., 2015. An Observational Study of the Impact of a Computerized Physician Order Entry System on the Rate of Medication Errors in an Orthopaedic Surgery Unit. *PLoS One* 10, e0134101. doi:10.1371/journal.pone.0134101
- [23] Hidle, U., 2007. Implementing technology to improve medication safety in healthcare facilities: a literature review. *J. N. Y. State Nurses Assoc.* 38, 4–9.
- [24] Kannry, J., McCullagh, L., Kushniruk, A., Mann, D., Edonyabo, D., McGinn, T., 2015. A Framework for Usable and Effective Clinical Decision Support: Experience from the iCPR Randomized Clinical Trial. *EGEMS Wash. DC* 3, 1150. doi:10.13063/2327-9214.1150
- [25] Kawamoto, K., Houlihan, C.A., Balas, E.A., Lobach, D.F., 2005. Improving clinical practice using clinical decision support systems: a systematic review of trials to identify features critical to success. *BMJ* 330, 765. doi:10.1136/bmj.38398.500764.8F
- [26] Forni, A., Chu, H.T., Fanikos, J., 2010. Technology utilization to prevent medication errors. *Curr. Drug Saf.* 5, 13–18.
- [27] Henneman, E.A., 2007. Unreported Errors in the Intensive Care Unit A Case Study of the Way We Work. *Crit. Care Nurse* 27, 27–34.
- [28] Singh H, Giardina T, Meyer AD, Forjuoh SN, Reis MD, Thomas EJ, 2013. Types and origins of diagnostic errors in primary care settings. *JAMA Intern. Med.* 173, 418–425. doi:10.1001/jamainternmed.2013.2777
- [29] Thomsen, L.A., Winterstein, A.G., Sondergaard, B., Haugbølle, L.S., Melander, A., 2007. Systematic review of the incidence and characteristics of preventable adverse drug events in ambulatory care. *Ann. Pharmacother.* 41, 1411–1426. doi:10.1345/aph.1H658
- [30] Palmieri, P.A., Peterson, L.T., Corazzo, L.B., 2011. Technological iatrogenesis: the manifestation of inadequate organizational planning and the integration of health information technology. *Adv. Health Care Manag.* 10, 287–312.
- [31] Weiner, J.P., Kfuri, T., Chan, K., Fowles, J.B., 2007. “e-Iatrogenesis”: the most critical unintended consequence of CPOE and other HIT. *J. Am. Med. Inform. Assoc. JAMIA* 14, 387–388; discussion 389. doi:10.1197/jamia.M2338
- [32] McDonald, C.J., 2006. Computerization Can Create Safety Hazards: A Bar-Coding Near Miss. *Ann. Intern. Med.* 144, 510–516. doi:10.7326/0003-4819-144-7-200604040-00010
- [33] Palmieri, P.A., Peterson, L.T., Ford, E.W., 2007. Technological iatrogenesis: new risks force heightened management awareness. *J. Healthc. Risk Manag. J. Am. Soc. Healthc. Risk Manag.* 27, 19–24. doi:10.1002/jhrm.5600270405
- [34] Sittig, D.F., 2008. A socio-technical model of health information technology-related e-iatrogenesis. *AMIA Annu. Symp. Proc. AMIA Symp.* AMIA Symp. 1209–1210.
- [35] Koppel, R., Metlay, J.P., Cohen, A., Abaluck, B., Localio, A.R., Kimmel, S.E., Strom, B.L., 2005. Role of computerized physician order entry systems in facilitating medication errors. *JAMA* 293, 1197–1203. doi:10.1001/jama.293.10.1197
- [36] Ratwani RM, Benda NC, Hettinger A, Fairbanks RJ, 2015. Electronic health record vendor adherence to usability certification requirements and testing standards. *JAMA* 314, 1070–1071. doi:10.1001/jama.2015.8372
- [37] Ratwani, R.M., Fairbanks, R.J., Hettinger, A.Z., Benda, N.C., 2015. Electronic health record usability: analysis of the user-centered design processes of eleven electronic health record vendors. *J. Am. Med. Inform. Assoc. JAMIA*. doi:10.1093/jamia/ocv050
- [38] Lessing, C., Straß, C., Standke, H.-J., Lux, R., 2015. Can Quality of Patient Identification be Influenced by Training? - Results of a Randomised Multicentre Study with Multimodal Intervention. *Gesundheitswesen Bundesverb. Ärzte Öffentlichen Gesundheitsdienstes Ger.* doi:10.1055/s-0035-1548855
- [39] Liua, H.-C., Li, H., Chang, H.-F., Lu, M.-R., Chen, F.-C., 2015. Application of Barcoding to Reduce Error of Patient Identification and to Increase Patient’s Information Confidentiality of Test Tube Labelling in a Psychiatric Teaching Hospital. *Stud. Health Technol. Inform.* 216, 919.
- [40] Spain, D., Crilly, J., Pierce, J., Steele, M., Scuffham, P., Keijzers, G., 2015. Can a barcode scanner for blood collection improve patient identification integrity in the emergency

- department? A prospective before-and-after study. *Emerg. Med. Australas.* EMA 27, 47–54. doi:10.1111/1742-6723.12334
- [41] Tamuz, M., Harrison, M.I., 2006. Improving patient safety in hospitals: Contributions of high-reliability theory and normal accident theory. *Health Serv. Res.* 41, 1654–1676. doi:10.1111/j.1475-6773.2006.00570.x
- [42] Freeman, M., 2014. Matching the right patient to the right care. *Can. Nurse* 110, 14.
- [43] Hillestad, R., Bigelow, J., Bower, A., Girosi, F., Meili, R., Scoville, R., Taylor, R., 2005. Can electronic medical record systems transform health care? Potential health benefits, savings, and costs. *Health Aff. Proj. Hope* 24, 1103–1117. doi:10.1377/hlthaff.24.5.1103
- [44] Aspden, 2007. Preventing Medication Errors: Quality Chasm Series.
- [45] Gillaizeau, F., Chan, E., Trinquart, L., Colombet, I., Walton, R.T., Rège-Walther, M., Burnand, B., Durieux, P., 2013. Computerized advice on drug dosage to improve prescribing practice. *Cochrane Database Syst. Rev.* 11, CD002894. doi:10.1002/14651858.CD002894.pub3
- [46] Walker J, Leveille SG, Ngo L, Vodicka E, Darer JD, Dhanireddy S, Elmore JG, Feldman HJ, Lichtenfeld MJ, Oster N, Ralston JD, Ross S, Delbanco T. Inviting patients to read their doctors' notes: patients and doctors look ahead: patient and physician surveys. *Ann Intern Med.* 2011; 155:811–819
- [47] Cahill, J.E., Gilbert, M.R., Armstrong, T.S., 2014. Personal health records as portal to the electronic medical record. *J. Neurooncol.* 117, 1–6. doi:10.1007/s11060-013-1333-x
- [48] George, T.P., 2014. Plugging into personal health records for patient safety. *Nursing (Lond.)* 44, 68–69. doi:10.1097/01.NURSE.0000453709.27952.e6
- [49] Morris, C.J., Savellyich, B.S.P., Avery, A.J., Cantrill, J.A., Sheikh, A., 2005. Patient safety features of clinical computer systems: questionnaire survey of GP views. *Qual. Saf. Health Care* 14, 164–168. doi:10.1136/qshc.2004.011866



### Capítulo III

## La utilización de las TIC como un factor de riesgo para la seguridad de los pacientes

*David Rojas de la Escalera*  
*Javier Carnicero Giménez de Azcárate*



### Resumen

La incorporación de las Tecnologías de la Información y la Comunicación (TIC) a la atención sanitaria es un hecho consolidado desde hace mucho tiempo, y se ha llevado a cabo con el objetivo de mejorar la eficacia, eficiencia y efectividad del sistema de salud. Sin embargo, y a pesar de su potencial, las TIC pueden suponer también riesgos para la seguridad del paciente. La gestión de estos riesgos debe comenzar con su análisis pormenorizado, para definir sus principales parámetros, evaluar sus posibles consecuencias y, finalmente, decidir la estrategia más adecuada para afrontarlos.

El estudio del sistema de información de salud muestra los principales puntos de vulnerabilidad para la seguridad del paciente. Teniendo en cuenta que el objetivo de registrar la información clínica es garantizar que el proceso asistencial quede debidamente caracterizado y se pueda conocer con exactitud en posteriores consultas, un primer riesgo claro es la posibilidad de que se comentan errores en la identificación de las

personas, elementos y acciones clave que intervengan en el proceso. Este riesgo se reduce con la creación, adopción, buen uso y evolución de estándares para la codificación de toda esta información, teniendo en cuenta todas las fases y posibles variaciones del proceso asistencial.

A este riesgo fundamental hay que añadir los correspondientes a cada etapa del ciclo de vida de un sistema TIC: diseño, desarrollo, implantación, utilización, mantenimiento y evolución. En este sentido, se trata de riesgos relacionados con el uso de las TIC e independientes en su mayor parte del ámbito profesional de la salud: requisitos funcionales mal definidos, diseños incorrectamente aplicados, infraestructuras erróneamente dimensionadas, formación insuficiente de los usuarios, carencias en los servicios de soporte y mantenimiento, etc.

Para reducir estos riesgos es necesario incorporar la seguridad del paciente a los objetivos de todo proyecto de desarrollo de un sistema TIC sanitario, y tenerla en cuenta en todos los procedimientos de trabajo y de gestión del proyecto. Existen algunas recomendaciones y buenas prácticas que pueden ser de ayuda para este tipo de actuaciones, como por ejemplo las guías SAFER.

## Introducción

Desde hace varios años, la utilización de las Tecnologías de la Información y la Comunicación (TIC) es una constante en la mayoría de los sectores profesionales, así como en el ámbito doméstico. En el sector sanitario existe un consenso más o menos general acerca de su potencial para mejorar la eficiencia y la calidad de los procesos corporativos, tanto clínicos como administrativos o de gestión, y en consecuencia para garantizar una asistencia de mayor calidad. Incluso en la coyuntura de los últimos años, caracterizada por la grave crisis económica y los sucesivos recortes presupuestarios, se ha considerado a las TIC como un instrumento fundamental para la transformación del actual modelo de provisión asistencial y la garantía de la sostenibilidad de los sistemas públicos de salud.

Sin embargo, al igual que toda herramienta de trabajo, las TIC tienen puntos débiles que pueden suponer un riesgo para la seguridad de los pacientes. Si bien algunos de estos riesgos son inevitables, es necesario conocerlos, evaluarlos y adoptar las medidas necesarias para minimizar

su impacto en la actividad asistencial y el perjuicio que pueden ocasionar al paciente. Las TIC deben tratarse de la misma forma que cualquier tecnología de salud, evaluándose su eficacia (¿cumple el objetivo previsto?); su seguridad (¿tiene efectos adversos o secundarios que impidan o desaconsejen su utilización?); su efectividad (¿cumple sus objetivos en condiciones reales?); y su coste, de forma que se pueda calcular su relación coste-efectividad. En resumen, se trata de que el balance entre beneficios y riesgos sea positivo, y de que los resultados compensen el esfuerzo económico.

Considerando que las TIC son también un instrumento clínico, la forma de proceder debe combinar la identificación previa de vulnerabilidades y el análisis retrospectivo de las incidencias y problemas acaecidos, que deben dar lugar a las correspondientes medidas preventivas y correctoras, respectivamente. Si además se tiene en cuenta que la utilización de las TIC en el proceso asistencial es cada vez mayor, también lo es en consecuencia su impacto potencial en la seguridad de los pacientes, por lo que es imprescindible llevar a cabo una gestión continua de riesgos y problemas. En otras palabras, la seguridad del paciente debe figurar entre los objetivos de los proyectos de desarrollo, implantación, mantenimiento y evolución de sistemas TIC sanitarios.

No se dispone de muchos estudios en la literatura científica especializada expresamente dedicados al análisis de los riesgos inherentes al uso de las TIC en el proceso asistencial. De hecho, la mayoría de los trabajos publicados al principio del presente siglo abogaban por este uso como una de las principales herramientas de apoyo en la gestión de la seguridad del paciente [1][2]. Hacia finales de la década pasada y principios de la actual, algunos estudios optaban por rebajar este entusiasmo inicial, poniendo en duda que la relación directa entre la implantación de sistemas TIC y la mejora de la seguridad del paciente fuese tan clara como se pensaba en un principio [3], o al menos afirmando que la segunda no podía ni debía considerarse como una consecuencia automática e inmediata de la primera [4].

En los últimos años se aprecia claramente una tendencia integradora, defendiendo el valor añadido del uso de las TIC en la asistencia sanitaria, pero debidamente alineado con los objetivos en materia de seguridad de los pacientes [5] [6]. Como resultado de ello algunas instituciones han definido planes estratégicos específicos para el desarrollo de sistemas TIC sanitarios seguros [7], y han creado guías de buenas prácticas en

esa misma línea [8] [9]. También se ha empezado a otorgar a las TIC el tratamiento de tecnología sanitaria, mostrándose los mismos niveles de preocupación en materia de seguridad del paciente que se han mostrado siempre con respecto a la tecnología sanitaria tradicional. Por ejemplo, el ECRI Institute incluyó dos riesgos relacionados con las TIC en cada una de las tres últimas ediciones (2013, 2014 y 2015) de su lista anual de diez principales riesgos derivados del uso de tecnología sanitaria<sup>7</sup> [10] [11] [12]. Por último, cabe destacar el desarrollo de proyectos con el objetivo de evaluar el nivel de seguridad de sistemas TIC sanitarios [13] [14].

### Algunos fundamentos básicos del análisis de riesgos

En el ámbito sanitario son perfectamente aplicables los métodos generales de análisis de riesgos. Estos métodos establecen la importancia de un riesgo basándose en dos de sus características principales [15]:

- El impacto, que mide la gravedad de las consecuencias en caso de que el riesgo desemboque en una incidencia o problema.
- La probabilidad de que se produzca una incidencia o problema como consecuencia de la existencia del riesgo en cuestión.

Una vez medidos o estimados estos dos parámetros se calcula su producto, que sirve como indicador de la vulnerabilidad derivada de la existencia del riesgo. De este modo, un riesgo que tenga un impacto potencial considerable pero una probabilidad de ocurrencia baja no será tan crítico como podría parecer a priori, y un riesgo con un impacto reducido podrá ser más preocupante que el anterior si su probabilidad es elevada.

Habitualmente se manejan solamente estos tres conceptos (impacto, probabilidad y el producto de ambos), pero un análisis de riesgos puede enriquecerse añadiendo el cálculo o medición de otros parámetros, como por ejemplo los siguientes:

- La dispersión, que mide la extensión del área de la organización afectada por los posibles problemas derivados del riesgo. En el caso asistencial, este factor podría tener en cuenta variables como el número de pacientes afectados o la cantidad de centros de la organización expuestos. Estrictamente hablando esta información ya habrá sido tenida en cuenta en el cálculo del impacto, pero puede ser interesante conocer el componente de dispersión en concreto.

<sup>7</sup> Los riesgos destacados fueron los siguientes: errores en la integridad de datos en HCE y otros sistemas de información (2013, 2014 y 2015), fallos de interoperabilidad en sistemas de información y dispositivos médicos (2013), negligencias en la gestión del cambio (2014), y protección insuficiente de sistemas y dispositivos frente a ciberataques (2015).

- La facilidad de detección. Cuanto más difícil de detectar sea un problema, mayor puede ser el daño ocasionado, e incluso puede haber dado lugar a nuevos problemas antes de ser detectado y corregido. Esta característica también se relaciona con el impacto, pero es un dato muy necesario a la hora de diseñar las medidas preventivas o correctoras pertinentes.
- La trascendencia, que mide el grado de difusión del conocimiento del problema en caso de que éste se produzca. Aquí se pueden tener en cuenta factores como el daño para la imagen de la institución, las posibles sanciones, o la pérdida de certificados de acreditación. Al igual que las dos anteriores, esta característica debe tenerse en cuenta a la hora de calcular el impacto potencial de un riesgo.

Como resultado de la evaluación de todos los parámetros anteriores, debe decidirse la estrategia de gestión de riesgos que se debe aplicar. Estas estrategias pueden ser de cuatro tipos [15]:

- Eliminación, mediante la adopción de las medidas necesarias para anular el riesgo. Por ejemplo, un riesgo de incendio se elimina mediante el uso de materiales ignífugos. En el ámbito clínico, el riesgo de extravío de una placa radiológica se elimina implantando un sistema PACS para el almacenamiento de imagen médica en formato digital.
- Mitigación, consistente en la minimización del riesgo, sin que éste quede completamente anulado. Siguiendo con el ejemplo del riesgo de incendio, una estrategia de mitigación es la instalación de extintores. En el ámbito clínico, un riesgo de pérdida de los estudios de imagen radiológica almacenados en el PACS se mitiga realizando regularmente copias de seguridad.
- Transferencia, mediante la cual se traspa a otro agente o entidad la responsabilidad del riesgo. Un ejemplo de transferencia de riesgo es la contratación de un seguro contra daños por incendio. En el ámbito clínico, se puede externalizar la gestión de un sistema PACS, o incluso se pueden contratar servicios de telerradiología a un externo.
- Aceptación, que supone no tomar ninguna medida al respecto y asumir las consecuencias del riesgo en caso de que se produzca algún problema. Si se estima que la probabilidad y el impacto de un incendio son muy bajos, y que por lo tanto no compensa incurrir en los gastos derivados de cualquiera de las otras tres estrategias, entonces se está optando por asumir el riesgo sin más.

Dependiendo de la situación pueden ser viables varias de las estrategias, en cuyo caso habrá de optarse por la que se considere más apropiada. En el peor de los casos sólo podrá recurrirse a la estrategia de aceptación, puesto que ésta siempre será viable.

## El modelo del sistema de información de salud

Toda acción dentro del sistema de atención sanitaria está encaminada, ya sea de forma directa o indirecta, a la provisión de la asistencia sanitaria, por esta razón en el sistema de información de salud los datos clínicos constituyen la base para todos los procesos corporativos. Este trabajo se centra en la seguridad del paciente, por lo que en él sólo se tratará la gestión de la información clínica dentro del proceso asistencial. Asimismo, debido a la dimensión de este proceso y a la gran diversidad de situaciones que pueden darse dentro de él, sólo se plantearán y examinarán algunos ejemplos de los casos más frecuentes e ilustrativos.

Los registros de información clínica deben contener los datos esenciales para describir de forma clara el estado de salud de un paciente y la asistencia que ha recibido. De este modo, posteriores consultas de esta información permitirán que cualquier profesional sanitario conozca con precisión las características del paciente y tome las decisiones clínicas pertinentes, además de registrar la nueva información que se genera como consecuencia de la nueva actividad asistencial, de forma que esté disponible en el futuro.

Además, la estandarización de la información clínica en el nivel corporativo del sistema de salud es imprescindible para que estos datos puedan ser reutilizados, tanto por parte de otros profesionales clínicos que participen en la asistencia al paciente, como por parte de los profesionales administrativos y gestores encargados del funcionamiento de la organización, siempre que se cumplan los requisitos previstos en las normas de protección de datos de salud. La necesidad de estandarización es aún más crítica si se tiene en cuenta que los sistemas de salud disponen de miles de profesionales que atienden a millones de pacientes, y que además cada uno de estos últimos tiene sus características propias.

La Tabla III.1 muestra varios ejemplos de datos básicos que deben registrarse o consultarse de manera individual durante la asistencia del paciente, y de los ficheros maestros en los que deben integrarse estos datos para garantizar la correcta identificación de las personas participantes, de los elementos empleados y de las acciones realizadas.

<b>Tabla III.1. Ejemplos de datos básicos que se emplean en la asistencia individual y ficheros maestros relacionados.</b>	
<b>Nivel individual</b> <b>Historia clínica del paciente</b>	<b>Nivel corporativo</b> <b>Ficheros maestros del SI de salud</b>
Paciente	Base de datos maestra de pacientes
Profesionales que lo han atendido	Base de datos maestra de profesionales
Servicios y centros que lo han atendido	Catálogo de centros, servicios, locales e instalaciones
Recursos materiales empleados	Catálogo de recursos
Diagnósticos	Codificación de diagnósticos
Prescripciones	Base de datos de medicamentos y productos sanitarios
Pruebas complementarias	Catálogo de prestaciones y codificación de procedimientos*
Consultas	
Procedimientos	
Muestras	Registro de muestras
Imágenes médicas	Registro de imágenes
Historia clínica en papel	Archivo de historias clínicas
* El catálogo de prestaciones se compone de todos los actos asistenciales individuales que conforman la oferta de servicios de una institución o centro: consultas, pruebas, procedimientos, técnicas, determinaciones, etc. En algunos países se utiliza el término tarifario.	

La importancia de todos estos datos se puede apreciar más claramente examinando algunas de las situaciones asistenciales más comunes. La Tabla III.2 recoge varios ejemplos de este tipo.

<b>Tabla III.2. Datos de identificación de personas, elementos y acciones imprescindibles en algunos procesos clínicos.</b>				
<b>Proceso</b>	<b>Etapa</b>			
<b>Consulta</b>	<b>Cita</b>		<b>Admisión</b>	<b>Atención</b>
	Paciente		Paciente	Paciente
	Profesional		Agenda	Historia clínica en papel (si existe)
	Tipo de prestación o servicio			Diagnóstico
	Agenda			Tratamiento
	Lugar donde tendrá lugar la atención (consulta, quirófono...)			Pruebas complementarias*
Historia clínica en papel**				
<b>Tratamiento farmacológico</b>	<b>Prescripción</b>		<b>Dispensación</b>	<b>Administración</b>
	Receta	Paciente	Paciente	Paciente
		Código de identificación de la prescripción***	Prescripción	
		Profesional	Profesional	Medicamento
		Medicamento	Medicamento	Dosis
		Diagnóstico		Vía
		Dosis	Presentación del medicamento	Hora
		Pauta		Profesional
		Vía		
Fechas inicio-fin				
	<b>Cita</b>	<b>Admisión</b>	<b>Realización de la Prueba</b>	
<b>Pruebas complementarias</b>	Petición	Paciente	Paciente	Paciente
		Profesional	Agenda	Profesional
		Procedimiento	Comprobación de preparación del paciente	Lugar o instalación
		Justificación clínica	Consentimiento informado	Procedimiento
	Agenda		Lugar o instalación	Comprobación de preparación del paciente
	Lugar o instalación donde tendrá lugar la prueba			
	Instrucciones al paciente			Toma de muestra/imagen
<b>Intervención quirúrgica</b>	<b>Programación</b>	<b>Ingreso</b>	<b>Alta</b>	
	Paciente	Paciente	Paciente	
	Profesional	Profesional	Profesional	
	Procedimiento	Monitorización	Monitorización	
	Quirófono	Procedimiento	Tratamiento	
	Habitación (si cirugía con ingreso)	Pruebas complementarias	Pruebas complementarias	
	Proceso preoperatorio			
* En algunos países se emplea la denominación exámenes auxiliares.				
** En caso de existir una historia clínica en papel, debe solicitarse al archivo para que esté disponible durante la realización de la consulta.				
*** En España, la legislación vigente establece que toda prescripción (impresa o electrónica) debe contar con un código de identificación (Real Decreto 1718/2010, de 17 de diciembre, sobre receta médica y órdenes de dispensación.)				

En el caso de una consulta médica, en el momento de la cita deben identificarse el paciente que pide la consulta, el médico que debe llevarla a cabo, el tipo de consulta que se está solicitando y la agenda en la que deben consignarse la cita, el lugar y otras necesidades que se puedan dar. Además, en caso de existir todavía una historia clínica en papel debe emitirse una solicitud al archivo para que esta información esté disponible en la consulta el día de la cita. Cuando llega este día, el paciente debe realizar un trámite de admisión en el que se compruebe su identidad y la existencia de la cita en la agenda correspondiente. Por último, durante la consulta se comprueba una vez más la identidad del paciente, así como la disponibilidad de su historia clínica (en papel o electrónica), y se procede al registro de la nueva información generada como consecuencia del episodio asistencial.

Si se prescribe un tratamiento farmacológico, el médico debe cumplimentar una receta en la que se identifican tanto él como el paciente, además del acto de prescripción propiamente dicho<sup>8</sup>, y se detalla la medicación prescrita: medicamento, dosis, pauta de administración, y fechas de inicio y fin del tratamiento<sup>9</sup>. En el momento de la dispensación, el profesional farmacéutico debe identificarse también, además de comprobar los datos de la receta y verificar que se trata del paciente correcto y que se dispensa el medicamento prescrito. Finalmente, en el caso de una prescripción hospitalaria deben comprobarse y registrarse los llamados “cinco correctos” (paciente, medicamento, dosis, vía y hora) [16], así como el profesional que administra la medicación al paciente.

Si un médico solicita una prueba complementaria, como por ejemplo una prueba radiológica o un análisis de sangre, debe cumplimentar una petición en la que una vez más se identifican tanto él como el paciente, se especifica el examen solicitado y se razona la petición desde el punto de vista clínico. Después debe tramitarse la cita correspondiente, además de facilitar al paciente las instrucciones de preparación que debe seguir (por ejemplo, acudir en ayunas o interrumpir la administración de medicamentos con una antelación determinada), si fuera necesario. El día del examen deben verificarse la identidad del paciente, la existencia de la cita, el cumplimiento de las

---

<sup>8</sup> Como se ha explicado al pie de la Tabla 3.II, en España cada acto de prescripción debe quedar debidamente identificado mediante un código, independientemente de que la prescripción se realice en formato electrónico o sobre papel.

<sup>9</sup> En algunos países la normativa legal vigente obliga a incluir también el diagnóstico al que corresponde la prescripción.

instrucciones de preparación y, si procede, la explicación, entendimiento y firma del consentimiento informado correspondiente. Para terminar, ha de registrarse toda la información que genera la realización de la prueba.

Cuando el paciente debe someterse a un procedimiento quirúrgico, deben coordinarse varias tareas que garanticen la disponibilidad de los profesionales y recursos necesarios (cirujano, enfermería, quirófano, habitación, instrumental, entre otros), además de ponerse en marcha un proceso preoperatorio durante el que, entre otras actividades, se hace un balance beneficio/riesgo del procedimiento. Si la intervención llega a realizarse, debe ir seguida de un exhaustivo seguimiento del paciente, tanto durante su estancia hospitalaria como después de recibir el alta<sup>10</sup>.

Las consecuencias de un error en el registro de estos datos pueden ser muy graves. Por ejemplo, un error en la identificación del paciente puede provocar que un proceso asistencial quede perfectamente registrado en lo referente a las acciones tomadas, pero sea asignado a un paciente distinto de aquel al que corresponde, causando un perjuicio a dos pacientes diferentes. De esta manera, puede ocurrir que se practique el procedimiento adecuado y se registre de forma apropiada, pero todo ello, procedimiento y registro, se relacione con un paciente incorrecto. Puede suceder también que la medicación prescrita o administrada al paciente no quede debidamente registrada, de modo que reciba una dosis errónea (ya sea excesiva o insuficiente) o bien fármacos que combinados puedan producir efectos adversos. Del mismo modo, si las peticiones no son correctamente registradas, el paciente puede ser sometido a pruebas redundantes o incompatibles. Puede darse también el caso de que las muestras recogidas sean enviadas a un departamento erróneo, donde se procesen de forma que queden inutilizadas para el propósito con el que se solicitaron los análisis. Esto obligaría a someter al paciente a una nueva toma de muestra, con el riesgo, o al menos las molestias y costes, que ello conlleva.

Estos ejemplos ilustran la necesidad de registrar correctamente no sólo cada uno de estos elementos de forma individual, sino también la vinculación existente entre cada uno ellos en cada acto asistencial: paciente, profesional, petición, prestación, muestra, departamento,

---

<sup>10</sup> Para un análisis específico de la seguridad del paciente en el bloque quirúrgico, véase el Capítulo V.

medicamento, etc. En otras palabras, el profesional no trabaja con datos aislados sino con conjuntos de datos, por lo que el registro de los mismos debe ser completo, estructurado y correcto para poder establecer y consultar la relación entre ellos y, en consecuencia, garantizar la seguridad del paciente durante la utilización de esta información a lo largo del proceso asistencial.

### Principales riesgos de los sistemas TIC sanitarios

De todo lo expuesto en el apartado anterior, se deduce que un primer riesgo claro de la utilización de las TIC en la actividad clínica corresponde a la necesidad de identificar correctamente las personas, elementos y acciones que definen un episodio asistencial y también de vincularlos correctamente entre sí, con el fin de poder registrar de forma correcta y completa la información de salud de los pacientes. Asimismo, estos datos deben ser recuperados y adecuadamente presentados al profesional que efectúe consultas posteriores, conservando siempre el valor del dato que se está manejando. Estos requisitos deben abordarse desde la fase de diseño del sistema TIC.

En la Tabla III.3 se recogen algunos de los principales riesgos inherentes a las distintas fases de la creación de un sistema TIC. Estas fases se describen a continuación a lo largo del presente apartado.

<b>Tabla III.3. Riesgos durante la creación de un sistema TIC.</b>		
<b>Diseño</b>	Dato no registrado	Dato recibido de una fuente errónea
	Dato registrado incorrectamente	Dato recibido con errores desde la fuente
		Dato registrado con un valor erróneo
		Dato registrado en una ubicación errónea
	Dato recuperado incorrectamente	Dato recuperado con una estructura errónea
		Dato recuperado de una ubicación errónea
<b>Desarrollo</b>	Funcionalidades omitidas o incorrectamente incorporadas	
	Incapacidad para soportar la carga de trabajo necesaria	
	Incapacidad para interoperar con otros sistemas	
	Limitaciones para modificar funcionalidades existentes e incorporar otras nuevas	
	Limitaciones en la capacidad de crecimiento para adaptarse a un aumento de la carga de trabajo	
	Carencias en el plan de pruebas que impidan la detección de errores existentes	
<b>Implantación</b>	Limitaciones o sesgos en el alcance del piloto	
	Convivencia prolongada del nuevo sistema con el sistema al que debe sustituir	
	Dimensionamiento incorrecto de la infraestructura TIC de base	
<b>Utilización</b>	Formación insuficiente de los usuarios del sistema	
	Relajación excesiva de los usuarios	
	Introducción manual de datos	
	Registro de datos de forma diferida	
<b>Mantenimiento y evolución</b>	Carencias en el proceso de gestión de incidencias y fallos	
	Procedimientos de respaldo inadecuados	
	Carencias en la incorporación de modificaciones en el sistema	

### Fase de diseño del sistema

El objetivo de la construcción de todo sistema TIC es incorporar una nueva herramienta de trabajo a un proceso de gestión, con el fin de ejecutarlo de forma más eficiente, efectiva o ambas. Esto se consigue automatizando parcial o totalmente algunas de las etapas del proceso, y añadiendo algunas nuevas funcionalidades que no tienen lugar en un proceso ejecutado manualmente pero son perfectamente viables mediante el uso de las TIC, como por ejemplo verificaciones automáticas de los datos (cumplimentación de campos obligatorios, uso de un rango discreto de datos, búsquedas asistidas o alertas, entre otros).

Esto significa que cada vez que se implanta un nuevo sistema TIC es necesario analizar exhaustivamente cada uno de los procesos de la organización en los que va a intervenir, así como la forma en la que estos procesos se van a llevar a cabo en el sistema, puesto que la aparición de nuevas funcionalidades puede suponer la introducción de modificaciones y también permitir la incorporación de mejoras que corrijan ineficiencias o incluso defectos en el proceso original. Si se omiten este análisis y la posterior reingeniería de procesos, el diseño del sistema puede contener errores, tanto de nueva aparición como heredados de los procesos organizativos implicados. Ejemplos de este tipo de situación pueden ser la omisión del registro de ciertos datos, o una codificación incorrecta de los mismos. Como se ha explicado con anterioridad, la identificación única de personas, elementos y acciones, así como el registro de la relación existente entre todos ellos en cada acto clínico, son de una importancia crucial.

Un aspecto muy importante del registro de los datos es la arquitectura o construcción de la información [17], un concepto que agrupa la definición de las estructuras de registro de los datos, la identificación de las fuentes de información de las que pueden proceder dichos datos, y el diseño de los flujos de información que pueden tener lugar durante el registro y posterior tratamiento de los datos almacenados. En otras palabras, debe definirse no sólo qué información debe ser registrada, sino cómo debe ser registrada y, posteriormente, procesada.

El ejemplo más claro de la importancia de la arquitectura de la información es nuevamente la identificación única de personas, elementos y acciones, puesto que resultado de ella son los distintos ficheros

maestros recogidos en la Tabla III.1. El proceso de gestión de estas bases de datos debe contemplar los siguientes aspectos:

- **Creación:** para crear un fichero maestro deben definirse claramente su estructura de datos y, en caso de que la información que deba albergar ya exista, también el proceso de carga inicial de los mismos. Lo más habitual es que un fichero maestro herede información que ya se está gestionando en una o varias bases de datos, lo que obliga a efectuar un proceso de migración, o incluso en soporte papel, lo que implica un registro manual de los datos si se desea que éstos estén disponibles en el nuevo sistema. Aquí se aprecian claramente varios riesgos. Por un lado, la estructura del fichero maestro debe ser compatible con la estructura que exige el registro de los datos. Por otro, el proceso de carga inicial debe realizarse de manera que se conserve la integridad de los datos migrados. El riesgo de esta última labor es mayor si se realiza de forma manual.
- **Mantenimiento:** independientemente de si el fichero maestro comienza su uso en blanco o con un conjunto inicial de datos, a partir de su entrada en producción adquiere una dinámica continua de actualización de la información registrada, con sucesivas altas, bajas o modificaciones de las distintas entradas. Asimismo, el fichero deberá adaptarse a nuevas necesidades de la organización que supongan cambios en la manera de registrar los datos, como por ejemplo un nivel de detalle más específico, una ampliación del rango de posibles valores o la incorporación de nuevos datos. En otras palabras, deben definirse y seguirse unos procedimientos para la adición, eliminación y edición de datos, y también para la evolución estructural del propio fichero, velando en ambos casos por la integridad de la información. Por ejemplo, en el caso de cambios en la estructura del fichero es posible que sean necesarias ciertas adaptaciones de los datos previamente existentes, de manera que sean compatibles con la nueva estructura. Un caso sencillo sería la incorporación del prefijo telefónico provincial español en el momento en que los números de teléfono de los pacientes pasaron de seis a nueve dígitos.
- **Acceso:** los datos de un fichero maestro deben poder ser consultados o utilizados desde el punto de la red asistencial en el que se encuentre el profesional que los solicite, y en el momento en el que sean requeridos. Este acceso debe llevarse a cabo garantizando en todo momento la integridad de esta información. Para ello deben definirse unos protocolos de consulta que garanticen la disponibilidad

de estos datos en tiempo y forma siempre que el acceso esté debidamente autorizado, y por el contrario protejan también la información contra cualquier acceso indebido, de acuerdo con una política de permisos previamente establecida [18]. Esta política es también un requisito para los protocolos de actualización de datos mencionados en el punto anterior. Su objetivo es proteger la información frente a posibles intrusiones en el sistema, como por ejemplo un ciberataque [19] o el uso de un terminal portátil robado o extraviado [20]<sup>11</sup>.

Un factor muy ligado al acceso a los datos es la presentación de la información. Además de ser completa y fidedigna, la información debe presentarse de forma amigable e intuitiva para el usuario, permitiéndole localizar rápidamente los datos exactos que quiere consultar, y facilitando el acceso a otros datos del paciente que también puedan resultar de interés. Una presentación que ofrezca demasiada información, que la presente de forma desordenada o que dificulte la navegación por los distintos contenidos incrementa la probabilidad de que el usuario no encuentre el dato que está buscando o, peor aún, de que tome un dato erróneo.

En conclusión, el diseño de un sistema TIC debe recoger con todo detalle el proceso de gestión de la información (captura, registro estructurado, procesamiento, consulta, modificación y presentación de los datos, entre otros) e incorporar todos los requisitos y particularidades que se identifiquen durante el análisis preliminar de los procesos previamente existentes. Un factor crítico de éxito para este diseño es una comunicación fluida y eficaz entre los usuarios clínicos y los profesionales TIC, dos colectivos entre los que ha existido tradicionalmente una brecha causante de varios conflictos, problemas y, en situaciones extremas, fracasos. Cada uno de ellos debe comprender que los proyectos de salud electrónica no son proyectos puramente tecnológicos, sino proyectos clínicos que requieren un conocimiento experto de las TIC, y asumir sus responsabilidades: el usuario clínico debe ser capaz de identificar y transmitir sus necesidades, y el profesional TIC debe ser capaz de comprenderlas y proponer soluciones. En caso contrario, el sistema resultante no responderá a las necesidades realmente existentes.

---

<sup>11</sup> Para un análisis específico de la seguridad de la información desde la perspectiva de la seguridad del paciente, véase el Capítulo VIII.

## Fase de desarrollo del sistema

Una vez diseñado el sistema debe acometerse la construcción física del mismo, que debe dar como resultado un instrumento de trabajo que cumpla rigurosamente los distintos requisitos definidos durante la fase de diseño. En otras palabras, esta fase consiste en añadir y combinar los componentes necesarios para llevar a la práctica un diseño teórico.

Para ello ha de comenzarse por la selección de estos componentes. La elección de la plataforma tecnológica es el primer factor de riesgo que aparece en esta fase. El mercado TIC se caracteriza por una gran oferta de soluciones, basadas en diferentes tecnologías, cuyas características, prestaciones y limitaciones no siempre están completa o correctamente especificadas. La base tecnológica del sistema TIC debe seleccionarse tras un estudio riguroso, teniendo en cuenta no sólo su capacidad para proporcionar la funcionalidad requerida, sino también aspectos de índole más técnica como su fiabilidad, su capacidad de crecimiento y evolución, sus posibilidades de interoperabilidad con otras plataformas, o su coste, entre otros. De lo contrario, puede darse el caso de que el sistema no sea capaz de asumir la carga de trabajo que suponga su puesta en producción, de admitir ampliaciones que le permitan adaptarse a nuevas necesidades de la organización, o de integrarse con otros sistemas para intercambiar datos.

La integración de sistemas es precisamente otro riesgo derivado del uso de las TIC. Además de que las distintas plataformas tecnológicas empleadas permitan la conexión física de los sistemas basados en ellas, deben definirse unos procedimientos que permitan su interoperabilidad, de forma que puedan compartir la información clínica del paciente. De lo contrario, cada dato tendrá que introducirse repetidas veces, una en cada sistema que lo necesite, con el riesgo que ello conlleva para la calidad de la información. En el caso extremo de que la cantidad de información que se maneje sea ingente, puede suceder que ni siquiera esta introducción manual sea una opción, y en consecuencia la información no estaría disponible fuera del sistema que la alberga. Una última posibilidad sería proporcionar al profesional un acceso a este sistema, pero debería seguirse el proceso de política de seguridad mencionado con anterioridad.

Uno de los últimos pasos de la fase de desarrollo es la realización de una batería de pruebas para comprobar el correcto funcionamiento del sistema antes de su puesta en marcha. Estas pruebas deben diseñarse de forma que cubran el espectro de casos de uso más amplio posible dentro de lo razonable, y ejecutarse una y otra vez hasta que los errores detectados sean corregidos y el funcionamiento del sistema sea satisfactorio. Por supuesto, es imposible simular al 100% un entorno real durante un plan de pruebas, pero de este modo se minimizarán los problemas post-arranque.

### Fase de implantación del sistema

La siguiente fase es la implantación del sistema, cuyo objetivo es incorporar la solución desarrollada al entorno real en el que debe desempeñar su función, por lo que se requiere una estrategia adecuada para su puesta en marcha. Aunque el sistema haya superado un buen plan de pruebas, debe tenerse en cuenta que algunos errores pueden no detectarse hasta su implantación en un entorno real. Por este motivo, dicha implantación debe llevarse a cabo de forma controlada, mediante la realización de una prueba piloto en un área lo suficientemente acotada como para ser manejable, pero también lo suficientemente extensa como para que sus resultados sean significativos [21]. En este sentido, la prueba piloto no deja de ser una extensión del plan de pruebas, con el valor añadido de tener lugar en un entorno real que permite realizar un refinamiento exhaustivo del sistema.

Una vez superada satisfactoriamente la etapa piloto, puede procederse con una expansión rápida del sistema. De hecho, la convivencia de sistemas nuevos con sistemas preexistentes es un factor de riesgo que debe tomarse en consideración. Teniendo en cuenta que la puesta en marcha de un nuevo sistema debe iniciarse con un piloto, esta convivencia es inevitable, pero su duración debe reducirse al mínimo plazo de tiempo posible. La existencia de más de un sistema supone un riesgo de información duplicada, disgregada o, peor aún, contradictoria, y este riesgo se presenta tanto en el caso de la convivencia entre sistemas TIC como en el de la convivencia entre un sistema TIC y un sistema basado en papel. Asimismo, esto también dificulta la adopción del nuevo sistema por parte de los usuarios más reticentes, que pueden aferrarse al sistema antiguo aunque sea por una mera cuestión de predilección.

Un último riesgo es la posibilidad de realizar un dimensionamiento erróneo de la infraestructura TIC de base. Todo sistema funciona soportado por una infraestructura hardware, software y de comunicaciones. Cuando esta infraestructura no cuenta con la capacidad suficiente, puede saturarse y provocar que el sistema no funcione correctamente. Es imprescindible calcular la carga de trabajo que supone el funcionamiento de los procesos de gestión soportados, así como tener en cuenta sus previsiones de crecimiento a medio y largo plazo. Estos cálculos teóricos deben refrendarse sometiendo al sistema a diversas pruebas de estrés que verifiquen su fiabilidad.

### Fase de utilización del sistema

Durante la utilización del sistema deben tenerse presentes los riesgos inherentes a su utilización. Uno de los requisitos para que un sistema TIC sea seguro es que los usuarios conozcan perfectamente cómo se utiliza. Para ello es necesario que se hayan realizado las actividades formativas necesarias y que se haya comprobado debidamente que los usuarios sean capaces de manejar el sistema. Estas actividades deben repetirse cada vez que se incorporen nuevos usuarios y también cada vez que se introduzcan cambios en el sistema, como por ejemplo nuevas funcionalidades.

Otro riesgo es una posible relajación de los usuarios como consecuencia de la automatización, ya sea parcial o total, de algunas de sus tareas, lo que puede provocar que no se revise con el debido rigor la información que se introduce en el sistema. Funcionalidades como el uso de plantillas o el habitual “copiar+pegar” son un ejemplo de este tipo de situaciones que pueden conducir a errores.

Mención especial merecen los riesgos relacionados con el registro de la información. El registro de nuevos datos es uno de los momentos de mayor vulnerabilidad para la calidad de la información. Los dos principales factores de riesgo en este proceso son la introducción manual de datos y su registro diferido. En otras palabras, lo ideal es que el registro de datos se automatice siempre que sea viable, y que se lleve a cabo de la forma más inmediata posible. Por ejemplo, si una enfermera monitoriza el pulso y la saturación de oxígeno del paciente a pie de cama, la forma de minimizar los riesgos es que proceda a registrar estos datos en la historia clínica en ese mismo momento, o mejor aún, que el pulsioxímetro empleado esté integrado con el sistema TIC y le transfiera automáticamente la información.

## Fase de mantenimiento y evolución del sistema

Paralelamente a la utilización del sistema debe llevarse a cabo un proceso de mantenimiento que asegure su correcto funcionamiento, y su recuperación en caso de problemas o averías. El volumen de usuarios en los centros asistenciales es en general tan cuantioso que es inevitable que se produzcan incidencias de forma relativamente frecuente. Estas incidencias deben ser debidamente notificadas, clasificadas, analizadas y resueltas. Los circuitos de comunicación deben estar claramente definidos, y los equipos encargados de atender las incidencias deben resolverlas en un plazo de tiempo acorde con su gravedad.

Una de las principales medidas de protección frente a fallos del sistema son los procedimientos de respaldo. Durante el funcionamiento del sistema, dos de los problemas más graves que pueden tener lugar son la pérdida de información y la imposibilidad de acceder a ella por un fallo en las infraestructuras de base. Para prevenir el primer caso es necesario contar con un protocolo de copia de seguridad de los datos registrados en el sistema, de manera que la información perdida pueda restaurarse, si no en su totalidad, sí en un porcentaje mayoritario que minimice la gravedad del problema. En el segundo caso, debe disponerse de una infraestructura secundaria de respaldo que sea capaz soportar el funcionamiento del sistema con unas prestaciones aceptables, mientras se solucionan los problemas que afectan a la infraestructura principal y se restablecen las condiciones normales de operación.

Otro aspecto a tener en cuenta es la evolución de un sistema, que implica un proceso similar al de su creación, aunque a menor escala. Las nuevas funcionalidades deben pasar por un ciclo de diseño, desarrollo, pruebas y utilización en el que vuelven a estar presentes todos los riesgos anteriormente expuestos.

## Recomendaciones y buenas prácticas

Como puede apreciarse, existen diversos riesgos inherentes al uso de las TIC en la gestión de la información clínica. Por extensión, las causas pueden ser también muy variadas. La primera de todas, y quizá la principal, suele ser la no inclusión de la seguridad del paciente entre los objetivos del sistema. Esto provoca que no se tengan en cuenta procedimientos de trabajo y funcionalidades que ayuden a garantizar

la seguridad del paciente. Después vienen posibles fallos en el diseño, desarrollo, implantación, utilización, mantenimiento o evolución del sistema, como se ha explicado en el apartado anterior.

Otras causas que cabe destacar derivan de las características habituales de las soluciones de mercado. Una circunstancia de los productos comerciales es que los proveedores deben proteger la ventaja competitiva que pueden suponer sus productos, motivo por el cual no suelen facilitar información muy detallada sobre los mismos. Además, estos productos presentan una elevada heterogeneidad tanto funcional como tecnológica, lo que puede dificultar la interoperabilidad con los demás sistemas de la organización. Esta heterogeneidad es extensiva a los propios entornos clínicos, ya sea entre diferentes instituciones o dentro de una misma, lo que dificulta aún más la interoperabilidad de sistemas e incluso la flexibilidad de la organización para sustituir un sistema por otro. Esto conduce a la creación de relaciones de dependencia con los proveedores finalmente seleccionados, y en consecuencia a una resistencia institucional al cambio de producto o proveedor.

Teniendo en cuenta todos los riesgos expuestos y sus posibles causas, pueden definirse las siguientes recomendaciones y buenas prácticas:

- Incluir la seguridad de pacientes como uno de los objetivos generales del sistema en todos los proyectos de TIC relacionados con la actividad clínica.
- Conocimiento exacto y detallado de las características propias de la organización: objetivos estratégicos, dimensión, complejidad y necesidades a corto, medio y largo plazo.
- Definición de objetivos y requisitos TIC específicos de seguridad del paciente, a partir de un análisis de riesgos de los procedimientos de trabajo, de las políticas corporativas de calidad y seguridad, y de la legislación vigente aplicable.
- Planificación exhaustiva de la arquitectura de la información: definición de las estructuras de datos, de las distintas fuentes de información y de los flujos de datos, identificando los posibles puntos de entrada en el sistema, consulta y actualización.
- Definición de una política corporativa de estandarización en varios niveles: organizativa, semántica, tecnológica y, en caso necesario, legal. La estandarización permite homogeneizar o al menos compatibilizar el significado, estructura y uso de los datos, haciendo

- viable su intercambio entre diferentes sistemas tanto dentro de una organización como entre organizaciones diferentes.
- Incorporación de funcionalidades que permitan al usuario configurar el sistema de forma personalizada, respetando siempre un umbral mínimo de homogeneidad de los procedimientos de trabajo. De esta forma se puede facilitar la adaptación individual de cada profesional a los nuevos sistemas.
  - Gestión profesional de la seguridad del paciente en sistemas TIC, evaluando periódicamente la eficacia de los mismos mediante:
    - Análisis de riesgos.
    - Establecimiento de puntos de control y límites críticos.
    - Definición de procedimientos de monitorización y verificación.
    - Detección, comunicación, análisis y registro de incidencias y problemas.
    - Definición, aplicación y registro de correcciones y mejoras.
    - Mantenimiento de documentación.
    - Cálculo de indicadores.
  - Planificación rigurosa de los servicios de soporte y mantenimiento del sistema y de la infraestructura TIC de base correspondiente. En este ámbito deben tenerse en cuenta actividades de carácter preventivo, correctivo y evolutivo, y definirse unos acuerdos de nivel de servicio que especifiquen los tiempos de respuesta y solución de cada tipo de incidencia o problema según su gravedad, de acuerdo con las necesidades de la organización.
  - Aplicación de una política de formación y concienciación de los usuarios del sistema, promoviendo la adherencia a los procedimientos de trabajo de la organización y el mantenimiento de una cultura corporativa de seguridad del paciente.

#### Un caso de uso: las Guías SAFER

Por supuesto, las recomendaciones expuestas son sólo algunas líneas generales de actuación que toda organización debe considerar y adaptar a su situación, prioridades y necesidades particulares, añadiendo o modificando lo que estime oportuno. Por ejemplo, el Gobierno de Estados Unidos ha promovido la creación de unas guías propias, denominadas SAFER Guides (Safety Assurance Factors for EHR Resilience, Factores de Aseguramiento de Seguridad para la Adaptación de la Historia Clínica Electrónica). A continuación se enumeran estas guías, con algunos ejemplos de las buenas prácticas recomendadas en ellas<sup>12</sup>:

<sup>12</sup> SAFER Guides: <http://www.healthit.gov/safer/safer-guides>

- Guías fundamentales:
  - \* Prácticas de alta prioridad:
    - Respaldo de datos y de parámetros de configuración de las aplicaciones, y redundancia de infraestructuras de hardware.
    - Registro de alergias, problemas y resultados mediante el uso de códigos estandarizados.
    - Diseño de la interfaz de manera que la información necesaria sea visible, legible e inteligible, y el sistema sea fácil de utilizar.
    - Trazabilidad del estado de las órdenes médicas.
    - Uso de la HCE para la prescripción de medicamentos y la solicitud de pruebas diagnósticas y procedimientos.
    - Monitorización de indicadores clave de seguridad.
  - \* Responsabilidades de la organización:
    - Compromiso de la alta dirección con la promoción de una cultura corporativa de seguridad.
    - Implicación de los usuarios en todos los niveles de la toma de decisiones relacionadas con la seguridad de la HCE.
    - Evaluación periódica de la formación a usuarios y de los servicios de soporte de sistemas.
    - Mantenimiento de un registro de fallos y riesgos relacionados con la HCE.
- Guías de proceso clínico:
  - \* Identificación de pacientes:
    - Utilización de un índice maestro de pacientes que contenga sus datos demográficos y su identificador o identificadores de historia clínica.
    - Inclusión de la información requerida para la correcta identificación del paciente en cada pantalla, documento impreso o pulsera identificativa.
    - Inclusión de dígitos de control en los números de historia clínica para prevenir errores en la introducción manual del dato.
    - Disponibilidad de un procedimiento de identificación temporal en caso de pacientes no identificados o fallo del sistema.
  - \* Órdenes médicas electrónicas (gestión de peticiones) con sistemas de apoyo a la toma de decisiones:
    - Registro de las órdenes de acuerdo con una codificación estándar, con posibilidad de búsqueda.
    - Participación de los usuarios en la puesta en funcionamiento, revisión y actualización de los sistemas de apoyo a la toma de decisiones.

- Minimización del uso de texto libre en la introducción de datos.
  - Envío electrónico de la información al responsable de la ejecución de cada orden.
  - Comprobación de alergias e interacciones medicamentosas del paciente.
  - Visualización de la información crítica del paciente durante todo el proceso.
- \* Informe de resultados de pruebas:
- Registro estructurado de los resultados de pruebas de laboratorio, según una nomenclatura estándar.
  - Asociación de códigos de interpretación de resultados en el caso de informes en los que predomine el texto libre, como radiología o anatomía patológica.
  - Visibilidad clara del cambio de estado de la prueba cuando los resultados están disponibles.
  - Notificación electrónica de cambios o enmiendas en los resultados de pruebas, complementada con una comunicación directa en el caso de cambios importantes.
  - Presentación amigable de la información, resaltando los valores de resultados fuera del rango de normalidad.
  - Limitación del uso de alertas a aquellas que sean clínicamente relevantes, para no “fatigar” al usuario.
- \* Comunicación entre clínicos:
- Visualización clara del remitente y de la fecha y hora de envío de cada mensaje.
  - Registro en la HCE de toda comunicación entre clínicos.
  - Envío rápido de la información clínica urgente, y registro de dicho envío en la HCE.
- Guías de infraestructura:
- \* Planes de contingencia:
- Redundancia del hardware que soporta aplicaciones críticas para la organización.
  - Disponibilidad de grupos electrógenos para uso en caso de corte del suministro eléctrico.
  - Respaldo de datos de los pacientes y de parámetros de configuración de las aplicaciones críticas.
  - Formación a usuarios en procedimientos de actuación durante fallos del sistema y de recuperación tras el restablecimiento del servicio.

- Existencia de una estrategia de comunicación no basada en TIC para su uso durante fallos del sistema.
- \* Configuración de sistemas:
  - Disponibilidad de suficientes puntos de acceso a la HCE en todas las áreas clínicas.
  - Existencia de mecanismos robustos para la autenticación de usuarios.
  - Realización previa de pruebas de funcionamiento del sistema antes de su implantación en un entorno real.
  - Control de niveles de acceso basado en la definición de permisos y roles de usuario.
- \* Interfaces de sistemas:
  - Uso de estándares para el intercambio de información entre la HCE y otros sistemas.
  - Prueba de las interfaces entre distintos sistemas para comprobar su correcta configuración y garantizar que la información es transmitida sin pérdidas, tanto en datos codificados como en campos de texto libre.
  - Existencia de un entorno de pruebas independiente del entorno de producción.
  - Monitorización periódica de la utilización y rendimiento del sistema, incluyendo el registro de errores de transmisión de datos y el volumen de transacciones entre sistemas.

## Bibliografía

- [1] Kohn L.T., Corrigan J.M. y Donaldson M.S., editores. *To Err Is Human: Building a Safer Health System*. Washington, D.C.: Committee on Quality of Health Care in America, Institute of Medicine; 2000.
- [2] Teigland C., Gardiner R., Li H. y Byrne C. Clinical Informatics and Its Usefulness for Assessing Risk and Preventing Falls and Pressure Ulcers in Nursing Home Environments. *Advances in Patient Safety* 2005; Vol. 3:69-85.
- [3] Parente S.T. y McCullough J.S. Health Information Technology And Patient Safety: Evidence From Panel Data. *Health Affairs* 2009; 28(2):357-60. doi: 10.1377/hlthaff.28.2.357
- [4] Black A.D., Car J., Pagliari C., Anandan C., Cresswell K. et al. The Impact of eHealth on the Quality and Safety of Health Care: A Systematic Overview. *PLoS Med* 2011; 8(1): e1000387. doi:10.1371/journal.pmed.1000387
- [5] Institute of Medicine. *Health IT and Patient Safety: Building Safer Systems for Better Care*. Washington, D.C.: The National Academies Press; 2012.
- [6] Sittig D.F. y Singh H. Electronic Health Records and National Patient-Safety Goals. *N Engl J Med* 2012; 367(19):1854-60.

- [7] Department of Health and Human Services. Health Information Technology Patient Safety Action & Surveillance Plan. Washington, D.C.: Department of Health and Human Services, Office of the National Coordinator for Health Information Technology; 2013.
- [8] Sittig D.F., Ash J.S. y Singh H. ONC Issues Guides for SAFER EHRs. *Journal of AHIMA*, 2014; 85(4):50-2.
- [9] Sittig D.F., Ash J.S. y Singh H. The SAFER Guides: Empowering Organizations to Improve the Safety and Effectiveness of Electronic Health Records. *Am J Manag Care* 2014; 20(5):418-23.
- [10] ECRI Institute. Top 10 Health Technology Hazards for 2013. *Health Devices*, 2012 Nov; 41(11):342-65.
- [11] ECRI Institute. Top 10 Health Technology Hazards for 2014. *Health Devices*, 2013 Nov; 42(11):354-80.
- [12] ECRI Institute. Top 10 Health Technology Hazards for 2015. *Health Devices*, 2014 Nov; 43(11).
- [13] Walker J.M., Hassall A., Bradshaw B. y Rezaee M.E. Health IT Hazard Manager Beta-Test: Final Report. Rockville, MD: Agency for Health care Research and Quality; 2012.
- [14] Dimick C. WARNING Health IT May Be Hazardous to Your Healthcare: New Health IT Hazard Manager Helps Providers and Vendors Track Electronic Health Systems' Side Effects. *Journal of AHIMA* 2014; 88(3):34-9.
- [15] Project Management Institute. Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®). 4ª ed. Newtown Square, PA: Project Management Institute; 2008.
- [16] Cuevas C., Neria M. y Benavente M.J. El sistema de información para la administración de medicamentos a pacientes hospitalizados. En: Carnicero J. (coordinador). La gestión del medicamento en los Servicios de Salud. Informes SEIS (8). Pamplona: Sociedad Española de Informática de la Salud; 2008. 135-63.
- [17] Indarte S. y Vero Á. Sistemas de apoyo a la toma de decisiones clínicas y de gestión en atención primaria de salud. En: Carnicero J., Fernández A. y Rojas D. (coordinadores). Manual de salud electrónica para directivos de servicios y sistemas de salud (II). Aplicaciones de las TIC a la atención primaria de salud. Informes SEIS (10). Comisión Económica para América Latina y el Caribe, Sociedad Española de Informática de la Salud; 2014. 181-202.
- [18] MacDonald R. Commentary: A patient's viewpoint. En: Mandl K.D., Szolovits P, Kohane I.S. Public standards and patients' control: how to keep electronic medical records accessible but private. *British Medical Journal* 2001, 322:283-7.
- [19] Perakslis, E.D. Cybersecurity in Health Care. *N Engl J Med* 2014; 371(5):395-7.
- [20] Cortez N.G., Cohen I.G. y Kesselheim A.S. FDA Regulation of Mobile Health Technologies. *N Engl J Med* 2014; 371(4):372-9.
- [21] Carnicero J. y Rojas D. Lessons learned from implementation of information and communication technologies in Spain's healthcare services: issues and opportunities. *Appl Clin Inform* 2010; 1(4):363-76.

## Capítulo IV

# TIC aplicadas a la seguridad del paciente dentro del laboratorio de análisis clínicos

*Miguel Angel De Cristóforo*

*Matías G. Dombald*

*Nereo N. Candenas*



## Resumen

Muchas son las instancias en las que la tecnología puede intervenir para lograr una mejora continua de la calidad y sobre todo influenciar positivamente sobre la seguridad del paciente durante el proceso de atención en el ámbito del laboratorio de análisis clínicos.

Para encarar en forma sistemática todo el proceso diagnóstico del laboratorio, se acepta dividirlo en distintas etapas denominadas comúnmente como “Pre-analítica”, “Analítica” y “Post-analítica”, que se describirán en los diferentes apartados de este capítulo.

El empleo de las tecnologías de la información y la comunicación (TIC) forman parte importante, si no ineludible, en el manejo de este proceso, al punto tal que no se puede concebir un laboratorio moderno sin sistema de información. Sin embargo, es importante tomar en cuenta que este aporte genera potencialmente nuevas posibilidades de error, que indefectiblemente deben ser consideradas y controladas.

## Introducción

La complejidad alcanzada por la tecnología y la influencia que los resultados del laboratorio pueden ejercer sobre el diagnóstico, el establecimiento de un tratamiento específico, el pronóstico de las patologías y su seguimiento, requieren el reconocimiento de la responsabilidad directa que el laboratorio de análisis clínicos tiene sobre el manejo de la salud de los pacientes.

En una concepción moderna, las exigencias en cuanto a la velocidad de la generación de resultados, el volumen, la disponibilidad de datos históricos en línea, el control de calidad para lograr la máxima eficiencia y la revisión dinámica de los procesos, requieren de un sólido sistema de información de laboratorio (SIL), eje alrededor del cual gira toda su operatoria.

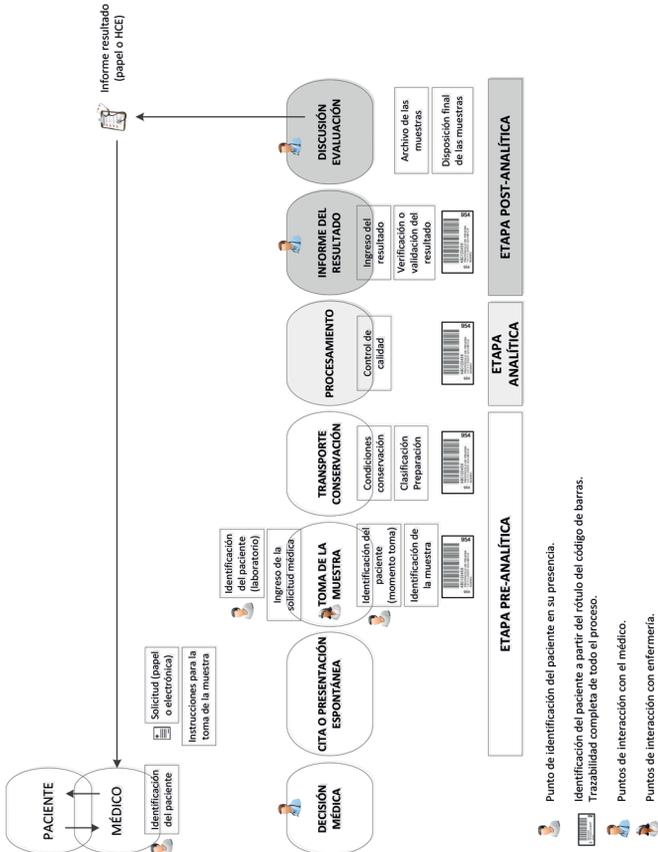
Las mejoras de los sistemas de información en el ámbito del laboratorio de diagnóstico clínico, introdujeron avances de gran impacto positivo en todas las actividades desarrolladas en el mismo, favoreciendo la comunicación efectiva con el personal de salud involucrado en la atención del paciente, médicos, enfermería, farmacia y otras áreas diagnósticas.

En sus comienzos los sistemas de información se ocupaban exclusivamente de las etapas administrativas de la atención, con injerencia fundamentalmente en la recepción de la petición médica y el informe de los resultados. En la actualidad los sistemas gestionan todas las fases del proceso de laboratorio y se integran e interaccionan con el resto de los sistemas clínicos [1].

En un SIL moderno, miles de datos en línea pueden ser elaborados y mostrados en forma ordenada, clara y confiable. Estos procesos involucran el ingreso de las peticiones médicas, sus informes, las interfases con los auto analizadores, los sistemas expertos de validación, el informe de resultados en tiempo y forma a las áreas críticas (emergencias), las consultas históricas, la integración en el contexto individual del paciente, el pasaje a la historia clínica electrónica, la gestión de control de calidad, y otras funciones esenciales cuya ejecución y disponibilidad exigen una disponibilidad 7x24, con todo lo que ello implica respecto a los resguardos y prevenciones tanto de software como de hardware.

# Modelo de la “cadena diagnóstica del laboratorio”<sup>33</sup>

## Ciclo: Solicitud - Paciente - Muestra – Resultado



**Figura 4.1.** El proceso diagnóstico de laboratorio.

Este modelo describe el proceso diagnóstico desde la necesidad médica de conocer el estado de salud de un paciente o realizar un diagnóstico como punto de partida, finalizando cuando el profesional a cargo tiene disponible el informe de resultados y a partir del mismo es capaz de tomar decisiones médicas (ver Figuras 4.1 y 4.2).

El proceso diagnóstico de laboratorio debe constituir una sucesión de pasos encadenados tras una lógica que nos permita arribar a conclusiones respaldadas científicamente y aseguradas por un estricto control de calidad.



La eficacia de todo el proceso depende de la fortaleza del eslabón más débil.

**Figura 4.2.** Eficacia del proceso diagnóstico de laboratorio.

### Paciente. Identificación.

La identificación inequívoca del paciente es una necesidad esencial de toda actividad en el área de la salud. Por supuesto que el laboratorio de diagnóstico clínico no se encuentra exento de este requerimiento, se describen a continuación cómo el empleo de las TIC puede ayudar a realizar una identificación más segura.

El proceso de identificación del paciente, por más simple que parezca, es crucial a la hora de obtener las muestras y/o materiales adecuados para los estudios que se van a realizar. Todos los procedimientos analíticos que son realizados en el laboratorio se ejecutan en ausencia física del paciente, sobre las muestras y materiales biológicos obtenidos oportunamente, confinados en contenedores específicos identificados con un rótulo. La única forma de certificar que los resultados obtenidos pertenezcan al paciente, es asegurar la identidad del mismo en el punto de toma y a partir de allí garantizar la trazabilidad de cada tubo o contenedor y sus eventuales alícuotas o fracciones, si las hubiera, a través de todo el proceso.

Los tubos y contenedores de muestras biológicas son la representación del paciente durante su procesamiento puertas adentro del laboratorio, por lo tanto deben estar identificados en forma clara, segura e inequívoca.

Este proceso debe anteceder a la atención en el laboratorio, en otras palabras, el paciente debe llegar al punto de partida de sus estudios ya identificado con los parámetros mínimos que adoptó la institución o lugar de atención.

El uso de las TIC para la identificación de los pacientes, es utilizado en una primera instancia en la línea de atención ambulatoria para identificar correctamente a las personas, mediante sus datos demográficos almacenados en los sistemas informáticos. Las normativas internacionales (Joint Commission, College of American Pathologists) [2] [3] sugieren el empleo de por lo menos dos datos independientes para la identificación segura de los pacientes, como son la fecha de nacimiento y el apellido-nombre. Cuando estos datos no sean suficientes se deberá recurrir a otros datos como número de documento de identidad, otros apellidos familiares o la foto actualizada, de estar disponible. En segunda instancia debe existir otro punto de identificación del paciente en el momento previo a la extracción de sangre u obtención de muestras, con los mismos datos que en la primera instancia. Aquí, los datos aportados por los sistemas informáticos, son contrastados con los datos obtenidos de la comunicación verbal con el paciente. Este doble control permite garantizar que se trata del paciente correcto.

La identificación certera del paciente debe incluirse dentro de los indicadores de gestión de calidad del laboratorio (véase Tabla IV.2). Para ello se registra el número de pacientes sin errores de identificación relacionándolos con el número total de pacientes atendidos; en ambientes hospitalarios, estos errores pueden clasificarse por tipo de paciente (internado, ambulatorio, urgencia). El registro de seguimiento de este indicador debe ser lo más cercano posible al 100%. En los casos en que el proceso de identificación falle, debe revisarse el evento y tomar las acciones correctivas puntuales para solucionar el mismo y por otro lado, es necesario evaluar las medidas preventivas adecuando el proceso para que no se repita en situaciones posteriores. Para aquellos casos en que la falla se deba al incumplimiento de los procesos según constan en los manuales de procedimientos, debe re-entrenarse al personal y dejar documentación que evidencie dicho entrenamiento [4].

Debe especificarse claramente al personal responsable de identificar al paciente, cuál es el procedimiento correcto. Las preguntas deben ser orientadas acerca de información que el paciente debe conocer y suministrar y no tienen que contener datos del mismo, ya que una distracción u obnubilación del paciente podría generar un error en su identificación.

**Ejemplos incorrectos de la identificación del paciente:**

¿Es Ud. Francisco García? o ¿Su fecha de nacimiento es el 01 enero de 1959?

**Ejemplos correctos para la identificación del paciente:** ¿Cuál es su nombre?; ¿Cuál es la fecha de su nacimiento?

Solicitud, pedido médico.

Las peticiones médicas en papel traen aparejados diversos tipos de errores que deben controlarse, por ejemplo, errores de interpretación por parte del operador que ingresa el pedido (ocurre fundamentalmente en especialidades de laboratorio como inmunología, virología o biología molecular<sup>13</sup>); errores de ilegibilidad por la letra del profesional o, cuando se solicita por códigos, los errores de tipeo del mismo. Las soluciones propuestas para errores generados con los pedidos manuales incluyen: formularios impresos, peticiones con perfiles fijos pre-impresos por servicio, doble chequeo de peticiones en tiempo real o diferido, incorporación de pedidos electrónicos.

La integración de los pedidos médicos a través de sistemas informatizados constituye un aporte extraordinario de las TIC como medio para evitar errores en la transcripción manual de los mismos. Estos aportes a su vez, generan otro tipo de errores sobre los que se debe trabajar (véase Tabla IV.1).

<sup>13</sup> Petición de estudio para toxoplasmosis: ¿IgG. IgA o IgM?; PCR: ¿proteína C Reactiva? o polimerasa Chain reaction.

Tabla IV.1. Fuentes de error en las peticiones médicas.			
Tipo de petición	Fuentes de error	Problemas asociados	Estrategias para su solución
En papel	Ilegibilidad.	Dificultades en la lectura por la letra del médico, que pueden llevar a: <ul style="list-style-type: none"> <li>• Desconocer lo solicitado por el profesional omitiendo su ingreso al SIL.</li> <li>• Pérdida de tiempo para solucionar la lectura</li> <li>• Interpretación errónea del estudio solicitado incorporando una práctica no solicitada.</li> </ul>	Formularios pre-impresos. Peticiones electrónicas a través de un repositorio único de estudios (Historia clínica electrónica o similar). Corrección de ingreso de las peticiones en forma diferida por personal especializado. Consulta al profesional del área en el momento del ingreso de la petición.
En papel	Peticiones genéricas.	Peticiones médicas dirigidas hacia alguna situación general sin especificar exactamente cuál es el estudio requerido. Ejemplo: “Hepatitis B”; “perfil hepático”, “estudio de coagulación”, “perfil autoinmune”.	Encuentros de educación continuada para el entrenamiento del personal médico respecto de la forma correcta de realizar las peticiones. Manual del usuario interno (en papel o electrónico) que sirva de consulta frente a la necesidad de realizar el pedido.
En papel	Codificaciones numéricas similares.	En ciertos laboratorios se utilizan, para acelerar el ingreso de las peticiones, códigos numéricos para identificar los estudios. En situaciones de sobrecarga de trabajo o agotamiento laboral pueden existir confusiones en el ingreso de dichos códigos.	Doble ingreso de la petición en tiempo real, el personal ingresa la petición al sistema y en una segunda instancia la reingresa, ambos ingresos deben coincidir. La detección de inconsistencias emite alertas para su solución. Corrección de ingreso de las peticiones en forma diferida por personal especializado.
En papel	Incorporación u omisión de prácticas.	Fundamentalmente en peticiones con numerosas prácticas o en aquellas en que la distribución del texto sobre la hoja es desordenado.	Formularios pre-impresos. Peticiones electrónicas a través de un repositorio único de estudios (Historia clínica electrónica o similar).
En papel	Error en la elección de los estudios dentro de formularios pre-impresos.	En aquellos formularios con casilleros para seleccionar estudios, puede haber confusión entre la lectura de la línea del texto y el casillero elegido (selección del casillero anterior o posterior).	Preparación de formularios con diseños especiales de contraste entre líneas contiguas. Peticiones electrónicas a través de un repositorio único de estudios (Historia clínica electrónica o similar).
Papel o electrónica	Omisión de una práctica en la petición médica indispensable para informar una solicitada.	El profesional omite solicitar un estudio indispensable para el cálculo o la interpretación de otro incluido en la petición. Ejemplo: <ul style="list-style-type: none"> <li>• Pedido de PSA libre, sin solicitar PSA total.</li> <li>• Pedido de colesterol HDL o LDL sin solicitar colesterol total.</li> </ul>	Encuentros de educación continuada para el entrenamiento del personal médico respecto de la forma correcta de realizar las peticiones. Para peticiones electrónicas ventanas de alertas solicitando su incorporación. Incorporación automática en el momento de efectuar la solicitud (estudios <i>reflex</i> ).

Tabla IV.1. Fuentes de error en las peticiones médicas.			
Tipo de petición	Fuentes de error	Problemas asociados	Estrategias para su solución
Electrónica	Peticiones mal seleccionadas en repositorios electrónicos.	<p>Cuando una determinada patología tiene múltiples opciones de estudios de laboratorio, el profesional médico debe seleccionar exactamente lo necesario para confirmar sus sospechas clínicas.</p> <p>Ejemplos:</p> <ul style="list-style-type: none"> <li>- El profesional busca “Hepatitis”. Debe seleccionar del listado las opciones relacionadas con sus sospechas clínicas:                             <ul style="list-style-type: none"> <li>• Diagnóstico de hepatitis aguda a virus A, B, C, E u otro.</li> <li>• Estudios confirmatorios de HCV</li> <li>• Diagnóstico de crónica</li> <li>• Control de vacunación,</li> <li>• Portación asintomática,</li> <li>• Genotipificación por biología molecular</li> <li>• Estudio de seguimiento por carga viral</li> <li>• Otros.</li> </ul> </li> <li>- Perfil de coagulación                             <ul style="list-style-type: none"> <li>• Tiempo de protrombina,</li> <li>• APTT,</li> <li>• Factores,</li> <li>• Otros.</li> </ul> </li> </ul>	<p>Opciones de ayuda (info buttons) que permitan la orientación sobre áreas específicas.</p> <p>Ayudas en línea para detectar incoherencias en la petición.</p>

Como punto de partida, el uso de las TIC en este particular y en relación a la seguridad del paciente han mejorado el proceso, eliminando la necesidad de transcribir las peticiones médicas en los sistemas hospitalarios o en los SIL, evitando de esa manera los errores mencionados anteriormente. No obstante, esta indiscutible mejora incorporada, expone al usuario solicitante a otro tipo de errores como por ejemplo la incorrecta selección del estudio desde un menú de opciones de laboratorio, debido a una distracción o de un error en la elección. A menudo se observan errores en la solicitud de estudios cuando el buscado por el médico tiene opciones múltiples. Por ejemplo, el médico quiere solicitar un examen para descartar una hepatitis aguda a virus B y al buscar en el archivo maestro se le presentan múltiples opciones<sup>14</sup> y en el apuro selecciona la incorrecta.

<sup>14</sup> Hepatitis B anticuerpos de superficie (anti HBs); Hepatitis B, antígeno de superficie (HBsAg), Hepatitis B anticuerpos anti core IgM (anti HBe IgM), Hepatitis B anticuerpos anti core IgG (anti HBe IgG), Hepatitis B anticuerpos anti e (anti HBe); Hepatitis B antígeno e (HBeAg); Hepatitis B, ADN por PCR; Hepatitis B, carga viral; Hepatitis B, genotipificación.

Cuando el médico dispone de herramientas informáticas adecuadas para realizar las solicitudes electrónicas de laboratorio, dicho proceso debe contemplar entre otros parámetros el tipo de paciente: Internado, Emergencias o Ambulatorio y la característica de su pedido: Urgencia o Rutina.

Si la aplicación que genera el pedido es externa al SIL, es requerimiento básico que la información de intercambio entre el sistema solicitante y el sistema del laboratorio (SIL), contemple la incorporación automática de las condiciones de identificación que mencionábamos anteriormente, junto con otros datos indispensables para la posterior evaluación de los resultados como el sexo, la edad, el diagnóstico presuntivo y otras informaciones relevantes según el estudio solicitado, ejemplo: paciente embarazada, fumador, control de anticoagulación.

Si se dispone de Historia Clínica Electrónica (HCE) es necesario considerar la forma de comunicación entre el sistema informático hospitalario (SIH) y el sistema informático del laboratorio (SIL). Sin lugar a dudas la plataforma *Health Level Seven (HL7)* ofrece estándares de comunicación que facilitan el intercambio de información clínica.

**La transferencia de las solicitudes médicas desde el SIH al SIL las convierte en “esperanzas de resultados”. El arribo de muestras físicas al laboratorio las convierte en “protocolos de laboratorio”.**

## Preparación del paciente

Para que la calidad de las muestras sea la óptima requerida por el Laboratorio, las indicaciones para la toma de las mismas deben estar disponibles para su consulta, tanto por parte del cuerpo médico en el momento de la prescripción, así como por pacientes durante la preparación. Contribución de las guías en línea para el usuario externo al laboratorio: médicos y pacientes.

Un muestreo correcto garantiza la calidad de los resultados emitidos por el laboratorio.

Todos los autores concuerdan que el control de los procesos pre-analíticos constituyen uno de los puntos claves para la emisión de resultados de calidad.

Las indicaciones para la toma de las muestras deben estar escritas en un lenguaje claro y coloquial, logrando de esta manera que no haya interpretaciones erróneas por parte de los médicos y/o pacientes.

Las TIC en este apartado contribuyen a la difusión y disponibilidad en línea de los instructivos, así como también ayudan al mantenimiento y la actualización de los mismos. En lugares con disponibilidad de historia clínica electrónica (HCE) el médico solicitante tiene la ventaja de visualizar/imprimir los instructivos durante el acto de solicitar los estudios. Esto favorece la revisión de las instrucciones junto con el paciente para asegurar una toma correcta de las muestras.

### Extracción. Requerimientos especiales. Conservación de las muestras.

Aporte categórico del empleo de código de barras (*Barcoding*) como método para la identificación segura de pacientes / muestras, en el proceso de ubicación, seguimiento y almacenamiento en el laboratorio. Recaudos a tomar en consideración.

Existen varias instancias en la atención de los pacientes donde se requiere su identificación, que debemos considerar en este apartado.

**Identificación de pacientes ambulatorios:** Tal como se menciona anteriormente, las personas deben estar previamente empadronadas en un archivo maestro. A partir de esta premisa, se recibe la solicitud médica en forma manual o electrónica, el operador del laboratorio debe verificar la identidad del paciente utilizando por lo menos dos datos demográficos independientes, por ejemplo, nombre completo y la fecha de nacimiento (esto ya fue discutido en el apartado Pacientes. Identificación). Los datos aportados por el sistema, que se muestran en pantalla, son contrastados con los obtenidos en la comunicación verbal con el paciente. Una vez verificada la identidad del paciente, el personal de laboratorio inicia la carga del pedido. Durante este procedimiento *pre analítico*, los empleos de las TIC ofrecen al operador las ayudas necesarias para disponer de los datos relevantes del paciente para su correcta identificación.

**Identificación de pacientes internados:** en las instituciones que disponen de una Historia Clínica Electrónica (HCE) la totalidad de

los pedidos médicos son ingresados electrónicamente en la ficha del paciente. La condición que debe cumplirse de forma estricta, es que la verificación de la identidad del paciente se debe realizar en el momento de la toma de la muestra, al lado de la cama del paciente. Para realizar este procedimiento existen diversas opciones que van desde la consulta oral al paciente (con distintos grados de complejidad originados en situaciones en las que el paciente esté inconsciente o con afecciones cognitivas) hasta la **utilización** de la pulsera identificadora colocada en el momento de la admisión del paciente.

Nunca utilizar datos inciertos como el número de la habitación/cama para la identificación del paciente, ya que pueden ocurrir cambios de ubicación no registrados.

**Identificación de pacientes de emergencias:** se siguen las indicaciones para pacientes ambulatorios o, en el caso de pacientes inconscientes o que no puedan responder a las preguntas, se pueden remitir muestras rotuladas en forma manual acordando una identificación transitoria hasta tanto se cumpla la correcta identificación del paciente.

El siguiente paso del proceso de identificación es la emisión de los rótulos para los tubos y/o contenedores, acción que preferentemente debe llevarse a cabo junto al paciente, ya que esa muestra o contenedor constituye la “representación” del paciente en todo su recorrido dentro del laboratorio.

El paciente debe ser identificado en el momento de la carga de la solicitud o pedido médico y se debe volver a identificar en el momento de la extracción cuando se rotulan las muestras o contenedores.

El apoyo de las TIC en esta etapa, ha ofrecido la oportunidad no solo de identificar correctamente al paciente, sino también de registrar otras variables de gran utilidad para la trazabilidad integral del proceso, por ejemplo, registrando al técnico de laboratorio que efectuó la extracción; el momento exacto en que fue realizada (fecha/hora) la toma de muestra, su procesamiento *pre analítico*.

Desde el punto de vista de gestión de procesos y recursos las TIC permiten medir la eficiencia en la atención de los pacientes, registrando los tiempos de espera en las distintas etapas desde su ingreso al sector de atención hasta que se retira a su domicilio.

Una vez finalizada la correcta identificación y atención del paciente, el mismo se “convierte” en muestras, las cuales seguirán un proceso complejo dentro del laboratorio que las convertirá en información de uso médico para la toma de decisiones.

El paso de toma de muestra constituye el segundo punto de corroboración de la identificación del paciente.

El empleo de códigos de barra (barcoding) ha ofrecido al proceso de identificación de muestras un beneficio de vital importancia que ha impactado directamente en la seguridad del paciente, la trazabilidad de las muestras y la velocidad de proceso.

El uso de código de barras como método para la identificación de las muestras permite registrar toda la historia de la misma (*tracking*), desde la extracción hasta el descarte, cuando todos los estudios estén finalizados.

El uso de dispositivos para la lectura de los códigos de barras ayuda a evitar errores de identificación a todo nivel. Dichos lectores deben estar disponibles en puntos de ingreso de muestras (*check in*), en puntos de seguimiento de las mismas (*tracking*), en los analizadores (*host query*), en los puntos de almacenamiento y descarte. Todos estos puntos constituyen potenciales fuentes de errores si en cada uno de ellos se debe ingresar manualmente la identificación del contenedor.

### Transporte, traslado controlado.

#### Aportes de las TIC al proceso de transporte de muestras.

El transporte de las muestras desde el lugar de extracción hasta el destino de procesamiento debe ser monitoreado de manera continua, registrando para cada muestra el tiempo, la hora y la temperatura de transporte. Para este registro los contenedores de transporte utilizan sensores de registro electrónico continuo de temperatura (*data loggers*). Este proceso garantiza la calidad de las muestras transportadas.

## Recepción segura de las muestras

Aportes de las TIC en el ingreso efectivo o registro de las muestras al circuito del laboratorio.

El ingreso (*check-in*) de las muestras en el sector *pre analítico* da inicio al procesamiento del pedido médico en el circuito del laboratorio. Mediante un programa de seguimiento (*tracking*) se realizan dos tareas simultáneamente, el direccionamiento de muestras a los sectores del laboratorio donde serán procesadas y el registro de la historia de las muestras o contenedores en su recorrido por el laboratorio.

Cada evento de seguimiento de muestras (*tracking*) se realiza en estaciones destinadas a tal fin, donde un simple escaneo del código de barras permite la toma de decisiones registrando en el SIL el lugar, fecha/hora y operador responsable del evento.

La importancia que las TIC ofrecen a través del tracking, es el control completo del flujo de las muestras por los distintos puntos de procesamiento dentro del laboratorio y el recorrido de cada una de las mismas, desde la extracción hasta el momento del descarte.

La disponibilidad de un sistema informático adecuado permite predecir y controlar eficientemente situaciones como, por ejemplo:

- ¿Debe la muestra mantenerse en condiciones especiales como refrigeración inmediata o conservación a temperatura corporal (37°C)?
- ¿La muestra se procesa como tal o debe someterse a un proceso de centrifugación?
- ¿A qué sector del laboratorio debe ir cada muestra?
- ¿El tubo debe destaparse para ser procesado?
- Si ya fue procesada en un sector. ¿Se debe enviar al archivo de muestras o se debe redireccionar a otro sector?
- ¿En qué momento se puede descartar definitivamente una muestra?

## Procesamiento Pre-Analítico, Fraccionamiento

Hasta el momento se expusieron las actividades *pre-analíticas* relacionadas con la identificación del paciente, de las muestras y su ingreso físico al

circuito de procesamiento, actividades que algunos autores mencionan como “*pre-pre analíticas*” [5][6]. Dentro de las actividades *pre-analíticas* del laboratorio existen algunas tareas rutinarias que pueden generar errores fundamentalmente en cuanto a las demoras para la entrega en tiempo y forma de los resultados.

**Se acepta que todas estas actividades pre-analíticas están sujetas a numerosas posibilidades de error [7][8].**

El uso de sistemas robóticos para el área pre-analítica permite automatizar tareas rutinarias que están sujetas a errores humanos o a la generación de accidentes con muestras, como:

- El direccionamiento erróneo de muestras a sectores del laboratorio.
- El destapado y tapado de tubos, indispensable para auto-analizadores que trabajan con alta velocidad, los que requieren el empleo de tubos destapados.
- La alicuotación (fraccionamiento) de muestras con el indispensable re-rotulado replicando el rótulo de origen (el fraccionamiento de muestras con rotulado manual puede generar errores de adjudicación),
- El control de la correcta asignación contenedor-prácticas solicitadas
- El control del volumen de muestras, la correcta relación muestra/ anticoagulante, etc.

En esta función el equipo robótico lee el código de barras de cada contenedor/muestra y actúa según las funciones pre-programadas por los especialistas, desde el sistema informático de Laboratorio (SIL), dejando las muestras listas para su procesamiento o separándolas cuando no cumplen con algún parámetro (Volumen, forma, calidad, identificación y asignación).

El uso de este tipo de equipamientos robóticos en esta etapa del proceso pre-analítico acelera los tiempos de llegada de las muestras a la estación de trabajo correcta y garantiza la optimización de tiempos en el proceso de las mismas, ya que permite detectar por su paso si hay muestras de un sector que tienen estudios pendientes en otros sectores.

## Procesamiento de las muestras

### **La implementación de las TIC para el procesamiento eficiente de las muestras requiere necesariamente su encuadre dentro de un programa integral de gestión de la calidad.**

Una vez que las muestras llegan a las estaciones de trabajo, comienza la etapa analítica del proceso. Los laboratorios con mediana y alta tasa de demanda o gran volumen de muestras, deben contar con analizadores automáticos que realizan los análisis correspondientes a cada muestra de acuerdo a los pedidos médicos ingresados al SIL (*host query*) y luego transmiten los resultados obtenidos para ser evaluados y validados por el profesional responsable. Estos equipos se comunican con el SIL por medio de interfaces que utilizan diversos protocolos estándares de comunicación (HL-7<sup>15</sup>, ASTM<sup>16</sup>, archivos planos, etc.). La comunicación bidireccional entre analizadores y SIL es la más efectiva en la transmisión de peticiones y de resultados, algunas de ellas ofrecen tareas de verificadores automáticos con reglas preestablecidas por los profesionales expertos en cada área.

La suma de TIC aplicadas a la etapa del procesamiento de muestras en el laboratorio (como son los analizadores, protocolos de comunicación, auto-verificadores, alertas varias, etc.) han logrado un impacto altamente positivo en la seguridad del paciente, minimizando los errores. Los errores analíticos en un laboratorio informatizado y automatizado, en el cual se trabaja con muestras y contenedores identificados mediante rótulos con códigos de barra (*barcoding*), se han llevado a una expresión mínima [9][10].

Así como las TIC influyen positivamente en todas las cuestiones de procesamiento automatizado, en cuanto a seguridad, exactitud y precisión en los resultados, exigen por otro lado la validación y mantenimiento continuo mediante indicadores de gestión que certifiquen el correcto funcionamiento.

La gestión de controles de calidad, se debe realizar por analizador, por analito<sup>17</sup> y por turno, asegurando la obtención de resultados dentro de

<sup>15</sup> Health Level Seven.

<sup>16</sup> American Society for Testing and Materials Standards.

<sup>17</sup> Analito es el componente o compuesto de interés analítico de una muestra, se puede asimilar a prueba o test.

los parámetros aceptables. Para los casos en que haya en funcionamiento más de un analizador para la misma determinación, se deben realizar controles cruzados en forma simultánea para asegurar la calidad y la independencia del analizador sobre la obtención del resultado.

Pese a los avances de la tecnología existe una considerable cantidad de estudios que se realizan manualmente y requieren inevitablemente la intervención humana. Ejemplos típicos de estos estudios lo constituyen las observaciones microscópicas, los estudios microbiológicos, y las pruebas de aglutinación entre otros.

Un apartado especial debería considerarse para el sistema de información del laboratorio de microbiología clínica que debe reunir características particulares para que pueda gestionar de forma eficaz la información necesaria para sus actividades exclusivas [11].

## Informe de resultados

### **Los distintos tipos de resultados generados en el laboratorio de análisis clínico y su forma de ingreso al SIL. Cómo las TIC pueden ayudar a reducir los errores durante la carga de resultados, mediante alarmas o sistemas alternativos de informe o verificación.**

Es importante destacar en este apartado que existen distintos tipos de resultados que genera un laboratorio:

- a. Resultados numéricos, considerando signo (+/-) y modificadores (>/<).
- b. Resultados discretos que, pese a ser de texto, los mismos adoptan valores fijos y predeterminados, ejemplo “reactivo”, “no reactivo”, “positivo”, “negativo”, “abundante”, “escasas”, “turbio”, “límpido”, colores, etc.
- c. Textos largos que pueden codificarse o textos libres.
- d. Imágenes o gráficos representativos.

Todos estos resultados que genera un laboratorio pueden ser ingresados en forma manual o electrónica, vía interface de comunicación de un auto-analizador con el SIL.

Cuando nos referimos a determinaciones que se procesan manualmente, el rol de la parametrización es vital, ya que en este caso

ya que en este caso las TIC aportan barreras o alertas necesarias para evitar todo tipo de errores que puedan ocurrir durante el ingreso manual de los resultados (rangos analíticos, rangos de referencia, rangos de validación para informe de resultados anormales, rangos de valores críticos o pánico donde está en juego la vida del paciente).

Los errores más comunes son los de tipeo, errores de asignación, errores de transcripción, reportes fuera de los rangos aceptables, etc.

Existen procedimientos que pueden atenuar estos errores como la doble carga en el ingreso de los resultados, doble chequeo contra el dato crudo, alertas configuradas ante el ingreso de valores no habituales o con diferencias significativas con los datos históricos del paciente (*delta-check*), siempre antes de ser validados por el profesional a cargo.

Algunos resultados del laboratorio dependen exclusivamente del operador humano, por ejemplo, aquellos estudios que dependen de la observación microscópica, las pruebas de aglutinación con lectura visual, corridas electroforéticas.

El ingreso de resultados en forma manual está expuesto a numerosos errores humanos en los que diversos factores propios del operador y del medio los condiciona como: fatiga, distracciones, errores de tipeo, interrupciones, alta carga de trabajo, etc.

Los resultados que ingresan mediante interfaces desde los analizadores evitan los errores mencionados en el punto anterior, sin embargo, los protocolos de comunicación requieren un minucioso proceso de validación mediante el cual se certifique su fiabilidad. Se deben tener en cuenta y descartar los errores por el efecto de variables como la configuración regional de la terminal, cantidad de cifras decimales, aproximación de cifras numéricas y traducciones automáticas.

Un sistema informático de laboratorio que se precie de influir sobre la calidad de sus resultados, debe ofrecer al operador las alertas necesarias para impedir el ingreso de resultados anómalos o prevenir al operador sobre aquellos que estén fuera del rango de referencia o que requieran una atención especial.

## Verificación de resultados

**Se describen los aportes de las TIC para evitar errores de validación. Así como las virtudes y problemas en la implementación de sistemas automáticos de verificación<sup>18</sup> y/o validación en línea.**

La verificación de los resultados constituye una operación totalmente independiente del ingreso de los mismos. En una situación ideal el profesional que verifica el resultado debería ser distinto al que realizó el ingreso; sin embargo, en normativas de acreditación como las del Colegio Americano de Patólogos (CAP) [3], este procedimiento puede ser efectuado por la misma persona siempre y cuando se realicen en dos momentos distintos.

Verificar un resultado obtenido es el proceso por el cual se evalúa el mismo, considerando datos del paciente, edad, sexo, estado fisiológico, diagnóstico, asociándolos con datos preestablecidos para cada estudio como rango reportable, rango de referencia, delta check, rango crítico, tendencias, repeticiones, etc.; antes de liberarlos al grupo médico.

Para laboratorios con alta demanda de estudios, la emisión diaria de miles de resultados exigiría una cantidad de profesionales extremadamente grande para llevar adelante los procesos de verificación y pese a esto, la operatoria se vería afectada por los errores humanos que genera esta actividad de alta complejidad. El diseño de auto-verificadores de resultados, que emulan los algoritmos de verificación que utilizan los profesionales del área, es un aporte fundamental de las TIC a las áreas de procesamiento e informe del laboratorio.

El Auto-validador es una aplicación que actúa a través de algoritmos *booleanos*, siguiendo una lógica establecida por especialistas del área, que marca como verificados resultados que cumplan con las reglas previamente definidas y dejando en pendientes aquellos resultados que requieren un análisis con intervención humana. Los datos auto-verificados pasan directamente a los sistemas terceros como la HCE sin intervención humana.

<sup>18</sup> El término "Verificación" puede encontrarse en algunos documentos expresado como "Validación" o "Liberación".

La implementación de estos aplicativos de auto-verificación requiere minuciosos chequeos previos para certificar su correcto funcionamiento, antes de ser puestos en producción con datos de pacientes. Asimismo, es necesario un control periódico de los mismos y cada vez que se agreguen, quiten o modifiquen parámetros o lógicas que afecten los algoritmos.

Los auto-verificadores deben tener configuraciones claras cuando se trata de valores numéricos.

El ingreso de un resultado y su verificación deben ser acciones independientes, sobre todo en el caso de las técnicas manuales. Para evitar errores, lo ideal es que un resultado manual sea validado por un profesional distinto al que realiza el ingreso del dato, aunque puede ser la misma persona pero en dos momentos separados, (en un tiempo ingresa los resultados y después los valida chequeando contra los datos crudos).

La verificación manual de resultados requiere un cuidadoso control a partir de los datos originales o crudos enviados por los equipos o resultados manuales registrados en planillas o libros de trabajo. Estos últimos están sujetos a errores humanos ya mencionados en el ingreso de resultados.

## Disponibilidad de los resultados

**Las TIC como factores fundamentales de la entrega en lugar, tiempo y forma de resultados. Sistemas de ayuda en la visualización. Comunicación efectiva de resultados con datos críticos para la salud de paciente (*panic values o critical values*).**

En este apartado se tratarán dos de los temas fundamentales en un laboratorio enfocados hacia la seguridad del paciente y en los que las TIC cumplen un rol fundamental:

- a. El informe en tiempo y forma de los resultados solicitados por el médico, medido desde que la muestra ingresa al laboratorio hasta que el resultado es informado y está disponible para el médico (*turn around time = TAT*)
- b. La comunicación efectiva de los Valores Críticos obtenidos en el laboratorio con la mayor celeridad posible.

Las TIC posibilitan gestionar grandes volúmenes de datos que de otra manera sería impensado poder lograrlo. Se definen TAT para cada prueba y tipo de paciente en particular (ambulatorio, rutinas de internados, urgencias y emergencias), lo cual permite, al utilizarlo como indicador, un estudio minucioso sobre cómo se están cumpliendo las peticiones médicas en tiempo y forma, considerando que este tiene relación directa con la salud del paciente. Se debe evaluar performance por horarios, por analito, por tipo de paciente, por sección o bien se puede estudiar sólo los casos en los que el tiempo de informe definido se excedió (no se cumplió con el tiempo de informe pactado).

El pasaje de resultados del SIL al SIH deber monitorearse adecuadamente para certificar que los procesos de comunicación están funcionando adecuadamente. El tiempo de grabación de los resultados en la historia clínica electrónica constituye para ello un indicador de gran importancia.

Como en todos los aplicativos de comunicación en formato electrónico, la emisión/recepción de los resultados debe tener su resguardo en otra metodología de comunicación, sea esta una página web de resultados del SIL, telefónica o en papel, para afrontar las contingencias provocadas por la caída del sistema SIH o algún componente de la comunicación.

En la comunicación efectiva de valores críticos las TIC juegan un rol especial, daremos una descripción del proceso.

Los resultados críticos, también llamados alerta o pánico, son aquellos que por su trascendencia sobre la morbilidad o mortalidad del paciente requieren de una atención clínica inmediata.

La comunicación de resultados “críticos” debe realizarse necesariamente desde el laboratorio, con un aplicativo que monitoree, en tiempo real, los resultados de las pruebas que tienen configurados parámetros considerados como críticos o pánico. En cuanto un profesional del laboratorio valida un resultado que cumple con los parámetros de criticidad, el aplicativo lo expone en una ventana emergente para que comunique inmediatamente el resultado al médico a cargo del cuidado del paciente, permitiendo que pueda actuar rápidamente en consecuencia. En esta etapa el sistema registra y

documenta el valor comunicado, el receptor de la comunicación, la confirmación del dato recibido (*read-back*) y los datos del comunicante. Tal como se expone en la Tabla IV.2, este constituye un indicador trascendental para la evaluación de la comunicación efectiva con trascendencia en la seguridad del paciente.

Si se dispone de Historia Clínica Electrónica (HCE) y existe comunicación entre el sistema informático hospitalario (SIH) y el sistema informático del laboratorio (SIL), la información viaja electrónicamente como parte del resultado, generando una alarma visible al profesional. A partir de la recepción de un resultado de valor crítico, el grupo médico debe dejar registro en la ficha del paciente en la HCE sobre el valor recibido, esta acción es llamada “read-back”, y la acción tomada sobre el paciente, como seguimiento.

## Seguimiento

### Aportes de las TIC a los procesos de seguimiento de resultados históricos y a los estudios de causa raíz cuando se producen no conformidades

La visualización de antecedentes y el uso de los mismos para la toma de decisiones en línea, dentro del laboratorio, es un importante aporte de las TIC a la seguridad del paciente. Permite:

- i. Tener una orientación del perfil de resultados del paciente y su seguimiento a través del tiempo, considerando incluso las patologías que sufre, por ejemplo, un paciente diabético está con parámetros descendientes en sus valores de glucosa porque está siendo medicado.
- ii. Por otro lado, la disponibilidad de los antecedentes permitiría detectar muestras que pudieran no pertenecer a un paciente determinado, por ejemplo, las presencias de resultados muy divergentes sobre parámetros estables podrían asumirse como un error en la asignación del paciente o que tengan deficiencias en su toma, desencadenando de esta manera un estudio detallado del incidente. En los análisis de causa-raíz el uso de las TIC, permite un análisis detallado de los registros de todos los eventos que sucedieron desde la identificación/recepción del paciente/ toma de las muestras hasta la verificación de los resultados, datos que sumados a toda la investigación del incidente permiten implementar ciclos de mejora continua, que redundan a futuro en la atención segura y de calidad de los pacientes.

## Indicadores de gestión del laboratorio

Aportes de las TIC a los indicadores de calidad y gestión del laboratorio.

La mejora continua y la gestión de la calidad del laboratorio son pilares fundamentales en la seguridad del paciente. Para ello el laboratorio debe contar con un panel de indicadores, diseñados adecuadamente, que permita la detección de puntos de mejora en los procesos, garantizando una rápida intervención-corrección y la previsión de fallas. El permanente monitoreo de estos indicadores permite evaluar si el laboratorio se encuentra dentro de los estándares internacionales y la comparación con otros laboratorios de similares características a nivel mundial (*Benchmarking*).

Es importante contar con indicadores en las distintas etapas de los procesos, como así también con otros indicadores de performance general (véase Tabla IV.2).

Tabla IV.2. Indicadores de gestión del laboratorio.		
Indicador	Descripción	Aportes TIC
<b>Etapas pre analítica</b>		
Tiempo de espera para pacientes ambulatorios.	<p>Es el registro del tiempo de espera del paciente desde su llegada al laboratorio o centro de extracciones, hasta el momento en que se retira del mismo, ya atendido.</p> <p>En el caso de no tener un servicio totalmente informatizado este tiempo se puede medir por muestreos periódicos, encuestas a los pacientes o ambos.</p> <p>Con ayuda de las TIC esto puede ser llevado a cabo en el 100% de los pacientes, pudiéndose registrar todas las etapas del proceso:</p> <ul style="list-style-type: none"> <li>i) Tiempo de espera hasta la atención administrativa.</li> <li>i) Tiempo de espera hasta la extracción de sangre.</li> <li>ii) Tiempo de la extracción.</li> </ul> <p>Se registra en cada caso el tiempo promedio y el tiempo máximo.</p> <p>Cada laboratorio establecerá el valor de corte sobre el tiempo de espera, a partir del cual deberán tomarse medidas correctivas y preventivas para solucionar el desvío.</p>	<p>Determinar la eficacia en la atención de los pacientes.</p> <p>Distribuir el personal administrativo y técnicos extraccionistas o flebotomistas según la demanda.</p>

Tabla IV.2. Indicadores de gestión del laboratorio.

Indicador	Descripción	Aportes TIC
Errores de ingreso de las prácticas de laboratorio .	Es el registro del porcentaje de errores en la carga de la petición médica. Estos errores incluyen: i. Interpretación de la petición manuscrita. ii. Inclusión de prácticas no solicitadas. iii. Omisión de una o más prácticas solicitadas.	Garantizar la exactitud de las peticiones médicas, asegurando que el profesional reciba los resultados que espera. Evitar la necesidad de realizar un nuevo muestreo.
Integridad de muestras recogidas por el paciente	Porcentaje de muestras rechazadas clasificadas según sus respectivas causas: contenedor incorrecto, incumplimiento de las instrucciones, conservación inadecuada, momento de toma incorrecto.	Este indicador permite tomar medidas correctivas inmediatas como instruir al paciente en forma especial corroborando el entendimiento de las instrucciones o suministrando el contenedor adecuado para la toma. Dentro de las medidas preventivas se mencionan la revisión periódica de las instrucciones escritas para la toma de muestra y el reentrenamiento del personal que da las instrucciones al paciente.
Registro de errores de identificación de pacientes ambulatorios.	Se registra el porcentaje de errores detectados en la correlación entre la identificación de la muestra versus la identificación del paciente.	Sobre este particular las TIC han aportado adelantos importantes como, el archivo maestro de pacientes <sup>19</sup> , solicitar como mínimo dos identificadores independientes (ejemplo: nombre y apellido + fecha de nacimiento), contar con la fotografía actualizada del paciente, identificar al paciente en el acto administrativo y en el acto de toma de la muestra.

<sup>19</sup> Todo paciente que concurra al laboratorio debe estar previamente “empadronado” en un repositorio único que asegure su correcta identificación.

**Tabla IV.2. Indicadores de gestión del laboratorio.**

Indicador	Descripción	Aportes TIC
Registro de errores de identificación de pacientes internados.	Se registra el porcentaje de errores detectados en la verificación de la identidad del paciente utilizando la pulsera identificatoria: pulsera ilegible, ausencia de pulsera, presencia de más de una pulsera.	Permite la identificación segura del paciente independizándose del lugar físico de internación (habitación / cama); del estado de consciencia del paciente; de la consulta a enfermería o a un familiar presente.
Solicitud de nueva muestra.	Se registra el porcentaje de muestras tomadas deficientemente: hemolisadas, coaguladas, insuficientes, contaminadas, contenedores equivocados.	La utilización de equipamiento de análisis interfaseado con el SIL permite la automatización de prácticamente todas estas situaciones, independizando su registro de la observación directa del operador.
Registro de quejas de pacientes.	Se analizan individualmente todas las quejas registradas por los pacientes.	Permite dar respuestas personalizadas a situaciones imprevistas que ocurren durante el proceso de atención.
Encuesta periódica de satisfacción del paciente.	Independientemente de los indicadores de proceso mencionados, una buena gestión requiere la evaluación periódica de lo que el paciente siente o percibe durante de su atención.	Permite detectar situaciones no previstas en el procedimiento de atención.
Conservación y transporte de muestras.	Se registra el porcentaje de muestras que no fueron conservadas/transportadas en forma adecuada: Temperatura de conservación o tiempo transcurrido hasta el momento de procesamiento. <sup>20</sup>	La inclusión de registros continuos y centralizados de temperatura a través de sondas calibradas permite el seguimiento de estas variables. El registro de cada punto de seguimiento (tracking) aprovechando el rotulado con código de barras, permite la emisión de alertas sobre muestras que deben ser procesadas dentro de un tiempo determinado.

<sup>20</sup> Ejemplo, las muestras de Estado Acido Base (deben ser procesadas inmediatamente), Lactato (deben ser mantenidas a baja temperatura hasta el momento de procesamiento), crioglobulinas (deben ser mantenidas a 37°C hasta su procesamiento).

Tabla IV.2. Indicadores de gestión del laboratorio.

Indicador	Descripción	Aportes TIC
<b>Etapa analítica</b>		
Verificación de la precisión, funcionamiento y desempeño de los equipos, auto-analizadores y metodologías manuales.	Registros de control de calibración Registros diarios de control de calidad Registros cruzados de control de calidad <sup>21</sup> Registros inter-turnos del control de calidad <sup>22</sup> Registro de lecturas cruzadas para pruebas que requieran la observación y experiencia del operador. <sup>23</sup>	La informatización permite la evaluación de estos controles en tiempos más rápidos. En lugares con altos niveles de productividad permite incluso la evaluación automática de estos indicadores en tiempo real. Permite la centralización de la gestión de calidad y el armado de paneles de control para supervisores y la dirección del laboratorio.
Eficiencia en la respuesta a las pruebas de evaluación externa.	Registro del porcentaje de aciertos en la evaluación de los controles externos de calidad (exámenes de competencia o Proficiency test); por sección del laboratorio o estación de trabajo y global del todo el laboratorio.	Permite la evaluación objetiva con una “mirada externa” y comparándose con otros centros internacionales donde se realizan las mismas pruebas con las mismas metodologías / equipamiento.
Registros de mantenimiento correctivo y preventivo del equipamiento de laboratorio	Registro de las horas de mantenimiento correctivo (reparaciones efectuadas sobre cada uno de los equipos) Registro de las horas de mantenimiento preventivo aplicadas sobre cada uno de los equipos utilizados en el laboratorio.	Permite evaluar la eficiencia de cada equipo, predecir desperfectos para prevenirlos, evaluar tendencias hacia desperfectos distintos a los registrados en los manuales del fabricante, anticipar la necesidad de aumentar el mantenimiento preventivo o reemplazar equipamiento
Contaminación de hemocultivos	Registro del porcentaje de hemocultivos contaminados	Permite determinar el cumplimiento estricto de las condiciones de toma de muestra. Su evaluación continua permite aplicar medidas correctivas re-entrenando al personal que efectúa las tomas.

<sup>21</sup> Cuando existe más de un equipo que realiza la misma determinación es necesario demostrar que independientemente del equipo sobre el que se procese la muestra, el resultado será el mismo.

<sup>22</sup> Cuando la cantidad de muestras a procesar es elevada, o cuando el equipo es utilizado por distintas personas en turnos secuenciales, es importante garantizar que el equipo funciona correctamente las 24hs del día y sus resultados son independientes del personal que los opere.

<sup>23</sup> Lecturas microscópicas, interpretación de colores / intensidades, pruebas de aglutinación, lectura de halos en pruebas de susceptibilidad a los antimicrobianos, etc.

**Tabla IV.2. Indicadores de gestión del laboratorio.**

Indicador	Descripción	Aportes TIC
<b>Etapa pos-analítica</b>		
Registro de TAT ( <i>Turn around time</i> )	Registro del tiempo transcurrido entre la obtención de la muestra o su ingreso físico al laboratorio, hasta que el resultado está disponible para el profesional médico para la toma de decisiones. Para los laboratorios que no registren trazabilidad (tracking), se calcula desde la fecha de la petición. Este registro puede considerar el porcentaje de resultados que excedieron el tiempo establecido para cada práctica y para cada tipo de pacientes (ambulatorio, internados, emergencias). Análisis del percentilo 90 de los tiempos de informe para cada estudio	El empleo de las TIC no solo facilita el estudio de este indicador para cada práctica del laboratorio sino que también permite el análisis individual por tipo de paciente, tal como se mencionó, pacientes ambulatorios, de urgencia en la guardia, internados, emergencias.
Respuesta de los auto-verificadores (Auto-validadores de resultados) por interface entre el SIL y los auto-analizadores.	Se registra el porcentaje de resultados auto-validados para cada equipo automatizado conectado al SIL sobre el que se apliquen reglas lógicas de verificación de resultados <sup>24</sup> .	Permite evaluar el correcto funcionamiento de los aplicativos de verificación automática. Permite considerar las lógicas de validación automáticas en el intento de reconfigurar parámetros.
Violación de parámetros de auto-verificación pre-establecidos.	Se registra el porcentaje de veces que un profesional valida un resultado que fue retenido por el aplicativo de auto-verificación.	Permite detectar posible lógicas de validación manual que puedan ser automatizadas.
Eficiencia en la comunicación de los valores críticos.	Registro del porcentaje de valores críticos informados en tiempo y forma. En este registro se considera: i) el tiempo transcurrido hasta la comunicación efectiva de cada valor crítico y ii) la confirmación de la recepción del informe por parte del profesional a cargo del paciente. (read back)	Permite evaluar y controlar uno de los puntos fundamentales en el cuidado del paciente como es la “comunicación efectiva”.

<sup>24</sup> Estas reglas, generalmente con lógicas “booleanas”, definidas por los responsables de cada especialidad del laboratorio, incluyen evaluación de la edad, sexo y otras condiciones fisiológicas, “delta check”, tendencias, rangos de validación, etc.

**Tabla IV.2. Indicadores de gestión del laboratorio.**

Indicador	Descripción	Aportes TIC
Productividad global del laboratorio.	Registro de la cantidad de prácticas informadas por personal involucrado.	Permite evaluar el rendimiento global del laboratorio y sus variaciones según la carga de trabajo, efectos durante las licencias ordinarias y extraordinarias, tasa de ausencias, etc. Permite predecir las necesidades de mano de obra según las variaciones de carga laboral a través del año.
Productividad por sección o estación de trabajo.	Registro de la cantidad de prácticas informadas por el personal involucrado en cada especialidad del laboratorio.	Permite los ajustes finos de lo indicado en el apartado anterior.
Recuperación de hemocultivos positivos.	Registro del porcentaje de hemocultivos positivos por tipo de paciente.	Permite la evaluación de la eficacia del procesamiento de hemocultivos en el sector de microbiología.
Distribución del pH de orinas completas de pacientes ambulatorios.	Registro del pH de orinas completas de pacientes ambulatorios para el estudio de su curva de distribución.	Permite evaluar las condiciones en que llegan las orinas completas al laboratorio y su conservación hasta el procesamiento y tomar acciones correctivas.
Distribución de valores normales de troponina.	Registro y estudio de la curva de distribución de valores normales de troponina.	Asegurar que los valores normales no se encuentran cerca del valor de corte entre normal y patológico.
Valores de medianas por prueba o analito.	Registro de la mediana de las distintas pruebas de laboratorio cuyos resultados se expresan numéricamente. Ejemplo mediana de los valores de colesterol, de glucosa, etc, para pacientes ambulatorios.	Permite la evaluación en tiempo real del funcionamiento de los equipos automáticos.
Modificación de resultados.	Se registra el porcentaje de resultados modificados, sus causas y la comunicación efectiva del cambio; el informe es global del laboratorio y particular de cada área.	Permite detectar fallas en los criterios de validación de resultados o errores en la transcripción de resultados manuales. Expone la necesidad de implementar medidas correctivas / preventivas si es posible o direccionar reentrenamientos al personal.

**Tabla IV.2. Indicadores de gestión del laboratorio.**

Indicador	Descripción	Aportes TIC
Tiempo de transferencia de resultados a la historia clínica electrónica.	Se registra para cada resultado el tiempo de envío a la historia clínica electrónica después de validado por el profesional del laboratorio y el tiempo que ese resultado tarda en ser grabado en la historia clínica electrónica quedando disponible para ser revisado por el profesional a cargo del paciente.	Permite detectar fallas en las interfaces de comunicación entre el SIL y el SIH.
Control de cálculos automáticos.	Se registran los errores encontrados en aquellos resultados en los que se involucra la ejecución de cálculos preestablecidos.	Permite encontrar y resolver errores de cálculos generados por el ingreso de datos erróneos o valores inesperados en las prácticas componentes del cálculo. Ejemplo: Triglicéridos muy elevados que no permiten el cálculo del LDL Colesterol.
Otros indicadores		
Tiempo de caídas del sistema ( <i>downtime</i> )	Se registra el tiempo de caída total y parcial del sistema y su influencia en el informe de resultados de pacientes	Permite tomar medidas correctivas y preventivas sobre el hardware disponible y el servicio de mantenimiento de sistemas.
Registro de no conformidades <sup>25</sup>	Se registra el número global de no conformidades.	Detectar problemas en los procesos.
Encuestas periódicas de satisfacción del usuario interno (profesionales médicos, residentes, etc.)	Se registran las respuestas, se efectúa una evaluación estadística y un auditor externo elabora conclusiones sobre los puntos de vista externos del funcionamiento del laboratorio. Se registran las respuestas, se efectúa una evaluación estadística y un auditor externo elabora conclusiones sobre los puntos de vista externos del funcionamiento del laboratorio.	Permite obtener una visión externa de la eficacia y eficiencia del laboratorio sobre los pacientes, receptores finales del proceso diagnóstico que se realiza en el laboratorio.

<sup>25</sup> No conformidades: incumplimiento de una normativa interna del laboratorio, distintas fallas producidas en los sectores por incumplimiento de lo indicado en los manuales de políticas y procedimientos.

Las TIC ayudan a racionalizar el flujo de trabajo desarrollado en el laboratorio, garantizando un proceso reproducible, de calidad constante y medible, con resultados altamente confiables disponibles en lugar, tiempo y forma.

## Conclusiones

En el comienzo de este capítulo se ha asimilado el proceso diagnóstico de laboratorio a un conjunto de pasos o eslabones unidos en una secuencia o cadena donde la eficiencia de todo el proceso depende de la fortaleza del eslabón más débil (véase Figura 4.1). Pensando en esta imagen, surge claramente que es responsabilidad de los profesionales del laboratorio identificar los puntos críticos (débiles) del proceso y establecer las medidas correctivas y preventivas necesarias para fortalecerlos.

Se ha mencionado en cada apartado cómo las TIC pueden facilitar el proceso diagnóstico de laboratorio para minimizar los impactos negativos sobre la seguridad del paciente.

Es importante rescatar que no existen procesos libres de error [12]. Particularmente en el laboratorio de diagnóstico clínico existen, numerosas oportunidades de error, a veces mencionados como “eventos adversos”. La única forma de evitarlos o minimizarlos es a través del establecimiento de un programa de calidad, que objetivamente establezca la estructura y el funcionamiento global del laboratorio, identificando los puntos críticos de control, los que adecuadamente seleccionados se utilizan para la evaluación del desempeño e implementación de ciclos de mejora continua. Esos puntos críticos se controlan a través de la selección de los denominados indicadores de calidad; parámetros que, monitoreados en forma continua permiten prevenir, detectar y eliminar o por los menos minimizar los eventos adversos que pueden influir sobre la seguridad del paciente.

## Bibliografía

- [1] López Urrutia A. El Laboratorio General: mecanización y gestión. En Escolar Castellón F, Carnicero Giménez de Azcárate J. Informes SEIS: El sistema integrado de información clínica. 1ra ed. Pamplona – España. Sociedad Española de Informática de la Salud, 2004. P. 123-144.
- [2] Joint Commission. National Patient Safety Goals Effective. Hospital Accreditation Program. EEUU, January 1, 2015. Disponible en: [http://www.jointcommission.org/assets/1/6/2015\\_NPSG\\_HAP.pdf](http://www.jointcommission.org/assets/1/6/2015_NPSG_HAP.pdf)
- [3] CAP. Laboratory Accreditation Program. Accreditation Checklists. College of American Pathologists. EEUU, 2015. CLSI. Autoverification of Clinical Laboratory Test Results, Approved Guideline. AUTO 10-A. Clinical and Laboratory Standards Institute (CLSI) Wayne, PA - EEUU, 2006.
- [4] Laboratory General Checklist, College of American Pathologists, 2015.
- [5] Laposata M, Dighe A, “Pre-pre” and “post-post” analytical error: high-incidence patient safety hazards involving the clinical laboratory, 2007 45(6):712-9.
- [6] Plebani M, Sciacovelli L, Aita A, Padoan A, Chiozza ML. Quality Indicators to Detect Pre-analytical Errors in Laboratory Testing. Clinica Chimica Acta 2014 432:44-48.
- [7] Briozzo G, Perego M del C, Der parsehian S. Seguridad del paciente: Contribución del Laboratorio Clínico. Indicadores y propuestas. Bioquímica y Patología Clínica (Argentina) 2008; 72 (2): 19-25.
- [8] Moreno Campoy EE, Mérida de la Torre FJ, Buño Soto A, Caballero Ruiz M, Cuadrado Cenual MA, Fernández Nogueira A et al. Seguridad del paciente. Documento básico, Revisión (2011). Sociedad Española de Bioquímica Clínica y Patología Molecular (SEQC). Comité Científico, Grupo de Trabajo de Seguridad del Paciente
- [9] Atay A, Demir L, Cuhadr S, Gulcan S, Unal H, Aksun S et al. Biochem Med (Zabreb) 2014; 24 (3): 376-382
- [10] Shahangian, Shahrom, Snyder, Susan. Laboratory Medicine Quality Indicators. Clinical Chemistry 2009; 131: 418-431.
- [11] Gil-Setas A, Mazón Ramos A. La gestión de la información del laboratorio de Microbiología clínica. En Escolar Castellón F, Carnicero Giménez de Azcárate J. Informes SEIS: El sistema integrado de información clínica. 1ra ed. Pamplona – España. Sociedad Española de Informática de la Salud, 2004. P. 123-144.
- [12] Aller RD. Management of the Laboratory Information System. En Travers EM, Clinical Laboratory Management. EEUU: Williams & Wilkins Co. 1997, p. 57-75.

## Capítulo V

# El riesgo en el Bloque Quirúrgico: Aportaciones de las TIC

*Carlos Emparán García de Salazar*

### Resumen

•

Junto con las Unidades de Cuidados Intensivos es en el quirófano el lugar donde mayor riesgo de complicaciones puede tener un paciente hospitalizado. Las buenas prácticas en términos de seguridad del paciente requieren una organización para la gestión de la seguridad. Los centros sanitarios deben desarrollar sistemas eficaces para asegurar, a través de la dirección clínica, una asistencia segura y aprender lecciones de su propia práctica y de la de otros.

La introducción de los sistemas de historia clínica electrónica, sistemas de recogida de datos intraoperatorios, o de imágenes digitalizadas de la intervención quirúrgica nos abre un campo de mejora en la seguridad del paciente que se puede enfocar en cuatro puntos: Primero, el uso de TIC y sistemas de HCE en el propio quirófano. Segundo, en el control y estandarización de procesos perioperatorios, desde la consulta hasta el alta del paciente. Tercero, el uso de archivos digitalizados quirúrgicos que sirvan de “cajas negras” quirúrgicas. Y cuarto, la creación de modelos de trabajo que, aunque estén basados en los ordenadores tradicionales, evolucionen a equipos portátiles de todo tipo en los que

se puedan integrar flujos de proceso clínico, gestión de alertas de riesgo, introducción de algoritmos de riesgo quirúrgico, y sistemas de volcado de datos a grandes bases de datos en los que se puedan realizar grandes análisis multivariantes desde procedimientos quirúrgicos comunes hasta procedimientos muy especializados o infrecuentes.

## Organización del Bloque Quirúrgico

El Bloque Quirúrgico (BQ) es, por una parte, el espacio donde se agrupa a todos los quirófanos con las diferentes características y equipamientos necesarios para llevar a cabo todos los procedimientos quirúrgicos previstos, y por otra una unidad organizativa, es decir, una organización de profesionales sanitarios, que ofrece asistencia multidisciplinaria a procesos asistenciales mediante cirugía, en un espacio funcional específico donde se agrupan los quirófanos con los apoyos e instalaciones necesarios, y que cumple unos requisitos funcionales, estructurales y organizativos, de forma que garantiza las condiciones adecuadas de seguridad, calidad y eficiencia, para realizar esta actividad.

El BQ funciona como una unidad intermedia, que presta servicio especialmente a los servicios quirúrgicos finales, que son sus clientes principales. Las unidades de Cirugía Mayor Ambulatoria, sin embargo, funcionan como unidades finales, pues dan directamente de alta a los pacientes atendidos en ellas. Pueden ser clientes del BQ las siguientes unidades enumeradas en la Tabla V.1.

Cirugía pediátrica	Angiología y Cirugía Vasculare	Cirugía general y digestivo	Cirugía maxilofacial
Ginecología	Cirugía cardíaca	Cirugía ortopédica y traumatología	Cirugía plástica y reparadora
Obstetricia	Cirugía torácica	Urología	Cirugía estética
Cirugía de Urgencias	Neurocirugía	Oftalmología y Cirugía refractiva	Otorrinolaringología

Ocasionalmente también puede prestar servicio a otras unidades finales como, por ejemplo las descritas en la Tabla V.2.

Cardiología	Dermatología	Obtención de tejidos	Extracción de órganos
Unidad de Fecundación	Unidad del dolor	Trasplante de tejidos	Trasplante de órganos
Endoscopias Digestivas	Radiología intervencionista		

A su vez, el BQ es cliente de numerosas unidades estructurales e intermedias del centro sanitario, estén o no externalizadas, como son las indicadas en la Tabla V.3.

Almacén	Dermatología	Esterilización	Gestión de pacientes
Gestión de residuos	Banco de sangre/tejidos	Limpieza	Medicina preventiva
Lavandería y lencería	Diagnóstico por la imagen	Seguridad	Farmacia
Mantenimiento	Laboratorios	Informática	

### Estructura del BQ

Como se ha mencionado, por BQ se entiende el espacio donde se agrupa a todos los quirófanos con las diferentes características y equipamientos necesarios para llevar a cabo todos los procedimientos quirúrgicos previstos, y por otra unidad organizativa.

Se recomienda que, si las condiciones estructurales, de volumen de actividad y de organización y gestión (incluyendo la gestión de personal) del centro lo permiten, se diferencie el BQ de la unidad de CMA (unidades de CMA autónomas).

### Gestión del BQ

El BQ es una unidad de gestión intermedia que provee servicios (el procedimiento quirúrgico) a los servicios finales, generalmente las especialidades quirúrgicas. En función de las necesidades derivadas del proceso de atención en el BQ, se recomienda la siguiente organización:

- Coordinador/a médico del BQ.
- Supervisor/a de enfermería del BQ.
- Comité de quirófano.

#### *Coordinador médico del BQ*

El papel del coordinador médico del BQ es de dirección y planificación. Debe servir de referencia y árbitro a los profesionales que desarrollan su trabajo en el BQ (anestesiólogos, cirujanos, enfermeras, auxiliares, técnicos, etc.) y al mismo tiempo de conexión entre estos y la dirección del centro.

#### *Supervisión de enfermería del BQ*

La supervisión de enfermería del BQ habitualmente es la responsable de la operativa del BQ. Esto no solo representa el personal de enfermería, personal auxiliar y técnico que trabaja en los quirófanos, sino que su responsabilidad en la operativa obliga a disponer con amplia capacidad ejecutiva para asignar y distribuir la cirugía programada en los quirófanos oportunos.

### Comité de quirófano

El comité de quirófano debe ser responsable de la planificación estratégica, monitorización y gestión del rendimiento de los quirófanos. Su composición es plural y esto significa que además de los responsables de planificación y de la operativa (coordinador y supervisión respectivamente) debe estar presente un responsable de la unidad de admisión de pacientes y los representantes de las distintas especialidades quirúrgicas.

El comité de quirófano es responsable de que las políticas de planificación, monitorización y gestión del BQ sean acordadas, implementadas y actualizadas. La Modernisation Agency recomienda la implantación de las siguientes políticas para el BQ (véase Tabla V.4).

<b>Tabla V.4. Políticas de planificación, monitorización y gestión del BQ.</b>	
Normas para la confección de los partes quirúrgicos	Procedimientos para elaborar los partes de quirófano.
	Procedimientos para comunicar los partes quirúrgicos a los quirófanos y salas.
	Tiempo límite para recibir los partes de quirófano en quirófanos y salas.
Normas de control de los partes quirúrgicos	Procedimientos para comunicar a las personas relevantes cambios en los partes de quirófano.
	Programación de la hora de comienzo y finalización de las sesiones quirúrgicas.
	Programación de la hora de comienzo y finalización de las sesiones quirúrgicas.
	Normas para la cancelación y reasignación de sesiones quirúrgicas:
Procedimiento para reasignación de sesiones	Nombramiento del responsable (por ej.: coordinador de quirófano) de reasignar las sesiones canceladas.
	Nombramiento del responsable de distribuir la información sobre sesiones canceladas.
Normas para el manejo de la cirugía traumatológica semielectiva y urgente	Deben incluir un protocolo específico para las operaciones semielectivas y urgentes a partir de las 21:00, y otro para las operaciones antes de las 21:00 horas.
Normas para los casos de cirugía electiva	Necesidades específicas del procedimiento (instrumental, personal, ubicación, tiempo necesario) y procedimiento de comunicación con el BQ.

### *Manual de organización y funcionamiento*

El BQ deberá disponer de un manual de organización y funcionamiento en el que se refleje:

- a. El organigrama de la unidad.
- b. La cartera de servicios.
- c. La disposición física de la unidad y los recursos estructurales y de equipamiento de que dispone.
- d. El manual de normas de organización y funcionamiento:

El manual debe contener una delimitación de su ámbito de aplicación, debe definir el personal al que va destinado y finalmente el horario de su aplicación. En el mismo se definirán los circuitos de circulación de los pacientes, del personal y de los equipamientos en función del diseño del BQ en que se aplique.

### *Gestión de pacientes*

#### *Admisión*

Aunque está integrada en todo el centro, las actividades y funciones de admisión deberán ser desarrolladas, de forma idónea, por la unidad del BQ.

#### *Documentación e historia clínica*

La documentación clínica está integrada por el conjunto de documentos resultantes del proceso asistencial, cualesquiera que sean su formato y soporte.

#### *Historia clínica*

La historia clínica deberá ser única para cada paciente y deberá ser compartida entre profesionales, centros y niveles asistenciales. Asimismo, deberá cumplir las exigencias técnicas de compatibilidad que cada servicio de salud establezca.

La información asistencial recogida en la historia clínica podrá constar en soporte papel o a través de medios informáticos, electrónicos o telemáticos, siempre que garantice su recuperación y uso en su totalidad.

En lo relativo al diseño, contenido mínimo, requisitos y garantías y usos de la HCE se atenderá a lo previsto en la Ley 41/2002 básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica. En su caso deberá figurar el documento de Instrucciones Previas.

### Hoja circulante / Hoja de ruta quirúrgica (HC/HRQ)

La HC/HRQ es el documento que caracteriza al BQ. Su soporte puede ser electrónico o papel y se diseña para circular por todo el proceso quirúrgico desde la llegada del paciente al BQ hasta la finalización del proceso quirúrgico en la URPA, sin perjuicio de establecer otro criterio más restrictivo o expansivo y de otros documentos más específicos de los distintos servicios quirúrgicos. La HC/HRQ establece aquellos pasos imprescindibles para asegurar la calidad del proceso quirúrgico y en cada situación con la firma de la persona responsable. En distintos espacios bien delimitados se exponen de forma clara y ordenada los siguientes datos (véase Tabla V.5):

<b>Tabla V.5. Datos que debe incluir la HC/HRQ.</b>			
Datos administrativos	Fecha prevista de intervención.	Diagnóstico.	Procedimiento/s previsto/s.
Nivel de complejidad anestésica	Medicación habitual (especial mención anticoagulantes, etc.).	Tipos de anestesia prevista.	Alergias conocidas. Previsión de transfusión.
Check-List Quirúrgico	Disponibilidad de instrumentación específica.	Señalización del miembro afectado.	Recuento de gasas realizado.
Protocolos perioperatorios	Recordatorio de ayunas tiempo antes de la intervención.	Monitorización perioperatoria	Criterios de alta.

## Informe de alta

Al final del proceso asistencial, así como con ocasión de traslado, el paciente tiene derecho a la expedición por el centro del informe de alta médica a que se refiere la Ley 41/2002, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica.

## Protección de datos sanitarios

Los datos de carácter personal relativos a la salud del paciente tienen la consideración de datos especialmente protegidos a los efectos previstos en Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal LOPD.

## Control de tiempos quirúrgicos

Un problema que habitualmente se encuentra al analizar los datos de funcionamiento de los quirófanos es que los profesionales que trabajan en ellos no aceptan los resultados por no estar de acuerdo con el modo en que se han recogido o se han analizado los datos. Los hospitales disponen, en general, de datos suficientes aunque dispersos. En este sentido, se aconseja una postura pragmática: un número reducido de datos relevantes recogidos de forma automática es mejor que contar con muchos datos obtenidos de forma manual o que realizar un esfuerzo titánico para tener acceso a muchos datos a través del diseño de un sistema informático ad hoc.

## Indicadores de rendimiento

Para conseguir un buen rendimiento de los quirófanos es importante que el primer caso del día comience a la hora prevista, que el tiempo entre caso y caso sea mínimo, que la tasa de cancelaciones sea baja, que los errores de programación sean escasos y la programación esté bien ajustada. Para conseguirlo se deben registrar los retrasos sobre la programación prevista y sus causas, las suspensiones de cirugías y sus causas y los desajustes entre la duración prevista de los procedimientos y la real. Estos datos deben resumirse y presentarse de modo que sea factible interpretarlos y deducir conclusiones, además de permitir un seguimiento de la actividad por todos los interesados.

## Sistema de información

El sistema de información estará integrado en el sistema general del hospital, debiendo atender a los distintos requerimientos del BQ. Todo el sistema de información debería ser accesible en formato digital, por medio de la HCE en todas sus vertientes:

- Gestión de pacientes:
  - Filiación.
  - Citación.
  - Admisión.
  - Alta y codificación.
- Gestión de la documentación clínica.
  - Estación clínica:
  - Historia clínica electrónica.
- Gestión de quirófanos.
  - Aplicaciones departamentales (laboratorio, diagnóstico por la imagen...).
- Gestión económico-administrativa y de servicios generales:
  - Almacén (pactos de consumo, gestión de stocks, solicitudes de compra, etc.).
  - Farmacia (sistema de prescripción electrónica, unidosis, sistema de conciliación de medicación).
  - Laboratorio de Hematología en la gestión del banco de sangre.
  - Contabilidad.
  - Esterilización.
- Gestión de personal (incapacidad transitoria, incidencias, permisos, sustituciones, etc.).
  - Evaluación (cuadro de mando):
  - Costes por proceso (contabilidad analítica).
  - Encuestas de satisfacción.
  - Indicadores de actividad.
  - Indicadores de calidad.
  - Indicadores de rendimiento.

## Aspectos esenciales de la seguridad en el paciente quirúrgico

Este capítulo está dedicado a aquellos criterios y orientaciones referidos a la seguridad del paciente durante su asistencia en el BQ. La OMS ha desarrollado un manual para la implantación del listado

de comprobación de la seguridad en cirugía (Surgical Safety Checklist) (véase Tabla V.6).

Tabla V.6. Lista de verificación de la seguridad de la cirugía (1° ed.). Organización Mundial de la Salud.		
Antes de la inducción de la anestesia	Antes de la incisión cutánea	Antes de que el paciente salga del quirófano
ENTRADA	PAUSA QUIRÚRGICA	SALIDA
<input type="checkbox"/> El paciente ha confirmado: <ul style="list-style-type: none"> <li>• Su identidad</li> <li>• El sitio quirúrgico</li> <li>• El procedimiento</li> <li>• Su consentimiento</li> </ul> <input type="checkbox"/> Demarcación del sitio / No procede	<input type="checkbox"/> Confirmar que todos los miembros del equipo se hayan presentado por su nombre y función <input type="checkbox"/> Cirujano, anestesista y enfermero confirman verbalmente: La identidad del paciente El sitio quirúrgico El procedimiento	El enfermero confirma verbalmente con el equipo: <input type="checkbox"/> El nombre del procedimiento realizado <input type="checkbox"/> Que los recuentos de instrumentos, gases y agujas son correctos (O no proceden) <input type="checkbox"/> El etiquetado de las muestras (Que figure el nombre del paciente) <input type="checkbox"/> Si hay problemas que resolver relacionados con el instrumental y los equipos
<input type="checkbox"/> Se ha completado el control de la seguridad de la anestesia <input type="checkbox"/> Pulsioxímetro colocado y en funcionamiento	Previsión de eventos críticos <input type="checkbox"/> El cirujano revisa: Los pasos críticos o imprevistos, la duración de la operación y la pérdida de sangre prevista <input type="checkbox"/> El equipo de anestesia revisa: Si el paciente presenta algún problema específico <input type="checkbox"/> El equipo de enfermería revisa: Si se ha confirmado la esterilidad (con resultados de los indicadores) y si existen dudas o problemas relacionados con el instrumental y los equipos	
¿Tiene el paciente: Alergias conocidas? <input type="checkbox"/> No <input type="checkbox"/> Sí Vía aérea difícil / Riesgo de aspiración? <input type="checkbox"/> No <input type="checkbox"/> Sí, y hay instrumental y equipos / ayuda disponible Riesgo de hemorragia > 500 ml (7 ml/kg en niños)? <input type="checkbox"/> No <input type="checkbox"/> Sí, y se ha previsto la disponibilidad de acceso intravenoso y líquidos adecuados	<input type="checkbox"/> Se ha administrado profilaxis antibiótica en los últimos 60 minutos? <input type="checkbox"/> Sí <input type="checkbox"/> No procede <input type="checkbox"/> Pueden visualizarse las imágenes diagnósticas esenciales? <input type="checkbox"/> Sí <input type="checkbox"/> No procede	<input type="checkbox"/> El cirujano, el anestesista y el enfermero revisan los principales aspectos de la recuperación y el tratamiento del paciente
<p><i>La presente lista no pretende ser exhaustiva. Se recomienda completarla o modificarla para adaptarla a la práctica local.</i></p>		

### Proceso de comunicación en el quirófano

Una comunicación eficaz en toda la organización es un elemento relevante para garantizar la seguridad en el quirófano. La cultura organizativa debe hacer énfasis en el trabajo en equipo sustituyendo la relación jerárquica por la del liderazgo.

Prevención de errores de localización de sitio quirúrgico, medicación y prevención de retención de cuerpos extraños

Las posibilidades de cometer errores en la localización del área quirúrgica, en el tipo de procedimiento o en la identificación del paciente, son mayores cuando la comunicación entre los miembros del equipo es inadecuada o ineficiente, cuando el paciente no participa en la señalización del área, y por la falta de procedimientos de verificación del lugar. Algunos factores de riesgo incluyen los siguientes (véase Tabla V.7):

Inadecuada evaluación del paciente.	Una cultura que no facilite la comunicación abierta entre los miembros del equipo quirúrgico y favorece la idea de que el facultativo siempre tiene la razón y no es cuestionado.	Más de un cirujano involucrado en el caso, tanto porque se practiquen múltiples procedimientos como porque el caso sea transferido a otro cirujano.
Inadecuada revisión de la historia clínica.	Problemas relacionados con escritura ilegible.	Presión por el tiempo (duración de la sesión; cirugía de emergencia).
Exclusión de algunos de los miembros del equipo quirúrgico del proceso de verificación.	Utilización de abreviaturas relacionadas con el tipo de cirugía, lugar o lateralidad.	Alteración del orden quirúrgico establecido
Comienzo del procedimiento anestésico antes de la verificación por parte del cirujano de paciente y cirugía planificada.	Características no habituales en el paciente, tales como grandes deformidades u obesidad.	



aparecen unidos en el BQ: el protocolo quirúrgico, habitualmente de tipo “libre” o dictado, las constantes vitales, los protocolos anestésicos, las imágenes radiológicas, y endoscópicas, el inventario quirúrgico o las peticiones de farmacia y de banco de sangre.

1. Las especialidades quirúrgicas son un reto en general. Históricamente los cirujanos han utilizado el dictado en la redacción de sus informes (protocolos quirúrgicos, interconsultas o altas) los beneficios más evidentes de los programas de historia clínica (formato de documentación, integración de imágenes) les obligan a cambiar una posición de comodidad importante frente al cambio que implica la HCE. Además, los protocolos quirúrgicos no se caracterizan por presentar grandes cantidades de datos estructurados para introducir en la HCE. Así mismo no tienen una alta proporción de pacientes recurrentes (menos del 5% de pacientes deberían requerir una reintervención o reingreso) por lo que una gran parte de los registros son “nuevos” registros. El área en la que los especialistas quirúrgicos pueden apreciar más fácilmente los beneficios de la HCE sería la interoperabilidad (utilizar distintas herramientas dentro de la HCE... imágenes radiológicas, endoscópicas, del quirófano, dentro de los documentos de gestión de quirófano como el protocolo quirúrgico) que necesita tiempo para lograrse. Un porcentaje importante de la información que se necesita en el BQ para la documentación proviene de notas operativas de pruebas invasivas del propio hospital, referencias o información recogida en las consultas. Todas ellas componen el elemento más importante de flujo de trabajo, y, en general, se basan en los resultados de laboratorio y pruebas de imagen electrónica.
2. A la hora de introducir una nueva programación de protocolos quirúrgicos que sean considerados eficaces por los cirujanos, el enfoque más acertado es el cambio de flujo de trabajo. Este modelo requiere un cambio más en los niveles de responsabilidad a la hora de introducir aquellos datos de niveles intermedios habitualmente estructurados (como los signos vitales, la historia, etc.) y conectarlos con la entrada de elementos del tipo de facturación de gastos. Estos dos grupos de datos (signos vitales o codificación de procedimientos) no suelen ser introducidos por los equipos quirúrgicos (los introducen el personal de enfermería o codificadores) que son “lobos solitarios” tradicionalmente muy resistentes a hacer ese tipo de documentación. La solución más adecuada es importar

- ese tipo de datos bien de los elementos del hardware o de bases de datos “inteligentes” generadas previamente por los servicios de codificación.
3. Dentro de las mejoras del BQ el poder utilizar software de dictado que pueda introducir elementos abiertos en plantillas de procedimientos estructurados permitirá mejorar la flexibilidad necesaria para recoger fidedignamente determinados tipos de procedimientos difícilmente estructurables en macros.
  4. Algunas HCE incluyen elementos de software que importa elementos descriptivos sobre los que puede añadirse elementos visuales (fotografías o videos) con los comentarios o edición gráfica de los cirujanos, lo que añade un verdadero valor añadido a la documentación electrónica.
  5. La interoperabilidad debe aplicarse en el software tan pronto como sea posible: la entrega de los resultados de pruebas de diagnóstico (especialmente imágenes y resultados de pruebas radiológicas o endoscópicas) y la documentación estructural del flujo de trabajo del hospital (notas operativas, informes de alta) deben integrarse en el flujo de trabajo durante la ejecución del procedimiento.
  6. El reconocimiento de voz con software específico crea un beneficio inmediato de los ahorros en los costos de dictado, mejorando la adopción de HCE.

#### Protocolos de instrumental y necesidades por procesos quirúrgicos

En los últimos años se han introducido en los BQ los denominados Packs de Procedimiento que contienen los dispositivos de un solo uso que se requieren para llevar a cabo un determinado y definido procedimiento quirúrgico. Todos estos productos están envasados de forma estéril y se entregan “ad hoc” en un solo paquete estéril, según las instrucciones especificadas por los componentes del equipo quirúrgico. Habitualmente las industrias de dispositivos o instrumental quirúrgico trabajan en estrecha colaboración con los equipos quirúrgicos en el diseño de adquisición y entrega de los paquetes estériles de una manera efectiva oportuna, eficiente y rentable. Este tipo de paquetes pueden ir desde hisopos quirúrgicos, suturas, bisturís y apósitos de heridas, a los catéteres cardíacos e implantes. El NHS británico estableció que la mayor parte de los procedimientos ambulatorios quirúrgicos (aproximadamente un 75%) podría llevarse a cabo con este tipo de cobertura de necesidades.

Uno de los aspectos fundamentales de este tipo de paquetes es su costo

1. Los Paquetes de procedimientos pueden generar un ahorro de costes al permitir un uso más racional de los elementos necesarios para las cirugías, empleando sistemáticas de “Just in Time” vinculadas a una adecuada programación quirúrgica.
2. Los Paquetes de procedimientos permiten a los hospitales reducir la cantidad de existencias (stock) de material quirúrgico necesarias para llevar un procedimiento en un momento dado y reducir el riesgo de caducidad de los productos que se consumen menos habitualmente. El uso de paquetes permite además a los administradores identificar más fácilmente el costo total del procedimiento, reduce la carga administrativa y los costes de gestión al disminuir la cantidad de tiempo necesario en el seguimiento y ordenar el inventario.

¿Cómo se puede integrar este tipo de estructura de trabajo en los modelos TIC del BQ? Es sencillo, colocando lectores ópticos de código de barras en cada quirófano por medio de los cuales se realice un inventario en tiempo real, y vinculado a la Historia Clínica, de los elementos utilizados en cada intervención quirúrgica. La integración de software tanto de las casas comerciales como de los propios centros hospitalarios, permite conocer el número de procedimientos (y las necesidades de instrumental o fungibles necesarios) y los costes asociados al mismo prácticamente en tiempo real. Asimismo, en lugar de necesitar grandes espacios de almacenamiento el BQ pasa a ser manejado como un centro de “punto-pedido” que vincula a la casa proveedora con el quirófano en pedidos “Just-In-time” vinculados a filosofías empresariales de tipo Lean. La reducción de costes en el BQ debido a la reducción física del almacén, al coste de su stock y a la reducción de personal administrativo es enorme y justifica la adopción de este tipo de medidas.

### Digitalización de procedimientos quirúrgicos

La digitalización de procedimientos quirúrgicos abiertos, endoscópicos o laparoscópicos, la recogida de imágenes en momentos críticos como pueden ser las situaciones del “safety view” y el análisis de situaciones de eventos adversos recogidos intraoperatoriamente en sistemas PACS son una parte fundamental del proceso de implantación de las TIC en el BQ

En el entorno quirúrgico de hoy, las razones para grabar imágenes y vídeo son amplias y variadas. Mientras que muchas instalaciones ven un valor en la capacidad de documentar la totalidad o parte de un procedimiento quirúrgico para su uso posterior, no hay normas establecidas que requieren documentación de cualquier procedimiento quirúrgico. El hecho de que la mayoría de procedimientos endoscopios o laparoscópicos son visualizados en HD y con interfaces “sencillos” para volcar las imágenes o secuencias de video a sistemas de recogida de imágenes hace que la accesibilidad y disponibilidad de los mismos pueda ser aún más compleja que la de los sistemas PACS.

En este momento el crecimiento de grabación digital ha traído muchas nuevas capacidades al BQ, incluyendo:

- Mejora de la calidad de la imagen.
- La velocidad y la flexibilidad en la edición.
- Compatibilidad con una amplia variedad de señales de la cámara.
- La capacidad de utilizar los medios digitales portátiles, como unidades USB.
- La capacidad para transmitir vídeo a redes hospitalarias.

La práctica de la transmisión de cirugías es una tendencia cada vez mayor especialmente en los hospitales académicos donde el video se puede transmitir a una sala de conferencias o en otra área del hospital donde la gente puede observar el procedimiento. Con el entorno informático adecuado, puede incluso transmitirse “en vivo” a cualquier IP del mundo.

Hoy en día, la mayor cantidad de los bloques quirúrgicos han hecho la transición a la alta definición (HD) sistemas de cámaras, con lo que la posibilidad de grabar imágenes en alta definición y video en el quirófano ha crecido, al igual que la necesidad de instalaciones para tener una solución de archivo para el almacenamiento de estos datos de tamaños muy considerables.

Otra pregunta que queda por responder es la aparición de un formato de archivo estándar entre los sistemas de captura disponibles en el mercado hoy. Esto es otra pieza del “entorno de frontera salvaje” que tiende a diferir de un centro a otro. En radiología, DICOM ha surgido como un estándar para la formación de imágenes de radiología. La mayoría de los sistemas en el lado de radiología pueden comunicarse con los dispositivos de formación de imágenes digitales utilizando el

estándar DICOM, y esos dispositivos son generalmente compatibles entre sí. En los próximos años las soluciones de endoscopia tendrán que adoptar en el ámbito quirúrgico, el modelo DICOM, que permite la comunicación entre los sistemas ayudando a mejorar el flujo de trabajo y, en definitiva, la atención al paciente.

## El papel de las TIC en el control y estandarización de procesos perioperatorios

### Integración de guías y vías clínicas en la Historia Clínica Electrónica

Hay pocos estudios científicos publicados sobre cómo los sistemas de HCE afectan la eficiencia clínica global y la agilidad en el proceso de documentación. La mayoría de los estudios se refieren a entornos de equipos médicos, radiológicos, difíciles de adaptar al entramado del BQ. Además, los pocos estudios realizados lo han hecho en entornos de CMA y no se pueden extrapolar a otros ámbitos como el BQ integrado con Unidades de Cuidados Intensivos. En particular, los sistemas de HCE o de gestión de almacén de quirófanos, son utilizados por los entornos de HCE en el hospital para integrar la documentación de enfermería quirúrgica y anestesia, (protocolos quirúrgicos, hojas de anestesia, hojas de instrumentación), gestión de materiales quirúrgicos, y la programación quirúrgica a corto, medio o largo plazo. La documentación, análisis y gestión de los procedimientos quirúrgicos, integrándolos en programas de gestión son tareas críticas que se han asociado con la calidad, el costo y la eficiencia de cuidados del área quirúrgica. Además, los procedimientos de quirófano y sus estancias asociadas pueden llegar a suponer hasta un 47% de los costos de los hospitales.

Por tanto, dentro de los retos de integración de la HCE se encuentra el evaluar los efectos de la implementación de los sistemas de información del BQ en torno a modelos de gestión de los tiempos quirúrgicos, la documentación de enfermería, el volumen quirúrgico, las necesidades de personal y salas de operaciones, o el tiempo de rotación entre procedimientos.

Este proceso no está exento de complicaciones. El primer problema que se encuentra en la implantación de HCE en el BQ es que el tiempo total empleado en la documentación intraoperatoria

empeora considerablemente después de la implementación de la HCE. El porcentaje de tiempo requerido para documentar los procedimientos a todos los niveles (gestión de materiales, hojas de circulante, protocolos quirúrgicos o introducción de tratamientos) se incrementa especialmente en procedimientos relativamente cortos como pueden ser los oftalmológicos o urológicos, no siendo significativos en grandes cirugías digestivas u oncológicas.

El empeoramiento en el tiempo la documentación después de la implementación de HCE se puede atribuir principalmente a varios factores. En primer lugar, el tipo de documentación usado y el hacer clic puntuales en interfaces de HCE puede ser más lento que los formularios en papel que han sido optimizados durante muchos años. Por ejemplo, en cualquier procedimiento documental quirúrgico se requiere que los usuarios naveguen en una o varias casillas de verificación para° seleccionar la vía de administración de medicamentos (por ejemplo intraocular vs. tópico), el lugar de la administración (por ejemplo, el ojo izquierdo), y el nombre de la prescripción del cirujano o la enfermera que lo dispensa para cada medicamento. En general, se admite que el tiempo de documentación de procedimientos menores o de CMA es más lento con la HCE que con formularios de papel.

Segundo, el volumen global de documentación requerida por el sistema de HCE es mayor que con el sistema previo de papel. Las bases de introducción de datos en protocolos quirúrgicos incluyen campos obligatorios (que no existían en los protocolos “escritos”), seleccionar elementos introducidos por las guías de práctica clínica de los centros, o indicar variaciones del procedimiento estándar que no era necesario documentar en el documento escrito antiguo. Este incremento en la información introducida redundante a medio plazo en los análisis de seguridad de los procedimientos, al permitir un análisis estructurado y sistematizado de los mismos. En general, se aprecia que el tiempo empleado en la redacción del documento y las variaciones de “estilo” en la elaboración de protocolos quirúrgicos disminuye con el tiempo.

Análisis de eventos adversos basado en la recogida de datos de la HCE agrupada por procesos

A medida que la necesidad de ensayar y practicar cualquier procedimiento quirúrgico con simuladores de pacientes, entornos de realidad virtual y pacientes estandarizados, sigue creciendo para los

cirujanos y el personal, la capacidad de documentar de forma extensa y con edición de imágenes y video es una herramienta muy valiosa. El reto no sólo es la captura de toda la información en alta definición (HD) en la HCE, sino además proporcionar las herramientas para que se pueda acceder a la información al instante y con un acceso cómodo. La capacidad para analizar e identificar las áreas de mejora en un procedimiento quirúrgico o en un proceso del BQ es una de las herramientas más poderosas en la prevención de errores que pueden ocurrir durante la atención al paciente real.

Los sistemas de integración documental optimizan la logística de integración del formato vídeo, la salida de equipamientos médicos, el audio y los datos de cualquier monitor implicado para que se pueda acceder desde cualquier lugar en el hospital en un momento posterior. El procedimiento es similar al de una caja negra, en la que es tan importante recoger los datos operativos, como la situación (tanto en audio como en video) que surge en todos los niveles de comunicación de los equipos quirúrgicos. Algunos hospitales han empezado a tomar nota de este tipo de capacidades operativas y han empezado a utilizar esta tecnología en entornos de documentación “live-paciente”. Esta integración documental permite registrar cómo trabajan los equipos en entornos difíciles y de alto estrés y luego realizar sesiones clínicas juntos o de forma remota, como parte de un proceso voluntario de auto-mejora. No obstante muchos centros no ven una mejora de este tipo de conceptos añadidos porque, desde un punto de vista legal, este tipo de registros “podrían volverse en contra del propio centro”. En realidad, se trata de hacer oídos sordos a las mejoras “naturales” que ha hecho el sector aeronáutico con sus cajas negras, y vendrán impuestas por elementos regulatorios de naturaleza superior. Evidentemente únicamente el registro de un evento adverso permite su posterior análisis y control.

Teniendo en cuenta los entornos digitales de los quirófanos hay una serie de consideraciones clave en la compra de nuevos equipos para satisfacer las necesidades de documentación dentro del BQ:

1. HD. Independientemente de si la instalación cuenta con sistemas de cámaras de alta definición de hoy, los bloques quirúrgicos deberían estar comprando sistemas de captura compatibles HD.
2. La capacidad para grabar múltiples entradas de datos de imágenes al mismo tiempo. Por ejemplo, los cirujanos pueden querer grabar

- el vídeo del endoscopio, la cámara de televisión de las luces de quirófano o del entorno del quirófano (la cámara sobre la mesa de quirófano, integrada en las luces de quirófano), y, en función del procedimiento, la entrada de otro tipo de imágenes como la fluoroscopia o el ecógrafo al mismo tiempo que se permita la grabación de los signos vitales de los pacientes desde el sistema de monitorización anestésico. Por lo tanto, el sistema de captura de imágenes digitales debe poder manejar más de una entrada.
3. Tecnología de vídeo en tiempo real. El sistema debe tener la capacidad de transmitir vídeo de forma simultánea, mientras se está grabando el procedimiento. Esto permite la transmisión de la cirugía para un público más amplio sobre la red hospitalaria o en entorno web.
  4. El sistema debe tener la capacidad de poder almacenar la información de forma casi inmediata al finalizar un caso, de forma que se pueda grabar el siguiente casi de forma inmediata. Algunos sistemas, hoy en día, al finalizar el caso, requieren una cierta cantidad de tiempo para grabar el procedimiento en un CD o para ubicar el archivo vinculado a la cirugía a un servidor de la red. Hay múltiples opciones, como por ejemplo, un dispositivo de captura que grave y borre de forma simultánea el procedimiento previo o transmite el caso a la red de forma simultánea, por lo que al final del caso, uno puede simplemente expulsar el disco y estar listo para la siguiente grabación.
  5. Desde el punto de vista estructural se aconseja también buscar la facilidad de acceso y ancho de banda, así como la capacidad de acceder a los procedimientos desde cualquier dirección IP (PC, tablet o móvil) del hospital sin forzar la infraestructura hospitalaria existente. Por ello, es fundamental para la adopción, y facilitar el uso y revisión de este tipo de tecnología en determinadas cirugías, desarrollar procesos de formación del personal. Al documentar sus procedimientos, los hospitales pueden identificar sus debilidades, identificando los puntos donde pueden estar fallando y luego construir un plan de estudios en torno a adoptar las mejores prácticas.

Sistemas de alerta perioperatoria y agrupación de pacientes de riesgo por procesos quirúrgicos

sobre tratamientos y servicios de documentación electrónica recomendó:

1. Disponer de un proceso que permita reconocer y responder tan pronto como la condición de un paciente parezca estar empeorando;
2. Desarrollar criterios escritos o integrados en la documentación o registros electrónicos que describan señales de advertencia de un cambio o deterioro de la condición del paciente y cuándo puede ser necesario solicitar ayuda;
3. Indicar mediante notificaciones claras al personal que debe buscar ayuda adicional cuando se alcanzan determinados parámetros objetivos acerca de la condición del paciente.

Este tipo de medidas quedan integradas en los modelos o sistemas del tipo EarlySense que está diseñado específicamente para abordar la atención al paciente, la seguridad y los problemas de calidad de las unidades perioperatorias. Las unidades de este tipo de sistemas y de la estación central de visualización (localizada en los controles de enfermería) permiten el control continuo de pacientes en los que no es posible una observación continua. El sistema transfiere alertas directamente al ordenador o a la sala de enfermería. La instalación de este tipo de sistemas es rápida y flexible y suele utilizar modelos de pantalla táctil muy fácil de usar. Toda la monitorización se puede realizar sin contacto directo entre el paciente y el dispositivo, utilizando un sensor colocado bajo el colchón. Este tipo de sistemas (que ya llevan integrados determinados teléfonos móviles) producen una baja tasa de falsas alarmas, y se suele comparar favorablemente con los dispositivos estándar, como la pulsioximetría o la monitorización electrocardiográfica continua (telemetría).

Los sistemas de alerta de monitorización de pacientes agudos y sub-agudos deben hacer crecientes énfasis en:

1. La detección temprana del deterioro de la condición del paciente y
2. La intervención urgente una vez que se detecta un problema.
3. Los nuevos conceptos de monitorización pueden adaptarse con éxito a las áreas no-UCI (URPA, zonas de CMA, plantas quirúrgicas) con una mínima interferencia de los flujos de trabajo existentes, el uso de tecnologías sin contacto y algoritmos especiales que minimizan las alertas.
4. Al proporcionar una alerta temprana de cambios en la condición de un paciente, el intervalo entre la aparición de deterioro del paciente y detección / acción por los médicos de la unidad médico-quirúrgica se reduce.

5. Este tipo de tecnología también tiene el efecto neto de la “modernización”, camas médico-quirúrgicas a un nivel superior de atención, ofreciendo una alternativa a la telemetría para aquellos pacientes que necesitan algo más que la atención médico-quirúrgica estándar, pero no requieren monitorización electrocardiográfica continua.

Los sistemas de alerta perioperatoria e identificación de pacientes de riesgo permiten optimizar el uso de unidades de costos diferenciados (Intensivos, cuidados intermedios, unidades de recuperación post-anestésica, plantas convencionales y unidades de CMA) asignando una ubicación, con sus cuidados personalizados a las necesidades del paciente quirúrgico.

## Bibliografía

- [1] Quintanas A., Gómez-Arnau J., González A. El bloque quirúrgico. En Ruiz P, Alcalde, J., Landa, J.I. Gestión Clínica en Cirugía. Sociedad Española de Cirujanos. Arán: Madrid. 2005, págs. 199-214.
- [2] JC. Hospital Accreditation Standards (HAS). Patient Safety Systems, accesible en [http://www.jointcommission.org/patient\\_safety\\_systems\\_chapter\\_for\\_the\\_hospital\\_program](http://www.jointcommission.org/patient_safety_systems_chapter_for_the_hospital_program)
- [3] AHRQ Guide to Inpatient Quality Indicators: Quality of Care in Hospitals - Volume, Mortality, and Utilization. Department of Health and Human Services. Agency for Healthcare Research and Quality. Junio, 2002. Version 3.1 (12 de marzo, 2007) (<http://www.qualityindicators.ahrq.gov>).
- [4] National Good Practice Guidance on Pre-operative Assessment for Inpatient Surgery. NHS Modernisation Agency. Marzo, 2003.
- [5] Postoperative Management in Adults. SIGN. Agosto 2004.
- [6] Cullinane M., Gray A. J. G., Hargraves C. M. K. , Lansdown M., Martin I. C., Schube M. (Recopilación). The 2003 Report of the National Confidential Enquiry into Perioperative Deaths. NCEPOD. Noviembre, 2003.
- [7] The Association of Anaesthetists of Great Britain and Ireland. Theatre Efficiency. Safety, Quality of Care and Optimal Use of Resources. Agosto, 2003.
- [8] The Association of Anaesthetists of Great Britain and Ireland. Recommendations for Standards of Monitoring During Anaesthesia and Recovery. Marzo, 2007.
- [9] The Association of Anaesthetists of Great Britain and Ireland. Immediate Postanaesthetic Recovery. Septiembre, 2002.
- [10] Gawande A.A., Studdert D.M., Orav E.J., Brennan T.A., Zinner M.J. Risk Factors for Retained Instruments and Sponges after Surgery. The New England Journal of Medicine. 2003; 348(3):229-235.
- [11] De Vries E.N., Ramrattan M.A., Smorenburg S.M., Gouma D.J., Boermeester M.A. The Incidence and Nature of In-Hospital Adverse Events: a Systematic Review. Qual. Saf. Health Care 2008;17:216-223.
- [12] DH. NHS Performance Indicators. Acute NHS Hospital Trusts. Febrero, 2002.
- [13] SCIP Process and Outcome Measures. SCIP. Disponible en: <http://www.aha.org/aha/issues/Quality-and-Patient-Safety/scip.html>
- [14] Audit Commission. Operating Theatres. Guide to the Indicators. Module 5 of 6. Versión 1, Noviembre 2002.

- [15] Leaper D., Burman-Roy S., Palanca A., Cullen K., Worster D., Gautman-Aitken E., Whittle M. Prevention and Treatment of Surgical Site Infection: Summary of NICE Guidance. *BMJ* 2008;337:a1924.
- [16] Aranaz J.M. (Dir.). Estudio nacional sobre los efectos adversos ligados a la hospitalización. ENEAS 2005. Informe. Febrero 2006. Ministerio de Sanidad y Política Social, 2006.
- [17] WHO surgical safety checklist and implementation manual. Disponible en: [http://www.who.int/patientsafety/safesurgery/ss\\_checklist/en/](http://www.who.int/patientsafety/safesurgery/ss_checklist/en/)
- [18] SAGES. Guidelines for the Clinical Application of Laparoscopic Biliary Tract Surgery. Disponible en: <http://www.sages.org/publications/guidelines/guidelines-for-the-clinical-application-of-laparoscopic-biliary-tract-surgery/>
- [19] Peter H. Cosman, Christopher J. Shearer, Thomas J. Hugh, Andrew V. Biankin., and Neil D. Merrett. A Novel Approach to High Definition, High-Contrast Video Capture in Abdominal Surgery. *Ann Surg*. 2007 Apr; 245(4): 533–535.
- [20] Steven Nicholas Graves, Deana Saleh Shenaq, Alexander J. Langerman, and David H. Song. Video Capture of Plastic Surgery Procedures Using the GoPro HERO 3+. *Plast Reconstr Surg Glob Open*. 2015 Feb; 3(2): e312.
- [21] Boanca C, Rafiq A, Tamariz F, Lavrentyev V, Onisor D, Flerov E, Popescu I, Merrell RC. Remote video management for intraoperative consultation and surgical telepresence. *Telemed J E Health*. 2007 Oct; 13(5):603-7.
- [22] Emous M, Westerterp M, Wind J, Eerenberg JP, van Geloven AA. Registering the critical view of safety: photo or video? *Surg Endosc*. 2010 Oct;24(10):2527-30.
- [23] Ahmadi SA, Sielhorst T, Stauder R, Horn M, Feussner H, Navab N Recovery of surgical workflow without explicit models.. *Med Image Comput Comput Assist Interv*. 2006; 9(Pt 1):420-8.
- [24] White MT, Drapiza M, Mattos MA, Edelman DA. An automated system for video documentation of all instances of fundamentals of laparoscopic surgery training: feasibility and potential advantages of extended assessment. *Am J Surg*. 2015 Jan; 209(1):158-62.
- [25] Emparan C. Reengineering health procedures. *Rev Calid Asist*. 2009 Nov-Dec; 24(6):237-8.
- [26] Castellanos I, Ganslandt T, Prokosch HU, Schüttler J, Bürkle T. Implementation of a patient data management system. Effects on intensive care documentation. *Anaesthesist*. 2013 Nov; 62(11):887-90, 892-7. German
- [27] Wilke MH, Grube RF, Bodmann KF. The use of a standardized PCT-algorithm reduces costs in intensive care in septic patients - a DRG-based simulation model. *Eur J Med Res*. 2011 Dec 2; 16(12):543-8.
- [28] Castellanos I, Schüttler J, Prokosch HU, Bürkle T. Does introduction of a Patient Data Management System (PDMS) improve the financial situation of an intensive care unit? *BMC Med Inform Decis Mak*. 2013 Sep 16; 13:107.

## Capítulo VI

# Unidad de Cuidados Intensivos: Aportaciones de las Tecnologías de la Información y Comunicación

*Daniel Luna*

*Selene Indarte*

*Humberto Mandirola*

*Sonia Benítez*



## Resumen

El proceso de atención de pacientes en unidades de cuidados intensivos o *intensive care units* (UCI) es complejo y requiere un rápido acceso a información clínica del paciente. Entre otras características los pacientes muchas veces están inconscientes, intubados, polimedicados, con múltiples transductores y la mayoría de las veces sin la familia presente. Los pacientes tienen mayor exposición a sufrir errores médicos y los profesionales a cometer esos errores debido a que se encuentran inmersos en este escenario. Las tecnologías de la información y comunicación (TIC) desempeñan un rol fundamental para dichos procesos y tienen el potencial para, en muchos casos, prevenir dichos fallos, aunque su introducción también puede determinar la aparición de nuevas equivocaciones. Las TIC sin duda son una ayuda para tomar decisiones pero también pueden inducir a errores si no están adecuadamente diseñadas.

El propósito de este capítulo será desarrollar los tópicos arriba mencionados realizando una revisión narrativa de las fuentes de información disponibles. *En primer lugar*, se hará una breve referencia a características de los pacientes en UCI, procesos asistenciales y fuentes de riesgo para la seguridad del paciente en dichos procesos. *En segundo lugar*, se expondrán los componentes de un Sistema de Información clínico en UCI, así como los fundamentos sobre la clasificación de los sistemas basados en TIC en estas unidades asistenciales. *En tercer lugar*, se describe a las TIC como estrategia para la mejora en la seguridad del paciente, así como la integración de la Información en este nivel de atención. *Finalmente*, se otorgará especial atención a los nuevos errores que genera el uso de TIC en este escenario, así como los sistemas de reportes de errores en UCI.

## Características del paciente en la Unidades de Cuidados Intensivos

En las UCI se asisten pacientes con variables fisiológicas muy alteradas y de alto riesgo de eventos catastróficos. El proceso de ingreso tiene varias entradas con diferentes características y controles. El proceso asistencial posterior tiene un formato de cuidado continuo (7 días/24 hs.) y requiere la presencia permanente de profesionales de la salud, tales como médico, licenciado y auxiliar de enfermería<sup>26</sup>, más la participación de otros especialistas. La propia condición de estos pacientes hace que sobre un tratamiento programado, se inserten decisiones intercurrentes que se toman ajustándose a su evolución. Estas decisiones terapéuticas, son en general urgentes, a veces instantáneas porque tienen como objetivo la estabilización del paciente.

El equipo de salud trabaja en un marco de incertidumbre, generado por diversos factores: falta de información, información en silos no siempre puesta en el contexto, información incompleta, falta de tiempo para verificar o probar estrategias. Además trabaja en un ámbito de altas expectativas en cuanto a resultados, pese a que la realidad indica que es un área de alta mortalidad. Por otro lado su desempeño se evalúa tanto por los medios utilizados, como por resultados en cuanto a humanismo, ética, y aspectos legales [1].

---

<sup>26</sup> En España, los grados equivalentes son médico, diplomado o graduado en enfermería y auxiliar de enfermería.

## Fuentes de riesgo para el paciente

La variada procedencia de los pacientes plantea el desafío de implementar una correcta, completa y consistente transmisión de datos e información que garanticen la continuidad asistencial [2]. Entre otros aspectos, destacan la correcta y unívoca identificación del paciente, la comunicación, el acceso a los datos de salud relevantes, y el relato completo de las condiciones y circunstancias que lo llevaron a ingresar en la UCI, entre otros.

La identificación del paciente es uno de los puntos críticos, es una barrera importante en la prevención de eventos adversos, pues hace confiable la información asociada al paciente: alergias, comorbilidades, entre otros.

Por otro lado, la comunicación y documentación clínica inefectivas pueden afectar la continuidad del cuidado y tener un importante impacto en la seguridad del paciente. Los espacios de comunicación entre los profesionales se extienden más allá del registro clínico y cuando la información se deja en carteles o anotaciones se pierde [3]. La falta de conocimiento detallado acerca de los pacientes y la inadecuada comunicación de los planes de cuidado se suman a los problemas derivados de transferencias ineficientes, entre los diferentes niveles de atención o entre los profesionales actuantes. En el caso de las UCI, el cambio de equipos suele ser cada 12 ó 24 horas para los médicos y cada 6 horas para enfermería, la transferencia de información se hace en forma verbal y escrita. La transmisión verbal está limitada por temas de tiempo y de atención de los involucrados y en general no está estandarizada. El cambio de equipo o de nivel de cuidado (también denominado *handoff* en inglés) muy frecuentes están asociados a mayores complicaciones e internaciones prolongadas. Según la Joint Commission, más del 80 % de los eventos centinela están relacionados a la pobre comunicación y la planificación de la continuidad del cuidado. A pesar de la importancia de la documentación del *handoff*, éste no se considera como una parte oficial de las historias clínicas de los pacientes [4][5][6].

La inestabilidad inherente a estos pacientes requiere el soporte de funciones vitales con diversos procedimientos terapéuticos, farmacológicos y no farmacológicos, muchas veces invasivos y no

carentes de efectos indeseables. La correcta aplicación de estos procedimientos requiere una variedad importante de conocimientos actualizados:

- a. productos farmacológicos, sus efectos indeseables, contraindicaciones, y riesgos en asociación con otros fármacos.
- b. técnicas y procedimientos exigen no solo destreza sino también conocimiento de instrumentos, riesgos y controles.

En UCI, los médicos ven pacientes portadores de cualquier patología, la especialidad no está encuadrada en un marco de conocimiento acotado, sino que está definida por la inestabilidad de cualquiera de los sistemas fisiológicos mayores. La carencia o el error en los datos repercutirán en la toma de decisiones posteriores. La información necesaria para tomar decisiones es inabarcable sin apoyo fácilmente accesible.

Una asistencia de calidad implica mantener una adecuada visión sistémica del paciente y un trabajo en equipo consistente entre los profesionales de la salud. En las UCI, el proceso asistencial es conducido por equipos asistenciales que son cambiantes debido a la necesaria rotación de personal en un formato de cuidado continuo. Esta rotación de profesionales genera una sumatoria de enfoques, opiniones, destrezas y actitudes que impactan en la asistencia, pues aunque compartan los criterios para manejar estos pacientes complejos, la medicina es un arte y cada uno de los profesionales pone una cuota de su visión personal sobre la patología. Es complejo mantener una adecuada visión sistémica cuando el equipo de salud se concentra en sostener funciones en falla. El equipo asistencial de UCI está entrenado para dar soporte a pacientes inestables, tomando muchas decisiones en poco tiempo, esto requiere mucha concentración en cada una de las situaciones a resolver. Como contrapartida, esto conspira contra la visión global o sistémica de la situación. Es complejo concentrarse en un detalle sin perder la visión general.

Cada uno de estos puntos es fuente de error y de riesgo para la seguridad de los pacientes, cada uno de ellos puede y debe ser reconocido, y se deben generar los mecanismos de control y soporte para el equipo asistencial de forma de prevenir o minimizar su incidencia así como sus consecuencias.

## Componentes de un Sistema de Información clínico en Unidades de Cuidados Intensivos

Dentro de los componentes que integran la información en las UCI se encuentran los medios complementarios de diagnóstico, básicamente, laboratorio e imágenes, los sistemas de documentación clínica, los sistemas de prescripción de órdenes y administración de medicamentos, sistema de órdenes médicas o *Computerized Provider Order Entry* (CPOE), y finalmente los Sistemas de Soporte a la Toma de Decisiones, también denominados en inglés *Clinical Decision Support Systems* (CDSS). A esto se debe sumar la conectividad con los distintos dispositivos que tienen que recibir y enviar información a los sistemas de registro y alarmas. A continuación se describen los componentes mencionados:

1. Medios complementarios de diagnóstico, laboratorio e Imágenes: Dentro de los servicios de análisis fundamentales para respaldar la actividad asistencial de la UCI se encuentra Laboratorio e Imágenes. Los pacientes críticos requieren correcciones frecuentes y realizar estudios muchas veces en forma horaria, por lo cual la comunicación fluida con estos servicios de diagnóstico es esencial. En la Figura 6.1 se puede ver la integración de los mismos en la Historia Clínica Electrónica (HCE).



**Figura 6.1.** Medios complementarios de diagnóstico, laboratorio e Imágenes.

2. Documentación clínica: El médico siempre debe documentar lo actuado, tarea nada sencilla ya que al mismo tiempo debe cumplir con su tarea asistencial [7]. De la integración colaborativa de la información entre los distintos profesionales sin duda el principal beneficiario es el paciente. Se deben atender los distintos entornos y tareas para que esa integración colaborativa de la información sea realmente eficaz, por ejemplo a partir de las indicaciones médicas organizar la planificación de las actividades de enfermería con posibilidades de alertas facilitando el trabajo integrado y en equipo del grupo de profesionales intervinientes Otro aspecto importante que se debe tener en cuenta, son los datos epidemiológicos para lograr hacer estudios de comparaciones entre hospitales de la evolución del paciente de UCI .
3. CPOE y sistemas de administración de la medicación: La eficacia de los CPOE particularmente en áreas cerradas de UCI tanto adultos como pediátricas está documentada en varios trabajos [8]. Distintos estudios han demostrado que los sistemas de prescripción con CPOE ayudan a reducir los errores de medicación y eventos adversos relacionados con la administración de medicamentos [9].
4. Conectividad con dispositivos al lado de la cama del paciente o “bedside”. Integración de los dispositivos médicos con la HCE. La cantidad de dispositivos que se conectan a los pacientes en UCI (véase Figura 6.2) son un elemento a tener en cuenta: monitores multi-paramétricos que censan distintos parámetros del paciente, temperatura, frecuencia cardiaca, saturación de oxígeno, brindando datos en tiempo real, respiradores mecánicos, bombas de infusión (véase Figura 6.3). Muchos de estos dispositivos y sensores digitales que se usan en UCI vienen con conexiones bluetooth lo que permite transmitir datos sin cables. La comunicación inalámbrica y transmisión de datos están desempeñando un papel cada vez mayor en el entorno de cuidados intensivos (véase Figura 6.4). Esto también genera nuevos problemas como las interferencias electromagnéticas (Electromagnetic Interference EMI), por lo cual en muchas UCI se prohíbe el ingreso con teléfonos celulares dado que estos pueden intervenir en las comunicaciones con los equipos y generar su desprogramación [10]. Estos dispositivos inalámbricos o wireless abrieron un nuevo capítulo en la medicina intensiva y control de pacientes que se llama telemetría. Todos los datos biométricos como electrocardiograma (ECG), la frecuencia cardiaca, temperatura,

nivel de goteo, la presión arterial del paciente se transmiten por medio de estos dispositivos por la red en forma digital y pueden ser recogidos por distintos programas y ser vistos por distintos actores responsables del control del pacientes como enfermeros, médicos interconsultores e incluso transmitirse a distancia, abriendo un abanico de múltiples posibilidades [11]. No aprovechar las posibilidades de integración que ofrecen los equipos digitales con los sistemas de información es un desperdicio, son varios los equipos de trabajo e investigadores que están buscando los medios y plataformas para mejorar esta integración día a día con la finalidad de mejorar la calidad asistencial de los pacientes [12]. Todos estos equipos son computarizados y permiten ser programados, dar alarmas e interoperar con los sistemas de información [13].



**Figura 6.2.** Dispositivos electrónicos en UCI.



**Figura 6.3.** Bombas de infusión.



**Figura 6.4.** Dispositivos en la nube.

5. Los CDSS comprenden sistemas y alertas que son fundamentales en UCI. Las mejoras en varios aspectos de la atención al paciente a través del uso de las CDSS pueden conducir a mejores resultados en los pacientes [14]. Los CDSS ayudan significativamente a reducir los errores en la UCI [15]. En varios estudios las alertas han demostrado su utilidad, sin embargo se debe tener en cuenta que la sobreabundancia de alertas lleva a que el médico las desestime, la presencia de alertas debe pensarse para cada problema específico y para cada área en forma dinámica y teniendo en cuenta la usabilidad y la vigencia, debemos tener especial atención en eliminar la alerta cuando esta ya no tiene más razón de ser [16]. Los profesionales de la salud deben hacer esfuerzos para incorporar estas herramientas siempre que sea posible [12]. Cuando hablamos de alertas también se tienen que tener presentes las relacionadas con la vigilancia epidemiológica tanto intra como extra hospitalaria. Es importante armar alertas relacionadas con las infecciones intrahospitalaria, la posibilidades de detectar gérmenes potencialmente peligrosos multirresistentes y determinar causas y definir soluciones son elementos fundamentales para evitar la propagación de infecciones intrahospitalarias que tienen un alto impacto en los costos y en la morbilidad de los pacientes [17].

## Clasificación de los sistemas basados en Tecnologías de Información y Comunicación en Unidades de Cuidados Intensivos

Las UCI son unidades cerradas que debido a la urgencia de datos que requiere el sector, muchas de ellas tienen servicios complementarios propios, tales como laboratorio propio, sistemas de imágenes y administrativos para autorizar órdenes. Por lo tanto, los sistemas involucrados en estas áreas son prácticamente los mismos que los del resto del Hospital, pero orientados a satisfacer las necesidades de la urgencia. Los sistemas informáticos están cada vez más presentes en la UCI y forman parte del propio equipamiento del lugar, equipos que antes eran totalmente analógicos hoy son digitales con capacidad de procesar señales, recibir, mandar datos e interoperar con otros sistemas y dispositivos [18]. Dentro de la lista de estos equipos se encuentran los respiradores, monitores, electrocardiógrafos, oxímetros, capnógrafos, bombas de infusión, entre otros.

Las TIC comprendidas en las UCI se pueden dividir en tres grandes capas: asistencial, administrativo-asistencial y administrativa.

Dentro de los sistemas de la capa asistencial tenemos a su vez distintos tipos de programas:

1. Sistemas que controlan equipos, respiradores, sistemas de señales para monitores, electrocardiógrafos y distintos sensores que permiten hacer determinaciones e informar resultados en el momento (véase Figura 6.5). Los respiradores contienen programas que permiten hacer gráficos online y conocer todos los parámetros necesarios para manejar la asistencia mecánica respiratoria, tienen la posibilidad de programar alarmas y mostrar esta información en un monitor propio del equipo y, a su vez, poder transmitir mediante interfaces esa información a otros sistemas. En la Figura 6.6 vemos un respirador con la pantalla de monitor en donde nos muestra los datos programados, las alarmas y la curva respiratoria relacionada con el tipo de soporte de asistencia mecánica respiratoria que se le está brindando al paciente.
  - a. Aquí es importante tener en cuenta que cuando interactúan varios sistemas y equipos electro-médicos que transfieren datos de pacientes, es imprescindible hacer una correcta identificación del paciente. Para tal fin, se usa la Gestión de la Identidad del

Paciente (GIP) del inglés Patient Identity Management (PIM). El GIP permite determinar una identidad única para un individuo (paciente), expresada por un identificador único. El identificador único será producto de la combinación de datos tales como nombre, fecha de nacimiento, sexo, entre otros [19].



**Figura 6.5.** Pantalla de respirador.



**Figura 6.6.** Respirador Informatizado.

2. Sistemas de información y Gestión asistencial. Dentro de estos sistemas tenemos disponibles:
  - a. La HCE en donde los profesionales de la salud actuantes consignan los datos referentes a la evolución clínica, antecedentes, examen físico, informes de interconsulta, entre otros.

- b. CPOE. Es frecuente que estos sistemas de órdenes médicas se integren con los CDSS, lo que reduce considerablemente las tasas de errores relacionadas con la prescripción de medicamentos y efectos adversos relacionados con la medicación [20].
- c. Registro de Enfermería: permite manejar la administración de medicamentos, los controles de signos vitales, balances hidroelectrolíticos y las evaluaciones de enfermería.
  - i. Sistemas de administración de medicación por código de barras (Barcode Medication Administration Systems) que permiten garantizar que la medicación correcta llegue al paciente correcto identificado bien al paciente y al medicamento que este debe recibir. Los daños a pacientes ocasionados por errores de medicación evitables constituyen un serio problema y ponen en riesgo la vida del paciente, constituyen un serio problema con repercusiones asistenciales económicas y problemas de mala praxis. El sistema de doble control del inglés double-check ha sido diseñado para minimizar los errores en el suministro de medicación. El proceso de “doble chequeo” consta de un protocolo de control que deben seguir dos personas en forma independiente sobre puntos vulnerables con el objetivo de interceptar errores, porque es menos probable que dos personas distintas se equivoquen al controlar el mismo proceso. Este doble control es aconsejable por ejemplo para controlar bombas de infusión donde se administran medicamento de algo riesgo [21]. Un método de chequeo eficaz a la hora del suministro de medicamentos es el método de los “cinco correctos”, el mismo controla, la administración de la dosis correcta, del adecuado medicamento, al paciente indicado y en el tiempo y vía apropiada.” Este método se debe complementar con otro tipo de controles, tales como la preparación adecuada del medicamento, la administración mediante técnica correcta, la comprobación del periodo de validez del fármaco [22].
  - ii. CDSS, guías de práctica clínicas y alertas clínicas.

Dentro de la capa administrativo-asistencial se encuentran los sistemas de los estudios complementarios de diagnóstico y organizativos de la tarea asistencial, que corresponden también a los sistemas departamentales del Sistema de Información Hospitalaria.

1. Sistema de laboratorio de análisis clínicos del inglés LIS (Laboratory Information System): estos sistemas permiten gestionar todo lo que tiene que ver con el proceso de los laboratorios de análisis clínicos. Los LIS, a su vez, se comunican mediante interfaces con muchos equipos informatizados que tienen sus sistemas informáticos propios dentro del laboratorio que procesan las muestras en sí mismo, con interfaces unidireccionales o bidireccionales permitiendo que el LIS les informe qué muestras y qué determinaciones tienen que procesar, y recibir, a su vez, los resultados de estos autoanalizadores.
2. Sistema de Información de Radiología e imágenes del inglés RIS (Radiological Information System). Estos sistemas manejan todo lo referente a las imágenes médicas, tanto para los informes, para la gestión del servicio de imágenes y para el almacenamiento de las imágenes en sí mismas.
3. Sistema de admisión de pacientes del inglés ADT system (Admission, Discharge, Transfer), [23]. Estos programas permiten gestionar el ingreso, traslado y egreso del paciente así como administrar la dotación de camas de una institución incluyendo obviamente las camas correspondientes al sector de UCI.

Dentro de los sistemas de la capa administrativa pura se encuentran:

1. Módulos de recepción: permiten hacer la recepción de órdenes y mandarlas a los distintos sectores que corresponde para autorizar o para ser procesadas.
2. De facturación: interactúa con los programas asistenciales para recibir información de las prácticas que se le están realizando al paciente y poder facturar las mismas.
3. Gestión de órdenes y autorización de estudios.

Estos grupos de sistemas pueden andar en forma independiente, integrarse o interoperar entre sí. Para poder interactuar correctamente es necesaria la utilización de estándares terminológicos y de mensajería, sino las posibilidades de intercambio de información y aprovechamiento de la información entre sistemas se hacen prácticamente imposibles [24].

## **Tecnologías de Información y Comunicación como estrategia para la mejora en la seguridad del paciente**

Las TIC deben perseguir como principal objetivo mejorar la calidad asistencial y la seguridad del paciente (SP) o al menos minimizar el

riesgo de provocar daño innecesario como consecuencia de la atención médica. Se destacan para este propósito y se describen a continuación, los dispositivos de dispensación automática, los sistemas de dispensación, el sistema de farmacia, los sistemas de administración de medicación por código de barras, el CPOE, las tecnologías de bomba inteligente de infusión de medicamentos, o “*Smart*” *pump* en inglés, entre otros, teniendo en cuenta el proceso global que los involucra.

#### 1. Ciclo de la medicación

- a. CPOE: No hay ninguna duda de que ayudan a reducir los errores. Para que un sistema CPOE tenga éxito en su implementación, debe ser amigable fácil de utilizar y tener en cuenta la usabilidad. Un informe resumen del grupo Leapfrog [25] se centra en este y otros temas que se deben abordar a la hora de considerar la posibilidad de utilizar sistemas CPOE.
- b. Dispositivos de dispensación automática: Las TIC y la automatización de los procesos están modificando sustancialmente la dispensación de medicamentos en los hospitales, además de simplificar y transformar los contenidos de la práctica farmacéutica. La automatización, sin embargo, exige un importante cambio cultural y de trabajo para todas las unidades clínicas, pero sobre todo una reorganización en el trabajo, en las indicaciones médicas, en el servicio de farmacia y en el proceso de suministro de medicamentos por parte de enfermería. Estos dispositivos permiten la centralización de la información, y contar con información centralizada garantiza la accesibilidad y la calidad de los datos [22].
- c. Sistemas de dispensación (Robotics Dispensing Systems): Los Sistemas de Dispensación de Medicamentos Mediante Dosis Unitarias (SDMDU) surgieron en la década de los sesenta como mecanismo efectivo para la disminución de los errores existentes en la prescripción, preparación y administración de medicamentos. Estos sistemas deben responder a la exigencia de que la medicación de los pacientes. esté disponible en enfermería para su suministro en tiempo y forma, para lo cual es necesario hacer varias reposiciones al día. Con la dispensación tradicional sólo una pequeña parte del tratamiento del paciente está disponible en la Unidad de Hospitalización [23].
- d. Sistemas de administración de medicación por código de barras: la identificación correcta del paciente es fundamental, parece una tarea sencilla pero no lo es, los pacientes en medios hospitalarios y

más en UCI, sufren distintos grados de alteración de la conciencia por lo cual no pueden identificarse por sus propios medios. Para poder identificar automáticamente al paciente correcto, en el momento del ingreso en el hospital a cada paciente se le debe colocar una pulsera con código de barras para su correcta identificación. Para asegurarnos no cometer errores es importante considerar el método de los “cinco correctos”, este controla, la administración de la dosis correcta, del adecuado medicamento, al paciente indicado y en el tiempo y vía apropiada [22]. Los códigos 2D tipo QR o GS1 son capaces de ser escaneados multidireccionalmente, al revés, hacia atrás o hacia adelante e incluso en diagonal, lo que los convierte en la elección ideal en un entorno hospitalario. Identificar al paciente correcto es fundamental, pero para evitar errores es también importante identificar al medicamento correcto y esto la tecnología también puede ayudar. Muchos trabajos muestran que la tasa de error en la prescripción y administración de medicamentos en UCI en los procesos manuales es alta y disminuye sensiblemente informatizando y automatizando estos procesos [26].

- e. Tecnologías “Smart” pump: El desarrollo de las bombas de infusión ha revolucionado el modo en que el personal de enfermería administra la terapia intravenosa. A diferencia de los medicamentos, que se preparan y dispensan ajustándose a los requerimientos de cada paciente de forma individualizada, las bombas de infusión están diseñadas para ofrecer una amplia flexibilidad y poder utilizarse en cualquier unidad de hospitalización, tanto en pacientes adultos como en pacientes pediátricos [27].
- f. Sistemas de Farmacia (Pharmacy-based Computer Systems): Si bien los sistemas informatizados de farmacia hospitalarios son costosos, es necesario evaluar el costo beneficio que tienen respecto no solo del control administrativo de stock, compras y dispensación de medicamentos, sino del apoyo que brindan a la tarea asistencial [28]. Este sistema puede estar relacionado con sistemas ADT, sistemas de admisión, transferencia y descarga de datos, facturación, sistema informático de farmacia o sistema de información de cuidados a pacientes [23]. La gestión electrónica de la farmacoterapia tiene por fin mejorar y garantizar una utilización segura, de calidad y eficiente de los medicamentos por parte de los pacientes. En su diseño y desarrollo es necesario

tener una visión completa del sistema en la que sean prioritarios aspectos tales como: la integración de la información, la homogeneidad, la coherencia, la versatilidad, la seguridad de los datos, la capacidad de explotación y la escalabilidad [29].

2. Toma de decisiones

- a. Alerta de dosis para Insuficiencia renal (Alertas de dosificación renales - Renal Dosing Alerts): Son CDSS que permiten identificar problemas relacionados con los medicamentos y calcular los ajustes de cada droga a las distintas situaciones del paciente. Este tipo de CDSS permiten dar alertas sobre la dosis que se está usando y ajustar la misma de acuerdo a la función renal [30].
- b. Calculadores: Estas herramientas incluyen los Calculadores farmacocinéticos de dosificación (Pharmacokinetic Dosing Tools), tablas de dosificación, y herramientas de dosificación y gráficos. Estos están disponibles para varios fármacos como los aminoglucósidos, fondaparinux, digoxina, litio, teofilina, y vancomicina. El propósito de estas herramientas es evitar errores de dosificación debido a cálculos hechos a mano, estandarizar el proceso, y disminuir el tiempo requerido para calcular un régimen apropiado. Estas herramientas incluyen también ecuaciones de dosificación simplificadas para aquellos profesionales que deseen hacer cálculos a mano. Las herramientas gráficas son más rápidas y más fáciles de usar que los programas tradicionales o las calculadoras cuando se analizan los niveles séricos. Lo ideal sería que se pueda determinar el régimen inicial con la calculadora de dosificación y luego utilizar las herramientas gráficas para hacer ajustes de dosis [31].

3. Monitoreo de pacientes

- a. Monitoreo Inteligente basado casos similares. Existen iniciativas como la base de datos de Monitoreo Inteligente Multi-parámetro en UCI ( MIMIC del inglés Multiparameter Intelligent Monitoring in Intensive Care). MIMIC captura datos estructurados altamente granulares incluyendo los cambios en las señales fisiológicas minuto a minuto, así como cuando se administra la medicación y sus dosis. Tal detalle permite el modelado de la respuesta dinámica individual, lo que lleva a un mejor cálculo de riesgo-beneficio y la predicción de resultados. Esto a su vez permite el desarrollo de herramientas de CDSS en el punto de atención destinadas a proporcionar un pronóstico

confiable basado en datos comparables para las variables que influyen en los resultados pertinentes [32][33][34].

- b. Estas herramientas incluyen la HCE, plataformas de telesalud, los registros electrónicos, software de gestión de datos y sistemas de análisis. Los profesionales pueden usar las HCE y herramientas de automatización, en particular para identificar y estratificar a los pacientes, identificar las brechas de atención, medir los resultados, y animar a los pacientes a asumir más responsabilidad por su salud [35].
- c. Handoffs: La información que se encuentra en la documentación del handoff es importante para la toma de decisiones clínicas. Si la documentación se integra en la HCE, puede ser fácilmente accesible a los miembros del equipo de cuidado y esto podría mejorar la comunicación y reducir los errores médicos [4][5][6].
- d. Telemedicina en UCI (Tele-UCI): La atención en UCI requiere mucho personal entrenado. Existe un déficit de profesionales en el área debido a que la proporción de especialistas en UCI no ha variado. A este déficit se suma que la complejidad de los pacientes ha ido en aumento y muchas veces no se pueden trasladar a centros de mayor complejidad. La Tele-UCI permite solucionar el problema al disponer de profesionales en forma remota, no solo para el monitoreo sino para la consulta y toma de decisiones compartida con el equipo que se encuentra asistiendo al paciente en forma directa. La Tele-UCI a través del seguimiento continuo de los signos vitales del paciente, ha permitido identificar patrones de deterioro, y permite un cuidado proactivo, lo que puede reducir la mortalidad y el tiempo de internación. A esto se suma que en Tele-UCI las alertas y la evaluación por cámaras puede reducir el riesgo de caídas así como las extubaciones [36][37].

## Integración de la información en Unidades de Cuidados Intensivos

Evaluar la información en una UCI puede ser una tarea complicada debido a que el volumen de información que se maneja suele ser importante. En las UCI hay una amplia gama de datos que se generan de forma continua, que provienen de monitores fisiológicos, bombas de infusión intravenosa y administración de medicación, y de la asistencia ventilatoria, entre otros. Muchos monitores y dispositivos tienen sistemas

de alarmas que deben ser evaluados a lo largo de la jornada de trabajo [38]. El ambiente de la UCI puede ser rediseñado para reducir la carga cognitiva, los errores y los costos asociados y mejorar la comunicación de los profesionales de la salud. En ese aspecto, un número creciente de UCI están adoptando el Modelo Electrónico de Cuidado Crítico, del inglés *e-ICU Model* [39]. Este modelo comprende la reingeniería de la UCI teniendo en cuenta tanto el componente tecnológico como el uso de la tecnología, con el objetivo de mejorar la seguridad del paciente, optimizando la presentación de los datos y facilitando el flujo de trabajo del profesional actuante.

Esto implica utilizar las aplicaciones y equipamiento de tal modo que logren crear una red y conectarlas a un sistema de monitoreo central, que permita intervenciones oportunas al facilitar la identificación de problemas y la toma de decisiones. Este tipo de modelo permite que profesionales de la salud puedan interactuar con los pacientes incluso por fuera de la institución, pudiendo tener equipos remotos de trabajo [40].

En cuanto a la producción de reportes, la alternativa a un reporte estático de los datos producidos en la UCI, es desarrollar un sistema dinámico que ayude a la toma de decisiones y promueva estrategias de mejoramiento. Existen experiencias de sistemas expertos que con datos vitales predicen pacientes de alto riesgo de deterioro [34]. La solución más eficiente es instalar un sistema que muestre simultáneamente múltiples elementos del registro del paciente sin tener que acceder a cada sistema en forma individual [40]. Este tablero de mandos es el denominado dashboard clínico que da una retroalimentación o feedback en tiempo real, tal que permita tomar decisiones y hacer las correcciones necesarias.

En general, los 4 elementos para que un tablero de mandos sea efectivo son [41]:

1. Construirlo teniendo en cuenta un conjunto de medidas de desempeño.
2. Seleccionar el conjunto mínimo de medidas, entre 15 y 30.
3. Presentar los datos en forma gráfica.
4. Desarrollar gatillos o situaciones que actúan como disparadores de acción, también denominados en inglés triggers.

Hay que tener en cuenta que si se usan diferentes formatos de gráficos en la pantalla, puede ser más difícil detectar eventos críticos [42]. Muchos tableros usan un código de colores para mostrar la información a los usuarios, con el enfoque de “semáforo” donde el verde indica que no hay ninguna acción a tomar por el individuo y el rojo indica que se requiere una acción. También se usan listas de indicadores en forma de tablas, gráficos de barras y circulares. Puede ser usado como un protector de pantalla, estar continuamente visible, o acceder en forma pro-activa [43].

La integración de todos los datos pertinentes en un tablero pueden mejorar la eficiencia del personal, mejorar las decisiones, optimizar los procesos de flujo de trabajo y reducir descuidos y errores en la práctica clínica [38]. Cuando la información en tableros clínicos es accesible, su uso se asocia a mejoras en el proceso de atención del paciente por ejemplo, disminución de las tasas de neumonía asociada a la ventilación mecánica, o aumento de la prescripción de antibióticos en tiempo oportuno [43].

## Nuevas amenazas generadas por el uso de Tecnologías de Información y Comunicación en Unidades de Cuidados Intensivos

La implantación de TIC en la gestión de los servicios sanitarios es una realidad y ha aportado beneficios para médicos y pacientes [44]. Sin embargo, hay que analizar los puntos donde la implantación de un Sistema de Información Informatizado (SIS) puede generar o favorecer la aparición de errores. Un SIS no solo debe disminuir errores, sino que no debe contribuir a generarlos [45]. Se pueden identificar distintas instancias en las que se pueden generar dichas amenazas.

En las definiciones del software a usar, se deben analizar diversos aspectos, como se expresan en la Tabla VI.1.

<b>Tabla VI.1. Aspectos a considerar respecto al software.</b>		
<b>Etapa</b>	<b>Tomar en cuenta</b>	<b>Riesgos</b>
Diseño	Con visión sistémica Proceso asistencial integral	Pérdida de datos Error en los datos
Desarrollo	Necesidades de registro Condiciones de trabajo Más de un médico a cargo	Sub-registro Fraccionamiento de la información
Robustez*	Disponibilidad de la información Acceso ininterrumpido y a tiempo Seguridad	Falta de datos Fraccionamiento de la información
Interoperabilidad**	Transferencias entre distintos sectores Estudios fuera de UCI Procedimientos fuera de UCI Datos de monitoreo de otros instrumentos	Pérdida de datos Error en los datos
* Fuente: [44] ** Fuente: [45]		

Surge de la tabla que las principales consecuencias de los errores en el diseño del software están vinculados a la pérdida o fraccionamiento de la información, lo que indudablemente tendrá impacto en la toma de decisiones de los profesionales que la utilicen.

Hay que mantener un equilibrio entre el uso de las TIC para control de aspectos administrativos y su uso para dar soporte al proceso asistencial. El personal asistencial registra con objetivos asistenciales. No son rigurosos al registrar datos cuyo impacto clínico no es obvio. Los sistemas deben ser inteligentes en el análisis de la información asistencial para elaborar la información administrativa, epidemiológica o de gestión. Un sistema que requiera el ingreso de datos que el médico no valora, lleva a que se generen registros incompletos y esto conducirá a conclusiones erróneas.

Uno de los beneficios de las TIC es la incorporación de los CDSS [48]. Si esta herramienta, que debe ser una ayuda, enlentece el registro, u obliga a dar muchos pasos intermedios será subutilizada, no se leerán los mensajes ni las alertas. El sistema registrará que el médico recibió

el aviso, pero en realidad no hubo ninguna interacción con la misma y se perderán todos los beneficios y los controles que ayudan a minimizar errores.

Es necesario combatir la creencia de que un SIS bien diseñado puede sustituir el pensamiento clínico. La lógica informática se complementa con el conocimiento en salud para colaborar en disminuir la incertidumbre. De ninguna manera es un sustituto al juicio clínico, de la experiencia acumulada ni del conocimiento profesional. Es una fuente de riesgo que los profesionales confundan la herramienta con el objetivo.

## Sistema de reporte de errores en Unidades de Cuidados Intensivos

Una de las estrategias empleadas para disminuir los errores es aprender de ellos y evitar que se repitan. La información sobre los errores se puede obtener a través de la auditoría de registros clínicos y se pueden evaluar en los ateneos de morbi-mortalidad<sup>27</sup>, sesiones donde se discuten las complicaciones o muerte de los pacientes, sus causas y posibles soluciones. A estas estrategias se le suman los Sistemas de Reporte de Incidentes (SRI) considerados un requisito para el éxito en la implementación de una cultura de seguridad del paciente [49][50]. En general se basan en la notificación voluntaria y anónima de incidentes, dependiendo que los involucrados proporcionen información detallada. En un sistema efectivo, el reporte de incidentes debe provenir de todos los profesionales de la salud, además de enfermería, debe proteger la privacidad de los que reportan, la difusión de los incidentes debe hacerse en el tiempo adecuado, y la revisión de los incidentes debe permitir la implementación de mejoras [51].

La utilización de los SRI permite identificar los eventos, intervenir, pero no permite el análisis de los datos agregados. Muchas veces es anecdótico, no permite calcular tasas, y puede haber sesgo de selección o de reporte [52]. Dentro de las barreras percibidas se encuentran que no hay feedback o seguimiento, falta de tiempo u olvidos para reportar, no está claro quienes debe reportar, ni qué se debe reportar [53].

---

<sup>27</sup> Morbi-mortalidad corresponde a la contracción de “morbilidad” y “mortalidad”. Según la RAE, “morbilidad” se denomina a la proporción de personas que enferman en un sitio y tiempo determinado.

Si bien los sistemas tradicionales reciben información de cualquier sector del hospital, existen experiencias en ambientes específicos. Según un informe (en revisión) [54], en las UCI se usan tanto formularios en papel como electrónicos para el reporte de incidentes. A menudo incluyen secciones para la descripción del incidente, la lesión, tratamiento y acciones inmediatas tomadas para minimizar la repetición del incidente. La ventaja de los sistemas electrónicos es que permiten la presentación de informes confidenciales, y el ingreso en una base de datos analizables sin la demora y potencial error de la transcripción.

Dentro de los SRI específicos, se encuentra el Sistema de Reporte Seguro para Unidades de Cuidados Intensivos (SRS-UCI), del inglés Intensive Care Unit Safety Reporting System, sistema web voluntario y anónimo para la UCI, vigente entre 2001 y 2005. A diferencia del Sistema Australiano de Monitoreo de Incidentes (SAMI) o Australian Incident Monitoring System [55], el SRS-UCI recolectaba todo tipo de incidentes de múltiples UCI de Estados Unidos. Los datos se presentaban a través de informes mensuales, discusiones de casos y un boletín trimestral [56]. Se centraba en las condiciones en que trabaja el personal para prevenir y limitar el efecto de los errores más que en culpar a las personas por causar errores. Una evaluación posterior determinó que al implementar había que tener en cuenta la integración con las estructuras de reporte de incidentes existentes, la promoción del uso del reporte, así como la codificación y análisis de los eventos. La presencia de múltiples reportes no es recomendable, debería consolidarse en un único reporte y considerar cómo compartir la información con todos los interesados. Para estimular la participación, los sistemas de reporte deben ser intuitivos y amigables, anónimos, confidenciales, no punitivos y deben dar un feedback en tiempo y forma [57].

En el caso de España, en el ámbito nacional, podemos mencionar el Sistema de Notificación y Aprendizaje para la Seguridad del Paciente (SiNASP)<sup>28</sup>. Este sistema web de notificación voluntaria permite la notificación anónima y nominativa con de-identificación de los datos. El SiNASP está desarrollado y promovido por el Ministerio de Sanidad, Servicios Sociales e Igualdad. El sitio web presenta un área pública donde el profesional notifica los incidentes de seguridad. Luego de la notificación, continúa con diferentes niveles de agregación: el centro

---

<sup>28</sup> SiNASP, Sistema de Notificación y Aprendizaje para la Seguridad del Paciente. Disponible en: <https://www.sinasp.es>

sanitario, el área sanitaria, la comunidad autónoma, hasta llegar al ministerio. Finalmente, se realiza el análisis de los incidentes, utilizando el área privada del sitio web del SiNASP [58].

Otros ejemplos en España son el ISMP-España, el Programa d'Errors de Medicació-Gencat, el Sistema Español de Farmacovigilancia y el Sistema de comunicación y análisis de incidentes críticos de la Fundación Hospital Alcorcón [59].

## Conclusiones

La complejidad de los procesos y la sobrecarga de información pueden representar un problema en el momento de la atención de los pacientes en general, y más aun en los pacientes críticos. En las UCI los pacientes son de alto riesgo de eventos catastróficos que requieren la asistencia de profesionales de la salud en forma permanente. La propia condición de estos pacientes hace que se tomen decisiones terapéuticas urgentes con objetivo de estabilizar al paciente. Los equipos de salud trabajan en un marco de incertidumbre con altas expectativas en un área de alta mortalidad. La carencia o el error en los datos repercutirán en la toma de decisiones posteriores. La incorrecta identificación del paciente, la falta de acceso a los datos de salud relevantes, el relato incompleto de las condiciones y circunstancias que llevaron al paciente a la UCI, y la falta de comunicación en el equipo interviniente, o el uso de canales inadecuados son fuente de error y de riesgo para la seguridad de los pacientes.

Las TIC comprendidas en las UCI incluyen desde sistemas que controlan equipos, respiradores, sistemas de señales para monitores, electrocardiógrafos y distintos sensores, hasta la HCE, sin olvidar el CPOE o los sistemas de administración de medicación por código de barras, además de los CDSS generando información de forma continua. También hay que tener presente a dispositivos de dispensación automática, las tecnologías “Smart” pump, teniendo en cuenta el proceso global que los involucra. Aquí cobra importancia la integración de los dispositivos con la HCE, no solo a los efectos del registro de información, si no para contar con un reporte dinámico de los datos producidos en la UCI. Esto promueve estrategias de mejoramiento y permite tomar decisiones y hacer las correcciones necesarias. El proceso de atención de pacientes en las UCI requiere un rápido acceso

a información clínica del paciente. Indudablemente las TIC son una ayuda para tomar decisiones pero también pueden inducir a errores si no están adecuadamente diseñadas. En la Tabla VI.2 se describen los riesgos en la implementación de los Sistemas, así como soluciones y oportunidades encontradas.

<b>Tabla VI.2. Riesgos en la implementación de los Sistemas, Soluciones y oportunidades.</b>		
<b>Riesgos</b>	<b>Definición</b>	<b>Soluciones y oportunidades</b>
Confundir la herramienta con el objetivo	Se focaliza en el uso del sistema en lugar de explotar sus funcionalidades	Proyecto y estrategia bien definido
Sistemas mal diseñados	No basados en estándares, fraccionados, flujos de información inadecuados	Diseño adecuado, con conocimiento del tarea asistencial
Incorrecta Identificación de pacientes	Falta de Índice Maestro de Pacientes (del Inglés Master Patient Index - MPI -), identificador único, incorrecta administración de personas	Tener un MPI nacional o local, adecuadamente estructurado y mantenido
Brecha de apropiación	Se usa el sistema pero no se sabe ni se estimula a sacarle el máximo provecho ni a sugerir mejoras	Capacitar y superar las brechas de apropiación
Cansancio por alertas	Múltiples alertas que interfieren constantemente con el trabajo. El usuario deja de prestarles atención	Diseño adecuado, con conocimiento del tarea asistencial
No lograr alta disponibilidad del sistema	Los sistemas de información en salud deben estar operativos 7 días a la semana y 24 horas al día	Hardware adecuado, mantenimiento adecuado. Sistemas de respaldo
Fallas en la Interoperabilidad inter e intra-institucional que comprometen la continuidad asistencial	Flujo de información permanente entre distintas instituciones y entre distintos niveles asistenciales	Diseño en base a estándares. Políticas de interoperabilidad

## Bibliografía

- [1] Civetta, J.M., 1992. Critical care: how should we evaluate our progress? *Critical care medicine*, 20, pp.1714–1720.
- [2] Sanchez, L. & Casado, M., 2014. Continuidad de la atención de salud basada en la integración entre niveles asistenciales. In *Manual de salud electrónica*. pp. 159–177.
- [3] Coiera, E., 2014. Communication spaces. *Journal of the American Medical Informatics Association* : JAMIA, 21(3), pp.414–22. Available at: <http://www.pubmedcentral.nih.gov/articlerender.fcgi?artid=3994845&tool=pmcentrez&rendertype=abstract> [Accessed January 6, 2016].
- [4] Collins, S.A. et al., 2012. In Search of Common Ground in Handoff Documentation in an Intensive Care Unit. *Journal of Biomedical Informatics*, 45(2), pp.307–315. Available at: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3306473/>
- [5] Dyches, R., 2014. Implementation of a Standardized, Electronic Patient Hand Off Communication Tool in a Level III NICU. *OJNI*, 18(2). Available at: <http://www.himss.org/ResourceLibrary/GenResourceDetail.aspx?ItemNumber=30535>
- [6] Vawdrey, D.K. et al., 2013. Implementation of a Computerized Patient Handoff Application. *AMIA Annual Symposium Proceedings*, 2013, pp.1395–1400. Available at: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3900153/>
- [7] Cerón Díaz, U. et al., 1996. Base de datos para el control de calidad y utilización de recursos en la unidad de terapia intensiva. *Rev. Asoc. Med. Crit. Ter. Intensiva*, 10(5), pp.195–201. Available at: <http://bases.bireme.br/cgi-bin/wxislind.exe/iah/online/?IsisScript=iah/iah.xis&src=google&base=LILACS&lang=p&nextAction=lnk&exprSearch=184183&indexSearch=ID>
- [8] Cordero, L. et al., 2004. Impact of Computerized Physician Order Entry on Clinical Practice in a Newborn Intensive Care Unit. *Journal of Perinatology*, 24(2), pp.88–93. Available at: <http://www.nature.com/jp/journal/v24/n2/abs/7211000a.html>
- [9] Potts, A.L. et al., 2004. Computerized Physician Order Entry and Medication Errors in a Pediatric Critical Care Unit. *Pediatrics*, 113(1), pp.59–63. Available at: <http://pediatrics.aappublications.org/content/113/1/59>
- [10] Gladman, A.S. & Lapinsky, S.E., 2007. Wireless technology in the ICU: boon or ban? *Critical Care*, 11(5), p.165. Available at: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2556738/>
- [11] Dextronix, 2015. ICU Telemetry. Available at: <http://www.dextronix.com/products/icu-monitor/>
- [12] Price, C.P. & Kricka, L.J., 2007. Improving Healthcare Accessibility Point-of-Care Technologies. *Clinical Chemistry*, 53(9), pp.1665–1675. Available at: <http://www.clinchem.org/content/53/9/1665>
- [13] Tsien, C.L. & Fackler, J.C., 1997. Poor prognosis for existing monitors in the intensive care u... : *Critical Care Medicine*. *Critical care medicine*. Available at: [http://journals.lww.com/ccmjournal/Abstract/1997/04000/Poor\\_prognosis\\_for\\_existing\\_monitors\\_in\\_the.10.aspx](http://journals.lww.com/ccmjournal/Abstract/1997/04000/Poor_prognosis_for_existing_monitors_in_the.10.aspx)
- [14] Williams, C.N., Bratton, S.L. & Hirshberg, E.L., 2013. Computerized decision support in adult and pediatric critical care. *World Journal of Critical Care Medicine*, 2(4), pp.21–28. Available at: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3953873/>
- [15] Landrigan, C.P. et al., 2004. Effect of Reducing Interns' Work Hours on Serious Medical Errors in Intensive Care Units. *New England Journal of Medicine*, 351(18), pp.1838–1848. Available at: <http://dx.doi.org/10.1056/NEJMoa041406>.
- [16] Mandirola Brieux, H.F. et al., 2014. Nutritional Alert in hospitalized patients. *European Federation for Medical Informatics and IOS Press. Studies in Health Technology and Informatics*, Volume 205, pp.697–70.
- [17] Klevens, R.M. et al., 2006. Changes in the epidemiology of methicillin-resistant *Staphylococcus aureus* in intensive care units in US hospitals, 1992-2003. *Clinical infectious diseases* : an official publication of the Infectious Diseases Society of America, 42(3), pp.389–91. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/16392087> [Accessed January 6, 2016].

- [18] Dedrick, J. & Kraemer, K.L., 2007. Globalization of Innovation: The Personal Computing Industry. Personal Computing Industry Center. Available at: <http://escholarship.org/uc/item/4v78b88r>.
- [19] Gliklich, R.E., Dreyer, N.A. & Leavy, M.B., 2014. Managing Patient Identity Across Data Sources. In R. Gliklich, N. Dreyer, & M. Leavy, eds. *Registries for Evaluating Patient Outcomes: A User's Guide*. 3rd edition. Agency for Healthcare Research and Quality (US). Available at: <http://www.ncbi.nlm.nih.gov/books/NBK208618/> [Accessed January 6, 2016].
- [20] Kuperman, G.J. et al., 2007. Medication-related Clinical Decision Support in Computerized Provider Order Entry Systems: A Review. *Journal of the American Medical Informatics Association*, 14(1), pp.29–40. Available at: <http://www.sciencedirect.com/science/article/pii/S106750270600209X>.
- [21] Dickinson, A. et al., 2010. Paediatric nurses' understanding of the process and procedure of double-checking medications. *Journal of clinical nursing*, 19(5-6), pp.728–35. Available at: <http://www.ncbi.nlm.nih.gov/pubmed/20500316> [Accessed January 6, 2016].
- [22] Cuevas, C., Neria, M. & Benavente, M., 2008. El sistema de información para la administración de medicamentos a pacientes hospitalizados. In *La gestión del medicamento en los Servicios de Salud. Informes SEIS (8)*. Pamplona: Sociedad Española de Informática de la Salud. Disponible en: <http://82.98.165.8/documentos/informes/secciones/adjunto1/05-SISTEMA-DE-INFORMACION.pdf>.
- [23] Hernández, M. & Andrés, J.L.P., 2001. *Sistemas automáticos de dispensación de medicamentos*, Combino Pharm. Available at: <http://books.google.com.ar/books?id=D403MwEACAAJ>.
- [24] Catley, C. & Frize, M., 2002. Design of a health care architecture for medical data interoperability and application integration. In *Engineering in Medicine and Biology*, 2002. 24th Annual Conference and the Annual Fall Meeting of the Biomedical Engineering Society EMBS/BMES Conference, 2002. *Proceedings of the Second Joint*. pp. 1952–1953 vol.3. Available at: [http://ieeexplore.ieee.org/xpl/login.jsp?tp=&number=10531111&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs\\_all.jsp%3Farnumber%3D10531111](http://ieeexplore.ieee.org/xpl/login.jsp?tp=&number=10531111&url=http%3A%2F%2Fieeexplore.ieee.org%2Fxppls%2Fabs_all.jsp%3Farnumber%3D10531111).
- [25] Long, A. et al., 2010. The Leapfrog CPOE Evaluation Tool: One Academic Medical Center's Experience. *PHSQ*. Disponible en: <http://psqh.com/the-leapfrog-cpoe-evaluation-tool>
- [26] Koliren, F. et al., 2007. The Effect of Computer-assisted Prescription on Critical Care Unit. Available at: <http://search.informit.com.au/documentSummary>.
- [27] Manrique-Rodríguez, S. et al., 2011. Bombas de infusión inteligentes: luces y sombras de una tecnología en desarrollo. *Medicina Clínica*, 137(8), pp.361–365. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0025775310001478>
- [28] Hope, C. et al., 2003. A tiered approach is more cost effective than traditional pharmacist-based review for classifying computer-detected signals as adverse drug events. *Journal of Biomedical Informatics*, 36(1–2), pp.92–98. Available at: <http://www.sciencedirect.com/science/article/pii/S1532046403000595>.
- [29] Martín, N. & Ceruelo, J., 2012. La gestión electrónica de la farmacoterapia. In *Manual de salud electrónica para directivos de servicios y sistemas de salud*. CEPAL. Available at: [http://82.98.165.8/documentos/informes/secciones/adjunto1/09\\_La%20gestion\\_electronica\\_de%20la\\_farmacoterapia.pdf](http://82.98.165.8/documentos/informes/secciones/adjunto1/09_La%20gestion_electronica_de%20la_farmacoterapia.pdf)
- [30] Martínez Bernabé, E. et al., 2014. Sistemas de soporte a la toma de decisiones clínicas en insuficiencia renal. *Farmacia Hospitalaria*, 38(3), pp.216–222. Available at: [http://scielo.isciii.es/scielo.php?script=sci\\_abstract&pid=S1130-63432014000300008&lng=es&nrm=iso&tlng=es](http://scielo.isciii.es/scielo.php?script=sci_abstract&pid=S1130-63432014000300008&lng=es&nrm=iso&tlng=es)
- [31] Sirot, E.J. et al., 2012. Therapeutic Drug Monitoring and Pharmacogenetic Tests as Tools in Pharmacovigilance. *Drug Safety*, 29(9), pp.735–768. Available at: <http://link.springer.com/article/10.2165/00002018-200629090-00001>.
- [32] Celi, A. et al., 2013. “Big Data” in the Intensive Care Unit. Closing the Data Loop. *American Journal of Respiratory and Critical Care Medicine*, 187(11), pp.1157–1160. Available at: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3734609/>.

- [33] Colman, E. et al., 2014. Learning from Big Data. *New England Journal of Medicine* journal, 370(23), pp.2161–2163.
- [34] Lehman, L. et al., 2011. Multiparameter Intelligent Monitoring in Intensive Care II (MIMIC- II): A public-access intensive care unit database. *Critical Care*, 39(February 2010), pp.952–960.
- [35] Lewis, N., 2015. Population Health Management Requires Better IT Tools. *InformationWeek*. Available at: <http://www.informationweek.com/healthcare/clinical-systems/population-health-management-requires-be/232901120>.
- [36] Murias, G. et al., 2010. Telemedicina: mejora de la calidad en la atención de los pacientes críticos desde la fase prehospitalaria hasta el servicio de medicina intensiva. *Medicina Intensiva*, 34, pp.46–55. Disponible en: [http://scielo.isciii.es/scielo.php?pid=S0210-56912010000100005&script=sci\\_arttext](http://scielo.isciii.es/scielo.php?pid=S0210-56912010000100005&script=sci_arttext)
- [37] Khunlertkit, A. & Carayon, P., 2013. Contributions of tele-intensive care unit (Tele-ICU) technology to quality of care and patient safety. *Journal of Critical Care*, 28(3), pp.315.e1–315.e12. Available at: <http://dx.doi.org/10.1016/j.jcrc.2012.10.005>.
- [38] Egan, M., 2006. Clinical dashboards: impact on workflow, care quality, and patient safety. *Critical care nursing quarterly*, 29(4), pp.354–361. Available at: <http://content.wkhealth.com/linkback/openurl?sid=WKPTLP:landingpage&an=00002727-200610000-00008>.
- [39] Breslow, J., 2005. The eICU® Solution: A Technology-Enabled Care Paradigm for ICU Performance. Available at: <http://www.ncbi.nlm.nih.gov/books/NBK22836/> [Accessed January 6, 2016].
- [40] Hamilton, D.K. & Shepley, M.M.C., 2010. *Design for Critical Care: An Evidence-based Approach* Routledge, ed., Elsevier/Architectural Press.
- [41] Lloyd, R.C., 2004. *Quality Health Care: A Guide to Developing and Using Indicators*, Jones and Bartlett Publishers.
- [42] Effken, J. a. et al., 2008. Clinical information displays to improve ICU outcomes. *International Journal of Medical Informatics*, 77(11), pp.765–777.
- [43] Dowding, D. et al., 2015. Dashboards for improving patient care: review of the literature. *International journal of medical informatics*, 84(2), pp.87–100.
- [44] Fundación Telefónica, 2008. Las TIC y el sector salud en Latinoamérica. Available at: [https://publiadmin.fundaciontelefonica.com/index.php/publicaciones/add\\_descargas?tipo\\_fichero=pdf&idioma\\_fichero=\\_&title=Las+TIC+y+el+sector+Salud+en+Latinoam%C3%A9rica&code=27&lang=es&file=las\\_tic\\_y\\_el\\_sector\\_salud\\_en\\_latinoamerica.pdf&\\_ga=1.94349726.222](https://publiadmin.fundaciontelefonica.com/index.php/publicaciones/add_descargas?tipo_fichero=pdf&idioma_fichero=_&title=Las+TIC+y+el+sector+Salud+en+Latinoam%C3%A9rica&code=27&lang=es&file=las_tic_y_el_sector_salud_en_latinoamerica.pdf&_ga=1.94349726.222).
- [45] Reason, J., 2000. Reason 2000 Human Error- Models and Management. *BMJ British Medical Journal*, 320, pp.768–770.
- [46] Sáez Crespo, R. & Gutierrez Covarrubias, R., 2008. Tecnologías aplicadas a la seguridad de la información. In *Seguridad de la información en entornos sanitarios*. Publicaciones SEIS, pp. 125–163.
- [47] Indarte, S. & Pazos, P., 2011. Estandares e interoperabilidad en salud electronica. CEPAL. Available at: [http://repositorio.cepal.org/bitstream/handle/11362/3938/S2011120\\_es.pdf?sequence=1](http://repositorio.cepal.org/bitstream/handle/11362/3938/S2011120_es.pdf?sequence=1).
- [48] Romano, M.J. & Stafford, R.S., 2011. Arch Intern Med -- Abstract: Electronic Health Records and Clinical Decision Support Systems: Impact on National Ambulatory Care Quality, January 24, 2011, Romano and Stafford 0 (2011): archinternmed.2010.527v1. *Archives of Internal Medicine*, p.archinternmed.2010.527-.

- [49] Kohn, L.T., Corrigan, J.M. & Donaldson, M.S., 2000. To Err Is Human: Building a Safer Health System. Available at: <http://www.nap.edu/catalog/9728/to-err-is-human-building-a-safer-health-system>.
- [50] Bañeres, J. et al., 2005. Los sistemas de registro y notificación de efectos adversos y de incidentes: una estrategia para aprender de los errores. *Revista de Calidad Asistencial*, 20(4), pp.216–222.
- [51] Farley, D.O. et al., 2008. Adverse-event-reporting practices by US hospitals: results of a national survey. *Quality and Safety in Health Care*, 17(6), pp.416–423. Available at: <http://qualitysafety.bmj.com/content/17/6/416.abstract>.
- [52] Pronovost, P.J. et al., 2008. Improving the value of patient safety reporting systems. In K. Henriksen, J. Battles, & M. Keyes, eds. *Advances in Patient Safety: New Directions and Alternative Approaches*. Agency for Healthcare Research and Quality. Available at: <http://www.ncbi.nlm.nih.gov/books/NBK43621/>.
- [53] Evans, S.M. et al., 2006. Attitudes and barriers to incident reporting: a collaborative hospital study. *Quality & Safety in Health Care*, 15(1), pp.39–43. Available at: <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC2563993/>.
- [54] Intensive Care Society, 2005. *The Intensive Care Society A Guide for Critical Care Settings Standards for critical incident reporting in critical care*, Available at: <http://www.ics.ac.uk/EasysiteWeb/getresource.axd?AssetID=456&type=full&servicetype=Attachment>.
- [55] Beckmann, U. et al., 1996. The Australian incident monitoring study in intensive care: AIMS-ICU. The development and evaluation of an incident reporting system in intensive care. *Anaesthesia and Intensive Care*, 24(3), pp.314–319.
- [56] Holzmüller, C.G. et al., 2005. Creating the web-based intensive care unit safety reporting system. *Journal of the American Medical Informatics Association : JAMIA*, 12(2), pp.130–139.
- [57] Lubomski, L.H. et al., 2004. Building a better incident reporting system: Perspectives from a multisite project. *Journal of Clinical Outcomes Management*, 11(5), pp.275–280.
- [58] SiNASP, 2015. *Información General del Sistema de Notificación y Aprendizaje para la Seguridad del Paciente*. Available at: [https://www.sinasp.es/SiNASP\\_InformacionGeneral.pdf](https://www.sinasp.es/SiNASP_InformacionGeneral.pdf).
- [59] Bañeres, J. et al., 2009. *Sistemas de registro y notificación de incidentes y eventos adversos*. Available at: [http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/pdf/excelencia/opsc\\_sp3.pdf](http://www.msssi.gob.es/organizacion/sns/planCalidadSNS/pdf/excelencia/opsc_sp3.pdf).



## Capítulo VII

# La seguridad transfusional y las tecnologías de la información y la comunicación

*Arturo Pereira Saavedra*



### Resumen

Al hablar de seguridad transfusional debe distinguirse entre la seguridad del producto sanguíneo (calidad y esterilidad) y la seguridad del proceso de la transfusión, tal como se lleva a cabo en los hospitales. Este último es muy sensible al error humano debido a la necesidad de realizar múltiples transcripciones de datos críticos, como la identidad del paciente, a la ausencia de control centralizado, a la coexistencia de procesos paralelos destinados a pacientes diferentes y a los lapsus inevitables del personal sanitario que pueden acabar en la transfusión incompatible de consecuencias graves.

El proceso de la transfusión se ha beneficiado poco de las tecnologías de la información y la comunicación (TIC) pues la única aportación destacable ha sido la incorporación de códigos de barras en la identificación del paciente y de los productos sanguíneos. Estos sistemas basados en códigos gráficos tienen numerosas limitaciones pues su capacidad para almacenar y renovar la información es baja, no eliminan la necesidad de acciones manuales y son poco útiles en algunos ambientes, como el quirúrgico, donde puede faltar la necesaria línea de visión directa entre el código y el lector.

Las tecnologías basadas en radiofrecuencia (RFID) superan esas limitaciones y es de esperar que contribuyan de un modo decisivo a la seguridad de la transfusión. Es importante que la implantación de sistemas RFID contemple todos los procesos hospitalarios que requieren la identificación del paciente y no sólo el de la transfusión.

## La transfusión sanguínea en terapéutica

La transfusión sanguínea es uno de los pilares sobre los que se asienta la medicina moderna, con una importancia comparable a la de los antibióticos, los quimioterápicos o el trasplante de órganos. En efecto, sin una transfusión segura y eficaz hubiera sido imposible el desarrollo de la mayoría de los tratamientos antineoplásicos, de los trasplantes de órganos y de muchas de las intervenciones quirúrgicas que hoy nos resultan habituales.

Además del importante papel que desempeña en la configuración de la medicina moderna, la transfusión sanguínea posee unas características peculiares que la distinguen de las otras terapéuticas médicas o quirúrgicas. Así, los componentes sanguíneos transfundidos sólo pueden obtenerse de la donación de sangre que realizan los ciudadanos de forma voluntaria. En España y en la mayoría de los países de nuestro entorno sociocultural, la donación de sangre es altruista y totalmente anónima pues ni el donante conocerá al receptor que se beneficiará de la donación ni este último sabrá de quién procede la sangre que le ha sido transfundida.

En contraste con ese carácter altruista, la transfusión posee la capacidad de transmitir enfermedades infecciosas gravísimas del donante al receptor, el ejemplo más dramático de las cuales fue la epidemia de sida transfusional que asoló la medicina transfusional durante la década de 1980 y principios de la siguiente. Además de la transmisión de enfermedades, la transfusión entraña otros riesgos debidos a la incompatibilidad inmunológica o de otro tipo entre el donante y el receptor. A modo de ilustración de esto último, conviene saber que si la transfusión se realizase al azar, sin pruebas de compatibilidad previas, más de la tercera parte de los receptores sufrirían complicaciones inmediatas muy graves, mortales en muchos casos.

Debido a estos dos últimos riesgos, pero principalmente a las consecuencias sanitarias, políticas y judiciales que siguieron a la epidemia de sida transfusional, la transfusión ha devenido la especialidad médica más regulada desde el punto de vista legal. En efecto, la transfusión y todo lo que la rodea ha de cumplir numerosas normativas emitidas por el Consejo de Europa, el Estado y las Comunidades Autónomas [1]. Además, ha de ajustarse a los requerimientos técnicos exigidos por las asociaciones científicas y profesionales. En España, tales requerimientos los fija el CAT (Comité de Acreditación de Centros y Servicios de Transfusión) [2], entidad que depende de la Sociedad Española de Hematología y Hemoterapia (SEHH) y de la Sociedad Española de Transfusión Sanguínea y Terapia Celular (SETS). En EEUU es la American Association of Blood Banks (AABB) [3] la que fija los estándares de calidad y en casi todos los demás países industrializados existe alguna entidad encargada de esa función.

Estas peculiaridades de la transfusión y en particular el contexto normativo son determinantes a la hora de establecer los mecanismos de seguridad transfusional pues éstos deberán ajustarse necesariamente a los requerimientos legales, los cuales siempre van retrasados con respecto a los avances de la medicina. Además, la normativa legal pone mucho más énfasis en los aspectos burocráticos ligados a la trazabilidad y el registro de productos y procesos que en los dirigidos a garantizar la seguridad de la transfusión. Así, por ejemplo, la capacitación del personal autorizado a transfundir y algunos aspectos críticos del proceso, como la identificación del paciente, quedan relegados al criterio de cada centro hospitalario. Por trazabilidad se entiende el registro detallado y sistemático del camino que ha seguido cada producto sanguíneo desde la donación hasta la transfusión. El motivo de tal registro es poder identificar al donante de sangre si el paciente presenta una infección que pueda atribuirse a la transfusión o, por el contrario, identificar al receptor si el donante presentase signos de una enfermedad transmisible tiempo después de la donación de sangre.

Otra característica de la transfusión, considerada aquí como sector sanitario, es el reparto de funciones entre los Bancos de Sangre Regionales, que en España se denominan de un modo equívoco “Centros de Transfusión”, y los “Servicios de Transfusión” hospitalarios. Corresponde a los primeros las funciones relacionadas con la obtención de las donaciones de sangre y de componentes sanguíneos, su análisis y procesamiento en los diversos derivados y su almacenamiento y

distribución a los hospitales. La legislación española impide la existencia de Bancos de Sangre de propiedad privada por lo que todos los existentes son de titularidad pública y dependen de los servicios de salud de las CCAA. Los Servicios de Transfusión están ubicados en los hospitales y suelen depender orgánicamente de los Servicios de Hematología. Ellos son los encargados de llevar a cabo las pruebas de compatibilidad, la selección de los componentes idóneos para cada paciente y todos los demás aspectos clínicos relacionados con la transfusión.

Esta división de funciones obliga a conceptualizar la seguridad transfusional en dos grandes componentes. Por una parte la *seguridad del producto*, que es responsabilidad directa de los Bancos de Sangre Regionales y, por extensión, de las autoridades sanitarias titulares de esos establecimientos y, por otra, la *seguridad del proceso* de la transfusión, la cual es responsabilidad de los hospitales y se engloba dentro del concepto más amplio de *seguridad clínica* aunque con las connotaciones que luego veremos.

## La seguridad transfusional

### Seguridad del producto

La separación de funciones entre Bancos de Sangre Regionales y Servicios de Transfusión permitió que a los primeros se les aplicasen criterios estrictos de control de calidad (good manufacturing practices) similares a los que se exigen a la industria farmacéutica o a la de productos alimentarios. El resultado ha sido impresionante. Si a principios de la década de 1980 el riesgo de transmisión transfusional del virus de la inmunodeficiencia humana (VIH) era de 1 por 100 unidades transfundidas en algunas áreas de Estados Unidos [4] y en España, a finales de esa década, el del virus de la hepatitis C (VHC) era también de 1:100 [5], ahora ambos riesgos son tan bajos que resulta imposible medirlos, han de estimarse mediante modelos matemáticos y se sitúan en el orden de uno por millón o por varios millones de unidades transfundidas [6]. Además se han desarrollado métodos de inactivación de gérmenes, aplicables por ahora sólo al plasma y a las plaquetas, que aunque son aún imperfectos, pues alteran las cualidades terapéuticas del producto, permiten augurar que los componentes sanguíneos lábiles (hematíes, plaquetas y plasma) tendrán un nivel de esterilidad comparable al alcanzado por los derivados plasmáticos manufacturados [7].

Así, pues, puede afirmarse que la seguridad del producto es muy grande en la actualidad aunque quede sujeta al riesgo imponderable de transmisión de enfermedades infecciosas emergentes para las que no existan aún métodos de detección. Aparte de los infecciosos, existen otros efectos adversos asociados al producto sanguíneo como, por ejemplo, el edema agudo de pulmón no cardiogénico (la *Transfusion-Related Acute Lung Injury* o TRALI de la bibliografía anglosajona) o la anafilaxia pero éstos no son más frecuentes que los que puedan atribuirse a cualquier medicamento de origen biológico.

### Seguridad del proceso

Al contrario de lo que ocurre con la seguridad del producto, la seguridad del proceso ha avanzado muy poco. Así, el riesgo de hemólisis aguda por incompatibilidad de grupo sanguíneo ABO, que casi siempre se debe a errores humanos, sigue en los mismos niveles que hace 40 años y constituye una de las causas principales de muerte por transfusión sanguínea [8]. De hecho, la causa del escaso avance en la seguridad del proceso se debe en parte al enorme progreso alcanzado en la seguridad del producto. En efecto, muchos expertos atribuyen la deficiencia del proceso a la asimetría que se da en la distribución de los recursos destinados a la seguridad transfusional, pues se siguen asignando a disminuir todavía más el riesgo de enfermedades infecciosas transmisibles por transfusión (EITT), que es ya muy bajo (seguridad del producto), en detrimento de las fases del proceso de la transfusión que resultan críticas para la prevención de errores de consecuencias fatales (seguridad del proceso) y en las que se profundizará más adelante [9][10].

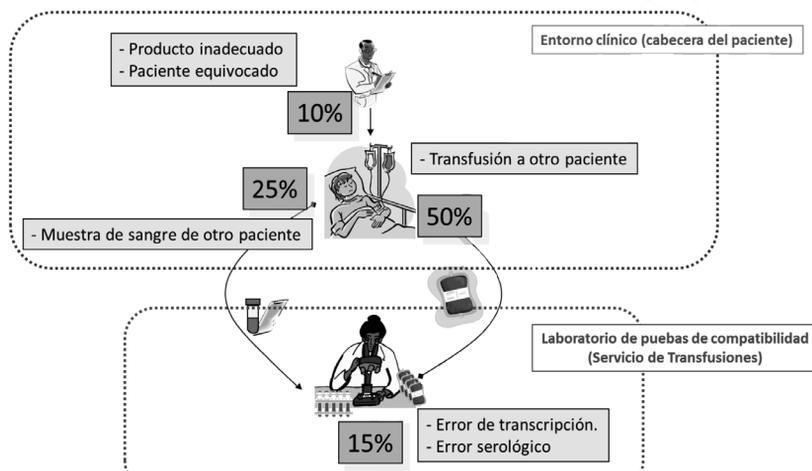
### Hemovigilancia

Con el fin de disponer de una información cuantitativa de los riesgos asociados a la transfusión, la mayoría de los países europeos han establecido sistemas de hemovigilancia de ámbito nacional o regional amplio que registran las complicaciones de esta terapéutica. En algunos países, como Francia, la declaración de efectos transfusionales adversos es obligatoria, como lo es en muchos países la de algunas enfermedades infecciosas. En otros, como la Gran Bretaña, la declaración es voluntaria pero el grado de cumplimiento es muy elevado. En España existen sistemas de hemovigilancia de declaración voluntarios y bien rodados en Cataluña y en el País Vasco, mientras que en el resto de las CCAA están menos desarrollados o no se han implantado aún. El Ministerio de Sanidad, Servicios Sociales e Igualdad publica

cada cierto tiempo los resultados agregados a nivel nacional aunque la fiabilidad de tales datos es dudosa por falta de sistematización en la mayoría del territorio [11]. Esa cuantificación de los riesgos de la transfusión proporcionada por los sistemas de hemovigilancia debería guiar la asignación de recursos hacia las deficiencias más notorias y potencialmente mejorables pero carecemos de pruebas de que eso sea así.

## El proceso de la transfusión sanguínea

El proceso de la transfusión comprende las fases y tareas que van desde la prescripción por parte del médico responsable del paciente hasta que este último recibe el componente sanguíneo indicado (véase Figura 7.1). Aunque la seguridad de este proceso se suele identificar con la realización de las pruebas de laboratorio de compatibilidad transfusional, lo cierto es que los principales puntos críticos quedan fuera del laboratorio de compatibilidad y del Servicio de Transfusiones. En efecto, la experiencia cotidiana y la bibliografía confirman que el error humano es la principal causa de accidentes transfusionales graves y que tal error ocurre con mucha más frecuencia en el entorno de la cabecera del paciente que en el laboratorio de compatibilidad transfusional.



**Figura 7.1.** Representación esquemática del proceso de la transfusión. Los porcentajes indican la fracción del total de errores que se producen en cada fase del proceso.

El proceso de la transfusión tiene unas peculiaridades que lo hacen particularmente vulnerable a la comisión de errores. Así, se producen múltiples transcripciones de datos críticos, como la identidad del

paciente, que pasa de la mente del médico al formulario de solicitud de transfusión, y de éste a los tubos con las muestras de sangre del paciente en las que se basará la compatibilidad, así como a las hojas de trabajo y a los registros del Servicio de Transfusiones. Luego, esos datos de identificación han de ligarse a un producto sanguíneo concreto que es el que volverá a la cabecera del paciente para ser transfundido.

No es raro, además, que coexistan múltiples códigos diferentes como el número de historia clínica, el de admisión, el asignado a la muestra de sangre del paciente, el que emplee el Servicio de Transfusiones, que puede ser diferente de los anteriores, y el de la unidad de sangre seleccionada para el paciente. Al final, todos esos códigos han de coincidir para garantizar que el enfermo reciba la bolsa de sangre correcta. Además, en el proceso de la transfusión intervienen muchas personas diferentes, ninguna de las cuales tiene el control de todo el proceso, y en los grandes hospitales no es raro que se estén procesando varias transfusiones a la vez, todo lo cual constituye un terreno abonado para la comisión de errores. A ello tenemos que añadir el deterioro de la atención que suele acompañar a las tareas repetitivas, el cual afecta sobre todo al personal del Servicio de Transfusiones, y los imponderables de la práctica clínica que puedan darse en la cabecera del paciente y que son causa frecuente de distracciones y lapsus de consecuencias a veces muy graves.

Muchas de las características que acabamos de mencionar son comunes a otros procesos que se llevan a cabo a diario en los hospitales, como la dispensación de medicamentos, las pruebas diagnósticas o las exploraciones invasivas, por lo que la seguridad transfusional debe considerarse dentro del ámbito, más extenso, de la seguridad clínica del paciente hospitalizado. No obstante, la transfusión es peculiar en el sentido de que una vez desencadenado el proceso mediante la solicitud cursada por el médico, éste ya no vuelve intervenir y el proceso funciona de modo casi automático en manos de personal sanitario no facultativo. El error en una prueba de laboratorio diagnóstica, como la cifra de glucemia o la de leucocitos (p. ej., porque la muestra de sangre proceda de otro paciente), tendrá que pasar por el criterio del médico que interpreta el resultado antes de que pueda tener repercusiones negativas sobre el paciente. En cambio, el mismo tipo de error en el proceso de la transfusión puede llevar a que el paciente reciba una unidad de sangre incompatible, pues ni el laboratorio de compatibilidad, ni el médico que ha indicado la transfusión, ni la enfermera que la realizará tienen medios para detectar el error en todos los casos.

Los sistemas de hemovigilancia que mencionábamos más arriba no están diseñados para registrar la casuística y la naturaleza de los errores que se producen en el proceso de la transfusión. No obstante, es bien conocido que algunas de las principales causas de morbimortalidad que sí registra la hemovigilancia, como es el caso de la transfusión incompatible, suelen estar producidas casi siempre por errores humanos. La bibliografía tampoco aporta una información útil sobre la frecuencia, la naturaleza y las consecuencias de los errores que se cometen en el ámbito de la transfusión por lo que debe recurrirse al conocimiento menos estructurado de los especialistas en Hemoterapia.

En la opinión del autor de este artículo el error humano es frecuente en el proceso de la transfusión y afecta sobre todo al personal veterano, quizá porque es el más propenso a los comportamientos automáticos. No obstante, la frecuencia del error transfusional no es superior a la del que pueda acontecer en la administración de medicamentos, algunos de los cuales como los citostáticos, las infusiones de potasio o de anticoagulantes o la insulina, por citar sólo algunos, pueden acarrear consecuencia tanto o más graves que el error transfusional.

Desafortunadamente, la ausencia de registros amplios de errores, incidentes y “cuasi-incidentes” impide cualquier comparación objetiva entre los que atañen a la transfusión y los relacionados con otros procesos. En el famoso informe del Instituto de Medicina de EEUU, “To err is human” [12], los errores de transfusión no estaban cuantificados por separado de los asociados a los medicamentos en general, por lo que es de suponer que eran comparativamente infrecuentes. En cambio, en un hospital canadiense de 1200 camas en el que se llevó a cabo un registro concienzudo de los errores transfusionales cometidos entre los años 2005 y 2010, se contó un total de 15134 errores (¡215 por mes!) aunque sólo 23 de ellos tuvieron repercusión sobre el paciente [13]. Los registros de hemovigilancia correspondientes al año 2013 muestran que la incidencia de transfusión incompatibles fue de 1:94.000 transfusiones de hematíes en España [11], 1:267.000 en Francia [12] y 1:288.000 en el Reino Unido [13]. Aunque estas cifras recogen sólo un tipo de error y deben considerarse, además, como la “punta del iceberg” del total de los errores transfusionales, son lo suficientemente pequeñas como para permitir afirmar que los errores transfusionales son bastante más infrecuentes que los relacionados con las terapéuticas medicamentosas.

En la Tabla VII.1 se resumen los principales factores que contribuyen a la inseguridad del proceso de la transfusión. Afortunadamente, la mayoría de las deficiencias mostradas en la tabla son susceptibles de corrección mediante la aplicación de las tecnologías de la información y la comunicación (TIC). En efecto, si en algo son insuperables los sistemas informáticos es en su capacidad para transferir y gestionar datos con una fiabilidad absoluta y para repetir cualquier tarea *ad infinitum* libre de errores.

<b>Tabla VII.1. Factores que contribuyen a la inseguridad del proceso de la transfusión.</b>
Procedimientos mal diseñados que propenden al error o dificultan su detección y corrección
Falta de procedimientos normalizados de trabajo
Métodos de identificación del paciente deficientes
Ausencia de un control centralizado de todas las fases del proceso que alerte cuando se haya obviado alguna de ellas o se detecten errores o incongruencias
Falta de sistemas de ayuda al médico prescriptor que eviten los errores de indicación y la prescripción al paciente equivocado
Múltiples transcripciones de datos críticos que con frecuencia se llevan a cabo de modo manual

## Contribución de las TIC a la seguridad del proceso de la transfusión

Los sistemas informáticos de gestión de transfusiones (SIT) son viejos conocidos de los Bancos de Sangre y de los Servicios de Transfusiones a los que llegaron hace más de tres décadas, mucho antes que a otros departamentos hospitalarios. Sin embargo, su contribución a la seguridad transfusional ha sido prácticamente nula hasta hace poco y aún ahora es menor de lo que debiera. Esto se debe a que los SIT están diseñados para llevar a cabo el registro y la trazabilidad veraces de los componentes sanguíneos y cumplir con los requisitos legales y estándares que regulan esas funciones y para poco más [2][3][16]. Suelen ser sistemas cerrados, de carácter propietario, poco amigables con el usuario y con escasas posibilidades de interconexión con los sistemas informáticos hospitalarios (HIS) y mucho menos con dispositivos móviles. Cuando se requiere tal conexión suele tener que recurrirse a interfaces o aplicativos desarrollados por terceros. Sólo recientemente algunos fabricantes han empezado a incorporar los estándares de mensajería que permiten la interconexión con los HIS. En cualquier caso, los SIT actuales quedan muy lejos de poder constituirse en los gestores del control centralizado del proceso de la transfusión al que hacíamos referencia más arriba.

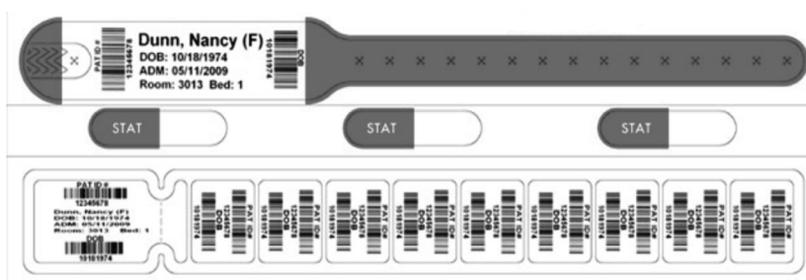
Un error frecuente, por sorprendente que parezca, es que el médico prescriba la transfusión al paciente equivocado. Hay dos factores que contribuyen a este tipo de error. Por una parte, la despersonalización que sufre el paciente al ingresar en el hospital, cuando deja de ser conocido por su nombre para pasar a serlo por el número de la habitación y cama que ocupa, y el hecho de que las prescripciones se realicen cada vez con más frecuencia en la cabecera del PC en lugar de la cabecera del enfermo.

Para contribuir a reducir este tipo de error se ha desarrollado la prescripción electrónica que permite informar al médico de datos claves del paciente, transcribe la identidad de éste sin errores e incluso puede incorporar sistemas inteligentes que ayuden a que la indicación se ajuste a los criterios establecidos. Estas solicitudes pueden transferirse por vía electrónica al SIT pero es necesario que se acompañen de la muestra de sangre del paciente. Además, la legislación española obliga a que consten en la solicitud la identificación del médico prescriptor y la de la enfermera que ha extraído la muestra de sangre, motivos por los que resulta difícil prescindir del soporte en papel salvo en los hospitales donde esté reconocida la firma electrónica del personal sanitario y se haya protocolizado de manera estricta la correspondencia entre el tubo con la muestra de sangre y el formulario de solicitud de transfusión.

En el área de la identificación de los pacientes, el sistema más extendido es de la pulsera con los datos de filiación del paciente y un código numérico único que se reproduce en varias etiquetas autoadhesivas que se transfieren manualmente al impreso de solicitud y al tubo con la muestra de sangre para las pruebas de compatibilidad. El Servicio de Transfusiones transfiere luego ese código a la bolsa del producto sanguíneo (manualmente o a través del SIT), lo que permite el chequeo con lector de código de barras en la cabecera del paciente en el momento de la transfusión. La función principal de este sistemas de pulseras es asegurar que el tubo con la muestra de sangre del paciente que se ha empleado en la pruebas de compatibilidad procede de la misma persona a la que luego se transfundirá la bolsa de sangre compatible.

Existen diferentes modelos de pulseras en el mercado pero todas poseen funcionalidades similares. No se aprovecha la pulsera de identificación que pueda llevar el paciente desde su ingreso porque es

necesario disponer de las etiquetas autoadhesivas que se transfieren al tubo de sangre y al impreso de solicitud. Las principales deficiencias de este sistema son su aplicabilidad exclusiva a la transfusión y el que parte de la transferencia de datos siga realizándose de modo manual. La Figura 7.2 muestra algunos ejemplos de tales pulseras.



**Figura 7.2.** Ejemplo de pulsera destinada a la identificación del paciente candidato a recibir una transfusión.

Por su parte, las bolsas de sangre vienen identificadas con una etiqueta en la que los datos principales están representados mediante códigos de barras para facilitar su transcripción electrónica (véase Figura 7.3). En la actualidad, la mayoría de los Bancos de Sangre españoles han adoptado el estándar ISBT 128, el cual es un sistema internacional de codificación de productos sanguíneos en el que cada bolsa posee un conjunto de códigos que la convierten en irreplicable en cualquier otro banco de sangre nacional o extranjero (ISBT es el acrónimo inglés de la Sociedad Internacional de Transfusión Sanguínea; [17]). La transcripción mediante lectores de código de barras resulta esencial en el sistema ISBT 128 pues ha de tenerse en cuenta que el identificador único de la donación de sangre está constituido por una cadena alfanumérica de 16 caracteres a la que se debe añadir otra con ocho o más caracteres que identifica el tipo de producto sanguíneo.

Los mayores inconveniente de este sistema basado en códigos de barra lineales es la gran densidad de códigos presentes en la etiqueta (véase Figura 7.3), lo que requiere lectores manuales y mucha atención por parte del usuario, y que cualquier dato adicional obligará a añadir un nuevo código de barras. Estas limitaciones pueden sortearse en parte mediante el empleo de códigos (tags) bidimensionales.



**Figura 7.3.** Ejemplo de etiqueta identificativa de una unidad de concentrado de hematíes. Una vez asignada al paciente se le adherirá al dorso otra etiqueta con los datos identificativos del paciente y los correspondientes códigos de barras (número de historia clínica, número de la pulsera, etc).

Los sistemas de identificación basados en código de barras contribuyen a disminuir los errores de identificación pero poseen limitaciones importantes. Así, necesitan una línea de visión directa entre el lector y el código, lo que no siempre es posible como, por ejemplo, cuando la pulsera de identificación del paciente queda bajo el campo estéril durante una intervención quirúrgica. La lectura de código de barras no permite el procesamiento simultáneo por lotes tanto de peticiones como de productos sanguíneos pues los códigos tienen que leerse

uno a uno. No debe olvidarse, además, que las bolsas de plástico de los productos sanguíneos son flexibles y susceptibles, por tanto, de arrugarse precisamente donde están impresos los códigos. Además, los cambios de temperatura desde la de almacenamiento de la sangre (2°-6° C) hasta la del ambiente en el que suele procesarse la distribución pueden condensar humedad sobre la etiqueta, lo que dificulta aún más su lectura.

Los sistemas de identificación por radiofrecuencia (RFID en el acrónimo inglés) soslayan muchas de las dificultades arriba mencionadas y llevan camino de convertirse en el método estándar de aseguramiento del proceso de la transfusión. Los sistemas RFID consisten en chips que se comunican mediante ondas de radio [18]. Estos chips pueden ser pasivos, los cuales sólo responden cuando son interrogados, o activos, que aparte poder almacenar datos son los emisores de energía que interrogan a los chips pasivos. Estos chips activos pueden colocarse en la pulsera de identificación del paciente, en los dispositivos móviles utilizados por el personal sanitario o en dispositivos fijos, denominados arcos, que pueden situarse en lugares estratégicos como la entrada a los quirófanos, al Servicio de Transfusiones o a las cámaras de almacenamiento de los productos sanguíneos.

Un diseño sencillo consistiría en incorporar un chip pasivo a la etiqueta de la bolsa de sangre y cargarlo en el Banco de Sangre con toda la información que consta en la etiqueta (identificador único, tipo de producto, grupo sanguíneo, fechas de producción y caducidad, etc.). En el Servicio de Transfusiones se le añadiría la información correspondiente al paciente al que va destinada la bolsa (número de historia clínica, código de seguridad de la pulsera, etc.). En la cabecera del paciente, el personal sanitario utilizaría un dispositivo móvil con un chip activo para interrogar y confrontar entre sí los datos del chip incorporado en la etiqueta de la bolsa y el de la pulsera del paciente.

La RFID no requiere una línea de visión directa entre el chip y el lector, la capacidad de almacenamiento, adición y reescritura de datos es muy superior a la que permiten los códigos gráficos y permiten el procesamiento simultáneo de múltiples productos. Esto último es de gran ayuda en la gestión de la distribución y la recepción de pedidos entre el Banco de Sangre Regional y los Servicios de Transfusiones hospitalarios. Un inconveniente asociado a la RFID es la interferencia

que puede producirse entre diversos chips cuando estén próximos entre sí. No obstante, la interferencia es fácil de soslayar mediante bucles de retroalimentación, la triangulación de los chequeos o la implantación de filtros de radiofrecuencia.

Si bien el grado de implantación de la RFID es aún escaso en el ámbito de la transfusión, la Sociedad Internacional de Transfusión Sanguínea ha publicado los criterios que deberían guiar la implantación de la RFID así como los estándares de compatibilidad con el sistema de códigos ISBT 128 [19]. La FDA norteamericana definió en 2013 las condiciones que deben reunir los sistemas de RFID aplicados a la transfusión [20], lo que ha abierto la puerta al desarrollo y comercialización de aplicativos destinados a ese uso. En España, algunos Bancos de Sangre Regionales están desarrollando sistemas propietarios en colaboración con empresas tecnológicas. Es muy probable, pues, que en los próximos años las tecnologías basadas en RFID desplacen a los códigos de barras.

No obstante, parece que el desarrollo de la RFID peca de la misma deficiencia que los sistemas de seguridad transfusional que le han precedido y ésta es la falta de extensibilidad vertical y horizontal. En efecto, para que resulte eficiente, un sistema basado en RFID ha de tener una aplicabilidad vertical entendiendo por tal todo el proceso que va desde la donación de sangre hasta la transfusión al paciente. En el sentido horizontal, el mismo sistema ha de ser aplicable a todos los procesos que se realizan en el hospital y no sólo al de la transfusión. Tales procesos incluyen las exploraciones complementarias, como el laboratorio o las pruebas de imagen, las exploraciones invasivas (p.ej. biopsia, endoscopia, etc.) y las intervenciones quirúrgicas, sin olvidar la localización del paciente dentro del hospital en tiempo real y la gran ayuda que puede proporcionar en la asignación de costes. Sin embargo, no parece que los sistemas de RFID que se están desarrollando en la actualidad contemplan esa amplitud de horizontes en cuanto a la aplicabilidad.

## Conclusiones

La seguridad de los productos sanguíneos en cuanto a la transmisión de enfermedades infecciosas es muy elevada. No lo es, en cambio, la del proceso de la transfusión puesto que resulta muy sensible al error humano, el cual puede llevar a la transfusión incompatible. Las TIC

contribuyen a incrementar la seguridad del proceso de la transfusión al evitar la transcripción manual de datos críticos, como los de filiación del paciente, al confrontar de modo automático la identificación de éste con la del producto sanguíneo y al proporcionar un control centralizado de todo el proceso. Los sistemas basados en RFID son los más adecuados para esa función aunque su implementación es aún escasa. La implantación ideal sería aquella que permitiese la trazabilidad completa del producto sanguíneo, desde la donación a la transfusión, y fuera aplicable a otros procesos hospitalarios aparte del de la transfusión.

## Bibliografía

- [1] Pereira A. La seguridad transfusional. *JANO*, Nov 2011; 87-92.
- [2] Fundación CAT. Estándares de Acreditación en Transfusión Sanguínea [Monografía en internet] [acceso 10 de septiembre de 2015] Disponible en:<http://www.catransfusion.es/estandares/index.html>.
- [3] Standards for Blood Banks and Transfusion Services (29th ed). American Association of Blood Banks. 2014.
- [4] Busch MP, Young MJ, Samson SM, Mosley JW, Ward JW, Perkins HA. Risk of human immunodeficiency virus (HIV) transmission before the implementation of HIV-1 antibody screening. *Transfusion*. 1991;31:4-11.
- [5] Barrera JM, Bruguera M, Ercilla MG, Sánchez-Tapias JM, Gil MP, Costa J, et al. Incidence of non-A, non-B hepatitis after screening blood donors for antibodies to hepatitis C virus and surrogate markers. *Ann Intern Med*. 1991;115:596-600.
- [6] Dwyre DM, Fernando LP, Holland PV. Hepatitis B, hepatitis C and HIV transfusion-transmitted infections in the 21st century. *Vox Sang*. 2011;100:92-8.
- [7] Klein HG, Anderson D, Bernardi MJ, Cable R, Carey W, Hoch JS, et al. Pathogen inactivation: making decisions about new technologies. Report of a consensus conference. *Transfusion*. 2007;47:2338-47.
- [8] Davenport RD. Hemolytic Transfusion Reactions. En: Simon TL, Snyder EL, Solheim BG, Stowell CP, Strauss RG, Petrides P, editors. *Rossi's principles of transfusion medicine*. Chichester, UK: Wiley-Blackwell, 2009. p. 811-25.
- [9] Dzik WH. New technology for transfusion safety. *Br J Haematol*. 2006;136:181-90.
- [10] Pereira A. Risk Management. En: Barbara AJA, Regan FAM, Contreras M, editors. *Transfusion microbiology*. Cambridge, UK: Cambridge University Press; 2008. P. 341-61.
- [11] Unidad de hemovigilancia. Informe 2013. [Monografía en internet] Ministerio de Sanidad, Consumo e Igualdad del Gobierno de España [acceso 30 de Septiembre de 2015] Disponible en: <http://www.msssi.gob.es/profesionales/saludPublica/medicinaTransfusional/hemovigilancia/docs/Informe2013.pdf>.
- [12] Kohn LT, Corrigan JM, Donaldson MS, editores, To err is human. National Academies Press, Washington DC, EEUU; 2000.
- [13] Maskens C, Downie H, Wendt A, Lima A, Merkle L, Lin Y, Callum J. Hospital-based transfusion error tracking from 2005 to 2010: identifying the key errors threatening patient transfusion safety. *Transfusion* 2014, 54: 66-73.
- [14] Agence national de sécurité du médicament et des produits de santé. Rapport d'activité Hemovigilance 2013 ([http://www.ansm.sante.fr/var/ansm\\_site/storage/original/application/8a2c3c478172fcf6e027742aed130adf.pdf](http://www.ansm.sante.fr/var/ansm_site/storage/original/application/8a2c3c478172fcf6e027742aed130adf.pdf). Consultado el 10 de septiembre de 2015).

- [15] PHB Bolton-Maggs (Ed), D Poles, A Watt and D Thomas on behalf of the Serious Hazards of Transfusion (SHOT) Steering Group. The 2013 Annual SHOT Report [Monografía en internet] The SHOT website. [acceso 10 de septiembre de 2015. Disponible en: [www.shotuk.org/wp-content/uploads/Annual-SHOT-Report-2013-Bookmarked.pdf](http://www.shotuk.org/wp-content/uploads/Annual-SHOT-Report-2013-Bookmarked.pdf).
- [16] Guidelines for the specification, implementation and management of information technology (IT) systems in hospital transfusion laboratories (working document) [Monografía en internet]. British Committee for Standardisation in Haematology [Acceso 10 de Septiembre de 2015]. Disponible en: [http://www.bcshguidelines.com/documents/IT\\_guidelinesAug14\\_final\\_v2.pdf](http://www.bcshguidelines.com/documents/IT_guidelinesAug14_final_v2.pdf).
- [17] ISBT 128: the global information estándar for medical product of human origin. [sede web] ISBT website [acceso 10 de Septiembre de 2015]. Accesible en: [www.iccbba.org](http://www.iccbba.org).
- [18] Roberts CM. Radiofrequency identification (RFID). *Computers & Security* 2006; 25: 18-26.
- [19] Knels R, Hohberger C, Davis R, Holcombe J, Ashford P, Bidet F et al. Guidelines for the Use of RFID Technology in Transfusion Medicine. *Vox Sang* 2010; 98: Supl 2.
- [20] Transfusion Medicine RFID Consortium. iTrace for blood centers receives FDA clearance [Monografía web] [acceso 10 de Septiembre de 2015]. Accesible en: [www.transfusionmedicinerfid.org/project-news/updates/121-itrace-for-blood-centers-receives-fda-510k-clearance.html](http://www.transfusionmedicinerfid.org/project-news/updates/121-itrace-for-blood-centers-receives-fda-510k-clearance.html).

## Capítulo VIII

# La seguridad de la información desde la perspectiva de la seguridad del paciente

*Raúl Martínez Santiago*



### Resumen

Seguridad es sinónimo de confianza y se debe hacer todo lo posible para evitar que ésta se rompa o al menos, si se rompe, recuperarla lo antes posible. Esto es extensible tanto a la seguridad clínica como a la seguridad de la información, que deben garantizarse al máximo.

La seguridad de la información, tanto en su vertiente técnica como normativa, debe ser siempre un elemento de suma y no de resta en la seguridad clínica. Como algunos aspectos de la seguridad de la información pueden ser contrarios a la seguridad de los pacientes, siempre se deben ponderar los distintos aspectos que intervienen en su ejecución, para lograr un equilibrio que por un lado asegure la seguridad de la información y por otro no ponga en peligro la seguridad de los pacientes. Por ejemplo, proteger con controles excesivos el acceso a la información clínica (confidencialidad, un componente de la seguridad de la información) puede ser perjudicial para la seguridad del paciente, si se dificulta tanto ese acceso que los clínicos desisten de consultar información que puede ser trascendental para la asistencia.

La seguridad de la información debe aportar calidad, tecnología y organización en la parte técnica, y garantías y adaptación a las necesidades en la parte normativa, para ser de utilidad a la práctica clínica.

Los incidentes de seguridad se deben registrar para analizar y detectar las causas, resolver los problemas y tomar medidas para que no vuelvan a ocurrir.

## Introducción

La sociedad en general tiene una actitud reactiva con muchos asuntos, es decir, sólo se percata de ellos cuando causan problemas o molestias. Con los sistemas de información en general y con su seguridad en particular ocurre lo mismo, nadie o muy poca gente los tiene en cuenta hasta que fallan o se producen errores. Por este motivo, los profesionales de estos sectores afirmamos que cuando no se habla de nuestra labor es positivo, porque eso significa que las cosas funcionan y no afectamos al resto de personas que dependen en parte de nosotros. En el mundo sanitario, con la seguridad clínica de los pacientes sucede algo parecido a lo que se acaba de describir.

El objetivo de este capítulo es reflexionar sobre lo que aporta la seguridad de la información desde la perspectiva de la seguridad clínica del paciente. Para alguien no familiarizado con estos términos puede resultar confuso el uso recurrente de la palabra seguridad. Siempre que se habla de seguridad, se pretende reflejar la ausencia de peligro o riesgo de algo. En este capítulo se va a analizar la relación entre la seguridad de la información y la del paciente. En principio, parece positivo para el paciente que no existan peligros relacionados con la información, pero como se detallará más adelante y como ya se ha indicado antes, en algunos casos se da la paradoja de que no siempre una mayor seguridad de la información se acompaña de una mayor seguridad para el paciente.

El término “seguridad de la información” incluye cualquier tipo de soporte, pero este capítulo se centrará en el electrónico, por lo que más bien se debería hablar de la seguridad de los sistemas de información o seguridad informática más que de la seguridad de la información.

En todo caso, podemos definir la seguridad de la información como una garantía de confianza en la información. La seguridad informática debe tener dos objetivos: la disponibilidad de la información y la protección de datos. La seguridad del paciente, por otra parte, la entendemos como una asistencia sanitaria sin sucesos, eventos o errores evitables o prevenibles [1].

En la mayoría de las ocasiones, las acciones evitables que producen incidentes de seguridad vienen provocadas por errores de la condición humana. Normalmente, en el caso de los sistemas de información, estas situaciones ocurren por la falta de controles suficientes en los desarrollos realizados que permitan su prevención.

La seguridad clínica del paciente se puede poner en peligro si los sistemas de información no cuentan con una seguridad lógica y física adecuada; se deben diseñar para evitar los errores humanos en la medida de lo posible, porque no podemos cambiar la condición humana, pero sí podemos cambiar los sistemas con los cuales los humanos trabajan [2].

Otras situaciones también provocadas por la condición humana son las explotaciones de las vulnerabilidades existentes en los sistemas que se denominan agujeros de seguridad.

En este capítulo se van a describir en primer lugar los aspectos técnicos de la seguridad de la información, analizando por un lado características como la integridad de los datos que se maneja y la disponibilidad de dicha información; y por otro la accesibilidad y la confidencialidad. Se concluirá que si todos ellos son ejecutados de forma correcta son acciones favorables para el paciente, y se reflejará la importancia de definir un modelo que garantice la precisión de la información generada y una arquitectura que asegure la disponibilidad de los datos en tiempo y forma.

En segundo lugar, se analizarán los aspectos normativos que es importante conocer para desarrollar una política de seguridad adecuada en las organizaciones.

Por último, como ya se ha comentado, se describirán casos de posibles paradojas donde existen situaciones de riesgo para la práctica clínica por la rigidez de la normativa que garantiza la protección de datos personales.

## Aspectos técnicos de la seguridad de la información

A continuación se tratarán los aspectos técnicos que sustentan la seguridad de la información, y que son la integridad, la disponibilidad, la confidencialidad y la accesibilidad. La accesibilidad es un término a medio camino entre la disponibilidad y la confidencialidad; no todo lo disponible es accesible, sólo cuando la confidencialidad lo permita en cada caso.

Siempre que se contemplen estos términos en positivo, la seguridad estará garantizada; en cambio, si se usan en negativo la seguridad estará condicionada. Como avance para entender estos términos, la integridad hace referencia al acceso a la información real y completa, la disponibilidad a la posibilidad de acceder a la información y la confidencialidad al acceso pertinente. Aunque se tratarán de forma independiente, en muchos casos son componentes relacionados. Por ejemplo, la integridad puede verse alterada tanto por la falta de disponibilidad como de confidencialidad.

Para entender mejor lo anterior vamos a utilizar un símil sobre algo conocido por todos. La información será el contenido de una caja depositada en un banco y los aspectos técnicos de la seguridad tendrán la siguiente correspondencia: por un lado la disponibilidad consistirá en las necesidades de acceso a esa caja, como por ejemplo el horario en el que necesitamos que el banco esté abierto y la posibilidad de desplazarnos al lugar donde se encuentra la caja; la confidencialidad define a quién y con qué criterios se facilita la llave para acceder a esa caja; y la integridad se corresponde con la certeza o garantía de que el contenido de la caja no cambia, es decir, si se había depositado oro de ley, que tengamos un certificado que nos asegure que es el mismo oro de ley. En la Tabla VIII.1 se muestra una descripción de las garantías a cubrir por cada aspecto técnico y una palabra clave para aplicarlo de forma exitosa.

<b>Tabla VIII.1. Aspectos técnicos de la seguridad de la información.</b>		
<b>Aspecto</b>	<b>Garantías</b>	<b>Palabra clave</b>
Integridad	Acceso a la información original y correcta	Calidad
Disponibilidad	Acceso en cualquier momento que se demande	Tecnología
Confidencialidad	Acceso sólo a la información autorizada	Organización

La integridad se relaciona con la calidad porque depende de la excelencia aplicada en la gestión de la información, la disponibilidad se vincula a la tecnología porque es totalmente dependiente de ésta, y la confidencialidad se corresponde con la organización porque es muy importante establecer claramente las reglas de acceso a la información.

Uno de los argumentos que utilizan algunos profesionales para no usar la historia clínica electrónica es precisamente que la seguridad de la información no es la adecuada, es decir, que la información no es la que corresponde, que los sistemas fallan y no son accesibles, o que la confidencialidad les impide realizar su trabajo.

Para la gestión de la seguridad de la información existen estándares como la norma ISO 27001, basada en la gestión de riesgos y en la mejora continua de las organizaciones<sup>29</sup>, y guías de buenas prácticas como COBIT 5, que contiene un módulo específico de la seguridad de la información<sup>30</sup>. En ambos casos, el apoyo de la dirección de las compañías es vital para llevar a cabo estas iniciativas.

### Integridad

En primer lugar trataremos la integridad de la información, a pesar de que es el aspecto al que menos importancia se le da porque a priori parece el más fácil de conseguir, o se da por supuesto al menos.

Se entiende por integridad<sup>31</sup> de la información que los datos registrados previamente y los recuperados con posterioridad deben ser los mismos, sin que se haya producido ninguna modificación no controlada, pudiéndose además verificar la veracidad de los datos.

---

<sup>29</sup> Asociación Española de Normalización y Certificación (AENOR). Norma UNE-ISO/IEC 27001:2007.

<http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0040067&PDF=Si#.VuqDwtBciVA>.

<sup>30</sup> Information Systems Audit and Control Association (ISACA). COBIT 5. <http://www.isaca.org/COBIT/Pages/default.aspx>.

<sup>31</sup> No se debe confundir con la integridad referencial en las bases de datos, que tiene un objetivo similar pero no idéntico. En este ámbito se persigue, por ejemplo, que si un mismo campo está definido en dos tablas, los valores de este campo siempre deben existir y ser iguales tanto en la tabla maestra del campo como en la relacionada.

La integridad se debe salvaguardar durante todas las etapas del ciclo de vida de la información:

- Generación de los datos. La inserción de datos puede producirse manualmente en el propio sistema, generarse de forma automática e incluso provenir de un sistema externo. En el último caso, un riesgo importante a tener en cuenta es la duplicidad de la información en varios sistemas, situación que no es recomendable por demandar un alto nivel de sincronización; se debe respetar el principio de dato único. Es importante registrar la fecha y hora exactas de la inserción.
- Almacenamiento. Ocurre de forma simultánea a la generación de los datos pero tiene entidad propia por ser una capa específica de los sistemas.
- Uso. La información se puede consultar o modificar guardando rastro de cuándo, cómo y quién ha consultado o modificado qué datos.
- Archivo. Se debe garantizar la consistencia de los datos replicados. Es decir, que los datos que realmente disponemos en las copias de seguridad, independientemente del formato, sean correctos y se correspondan con los originales.
- Recuperación de datos. En esta etapa se deben definir medidas de prevención, como las pruebas periódicas de recuperación de datos para verificar que la información recuperada es la esperada para los casos en que se necesite realizar esta operación.
- Borrado y destrucción de datos. En este punto son importantes dos factores: la custodia de la información hasta que desaparece y la certificación de que dicha información ha sido eliminada.

Los riesgos asociados a la pérdida o manipulación indebida de la información son mayores cuanto mayor es el valor de ésta. Uno de estos riesgos son los ataques que se producen en la red. En el caso concreto de los ataques contra la integridad de los sistemas, estos ataques se denominan semánticos [3]. Esta amenaza implica la posible alteración de la información en cuanto a la interpretación del usuario que accede a consultarla, mediante la introducción de información falsa o la eliminación de información que cambia su sentido.

En la generación de documentos electrónicos, la *firma electrónica* es un mecanismo que hace posible la verificación de la integridad de dichos documentos, ya que permite detectar cualquier tipo de cambio efectuado

después de que el documento haya sido firmado, y también probar la firma de los documentos por una determinada persona. La herramienta base de la firma electrónica es el certificado digital, que usa dos claves criptográficas para identificar de manera unívoca a su propietario, una pública y otra privada (esta última no se debe ceder ya que puede usarse para suplantar a una persona). La emisión de estos certificados es realizada por los proveedores de servicios de certificación, que en España son supervisados y controlados por el Ministerio de Industria.

La normativa básica española sobre firma electrónica se recoge en la Ley 59/2003, de 19 de diciembre, de Firma Electrónica<sup>32</sup>. Esta ley, aparte de establecer el concepto de firma electrónica, también describe la firma electrónica avanzada como aquella que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a los que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control; y la firma electrónica reconocida, que es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. Una de las causas del escaso éxito de la puesta en marcha de sistemas con estas características ha sido la falta de usabilidad asociada a los dispositivos y navegadores donde se almacenan los certificados. Esto últimamente se ha resuelto con plataformas de firma en la nube como Cl@ve Firma<sup>33</sup>, desarrollada por el Gobierno de España.

Los sistemas de historia clínica electrónica suelen estar formados por distintas aplicaciones que deben estar integradas. Por esta razón es vital definir cuáles son los maestros de la información para salvaguardar la integridad de los datos. Aunque se usen estándares como el HL7 para el intercambio de información entre sistemas, siempre se corre el peligro de que la sincronización no sea perfecta. Un ejemplo de ello puede ser el siguiente: se registra una constante de un paciente en el sistema maestro y se han modificado en este último los valores de referencia, pero no se ha informado al sistema destino o el traslado de esta información al sistema destino se demora, por lo que podría ocurrir que no se reciba a tiempo un valor que debería provocar una alerta.

---

<sup>32</sup> <https://www.sede.fnmt.gob.es/normativa/firma-electronica>.

<sup>33</sup> [http://clave.gob.es/clave\\_Home/dnin.html](http://clave.gob.es/clave_Home/dnin.html)

Es decir, la integridad no sólo consiste que no se modifique la información generada, sino también en que se disponga de toda la información generada. Por lo tanto, si se comparte información entre sistemas debe hacerse con todos los datos existentes y no de forma parcial. Este es un caso típico del acceso a la historia clínica por parte de distintos servicios de salud.

La vida media de un sistema de información sanitario suele ser de 15-20 años. Cuando se toma la decisión por una razón u otra de cambiarlo, un apartado importante es la migración de la información previa. Si no se migra toda la información necesaria, la seguridad del paciente también puede correr peligro. Un ejemplo claro de ello es el cambio de los sistemas de información de los laboratorios, donde en la mayoría de las ocasiones desde el nuevo sistema no se puede consultar la información histórica del anterior.

Uno de los peligros más recientes y de actualidad para la seguridad de los pacientes son el autodiagnóstico y la automedicación, que ocurren básicamente cuando los pacientes consultan en Internet información sobre sus síntomas para buscar una solución, o cuando utilizan servicios de historia clínica personal en línea [4]. La información que aparece en muchas páginas web sobre medicina no está contrastada y tampoco existe una regulación al respecto. Se trata por tanto de un caso donde la integridad de la información está condicionada por las posibles fuentes de información utilizadas, por las políticas de actualización de la información y por los términos de uso de la información publicada, ya que se corre el riesgo de que se produzcan modificaciones no autorizadas de la información generada por una persona u organización. Algunas instituciones, como la Agencia de Calidad Sanitaria de Andalucía<sup>34</sup>, el Consejo General de Colegios de Médicos de España o el Colegio de Médicos de Barcelona, cuentan con programas y proyectos para acreditar páginas web con contenido sanitario. El objetivo final de estas iniciativas es certificar que el contenido mostrado es correcto, y para ello cuentan con una metodología de evaluación y con un comité de expertos que las avala. En la metodología utilizada se realiza una clasificación de las webs sanitarias, ya que no son lo mismo páginas informativas, institucionales o profesionales. Estas iniciativas pensadas para páginas web se deberían extender a los grupos relacionados con la sanidad en las distintas redes sociales existentes, ya que el problema es el mismo.

---

<sup>34</sup> Agencia de Calidad Sanitaria de Andalucía. Certificación ACSA.  
<http://www.juntadeandalucia.es/agenciadecalidadsanitaria/certificacion-acsa/>

Una incertidumbre más en la integridad es el llamado *big data*, una tecnología que analiza grandes conjuntos de datos con el objeto de obtener información estadística y modelos predictivos. Puesto que la información que genera no se puede considerar completa en ningún caso, se debe proceder con prudencia en cuanto a los resultados obtenidos, ya que a pesar de contar con un elevado potencial para la comprensión de determinadas enfermedades y su predicción, siempre se deben tener en cuenta otros aspectos conyunturales. Por lo tanto, los resultados del análisis del *big data* se deben considerar como una fuente parcial de información, dejando claro que no es la única.

En los tres casos comentados existe una relación directamente proporcional entre la integridad del sistema y el grado de fiabilidad para los clínicos, y por tanto de su uso.

### Disponibilidad

La disponibilidad se puede definir como la cualidad de un sistema de información que lo hace accesible para los usuarios. Lo que las personas valoran en general es que la falta de disponibilidad sea la mínima posible. Se considera obvio que los sistemas siempre están disponibles y no se aceptan las situaciones excepcionales que causan lo contrario. Si la información clínica no está disponible cuando es necesaria se puede causar un grave perjuicio al paciente. Por lo tanto, la disponibilidad está directamente relacionada con la seguridad del paciente.

El principio de disponibilidad de la información es el más tecnológico de todos los tratados en este capítulo porque depende en la mayoría de los casos de aspectos relacionados con la infraestructura, como las comunicaciones, el hardware y el software de base. Pese a que la falta de disponibilidad se puede producir tanto por problemas ocasionados por cualquiera de estos elementos, la mayoría de los casos están causados por el hardware.

Además, la disponibilidad es el aspecto más medible porque se puede evaluar mediante parámetros previamente definidos y aceptados por todos. Normalmente se usan porcentajes para medir la disponibilidad de la información, tomando el tiempo como variable global. Los contratos que se realizan con los proveedores de infraestructura recogen

acuerdos de nivel de servicio (ANS) que incluyen estos parámetros para medir la calidad del servicio prestado. Los ANS no son más que la garantía del cumplimiento de las necesidades definidas por un cliente ante su proveedor. El incumplimiento de estos ANS conlleva en la mayoría de los casos penalizaciones económicas, aunque también se pueden acordar otro tipo de contraprestaciones por el daño causado.

Las medidas para poder solucionar cuanto antes la falta de disponibilidad de un sistema dependen al menos de los siguientes factores:

- Detección del problema. Es primordial contar con herramientas de monitorización para detectar los problemas. Estas herramientas se basan en sondas periódicas que comprueban distintas características de la infraestructura, determinando si son correctas o no y notificándolo en caso negativo.
- Coordinación del personal involucrado en la respuesta ante el problema. Normalmente los servicios de tecnología están divididos en distintos servicios: sistemas operativos, base de datos, desarrollo, redes, seguridad. Es fundamental elegir el rol que los coordine, que debe contar con habilidades tanto técnicas como de gestión de equipos.
- Gravedad del problema. Como se recoge en la guía de buenas prácticas ITIL<sup>35</sup>, la clasificación de los incidentes es un requisito fundamental para determinar el impacto y la urgencia del problema detectado. En función de estos dos parámetros se fija la prioridad del problema. La nueva versión de ITIL contempla ya la gestión de la seguridad dentro del diseño del servicio.
- Complejidad del sistema. También como determina ITIL, la asignación del personal adecuado y disponible al problema originado es un factor que reducirá los tiempos de respuesta en la solución a dicha situación.
- Tiempo de respuesta en conseguir material de recambio en el caso de tratarse de una avería física. En muchas ocasiones los problemas surgen por un problema físico que exige sustituir algún elemento hardware. En la mayoría de los casos este material no se encuentra en el centro donde se ha originado el incidente y el tiempo de respuesta para su llegada suele depender de terceras partes, por lo que la logística es fundamental y es importante su seguimiento.

---

<sup>35</sup> AXELOS. What is ITIL® Best Practice?:  
<https://www.axelos.com/best-practice-solutions/itil/what-is-itil>

El concepto tecnológico que permite contar con una disponibilidad máxima es el de alta disponibilidad. Ésta permite continuar con el funcionamiento de un servicio aunque exista un fallo de software o hardware. Tanto en sistemas operativos como en bases de datos existen soluciones de todos los proveedores para su implementación. También todos los proveedores de hardware cuentan con productos para implantar esta solución tanto en servidores, cabinas de discos o elementos de red. En todos se sigue la misma técnica, basada en la redundancia de elementos.

Existen otros factores no tecnológicos que también condicionan la disponibilidad de los sistemas y de los centros de procesos de datos (CPD), como son los cortes de suministro eléctrico y las catástrofes naturales. En el primer caso los CPD también cuentan con soluciones como la duplicidad de líneas eléctricas o los sistemas de alimentación ininterrumpida, cuyas baterías entran en funcionamiento hasta que se ponen en marcha sistemas alternativos, como los grupos electrógenos, que generan electricidad a partir de un motor de combustión. En el segundo caso es vital diseñar planes de recuperación ante desastres, donde se define una arquitectura con un CPD principal y otro secundario como respaldo.

Por último, debemos remitirnos a los sistemas de información sanitarios donde la disponibilidad necesaria es total, ya que la atención sanitaria se presta todos los días del año a todas las horas del día, por lo que los porcentajes de disponibilidad se deben aproximar al 100% en todos los sistemas que estén relacionados con la asistencia.

Es obvio que en los sistemas no directamente relacionados con la práctica clínica no es necesario que se cumpla ese porcentaje. Con esto se quiere decir que es fundamental fijar el tramo horario en el que un sistema debe estar siempre disponible.

Otra característica de los sistemas sanitarios es su elevada complejidad por el alto número de integraciones que se requieren, al existir numerosos casos de uso y actores. En este sentido, el factor de la coordinación también comentado con anterioridad es fundamental, así como la documentación de las casuísticas posibles del flujo de pacientes con sus sistemas asociados.

En resumen, la disponibilidad incluida en la seguridad de la información es necesaria para garantizar la seguridad clínica de los pacientes.

## Confidencialidad

La confidencialidad en la seguridad de la información tiene el objetivo de garantizar que sólo las personas autorizadas accedan a dicha información. Así pues, lo primero que se debe regular es saber quiénes son las personas autorizadas, y en paralelo se deben diseñar y desarrollar los sistemas de información para poder soportar las medidas de seguridad correspondientes. En el diseño se analizará el método más adecuado para identificar a las personas que acceden y la política de perfiles con la que se contará.

Si se analizan los distintos métodos de identificación de personas con los que se cuenta en la actualidad, nos encontramos, como siempre suele ocurrir, que la tecnología aplicada a los sistemas va bastante por detrás de las soluciones más óptimas existentes. Esto ocurre por la complejidad de uso y por su elevado coste de implantación. Se podría decir que son mayoría los sistemas sanitarios que usan para la validación de usuarios un código y una contraseña, que tiende a ser única para todos los posibles sistemas de la organización. En segundo lugar están los sistemas que usan certificados digitales personales para uso profesional; estos certificados pueden estar incluidos en una tarjeta o en un dispositivo, o almacenados en red. El primer método es más recomendable desde el punto de vista de la seguridad, pero también el más costoso organizativamente. Por último, el sistema más novedoso pero casi sin uso en el entorno sanitario es el de autenticación biométrica, que se basa en las características físicas o de conducta del individuo para su identificación.

En cuanto a la política de perfiles, es decir, las distintas opciones de acceso y uso de las aplicaciones disponibles para los usuarios, suele ser un tema polémico porque no se trata de un problema técnico sino organizativo. Esto se acentúa aún más en las organizaciones sanitarias, donde siempre es costoso conseguir un consenso en la definición del acceso de cada profesión y de cada nivel de asistencia.

En general, la confidencialidad es imprescindible para la seguridad de los pacientes. Un caso que ilustra lo anterior podría ser el siguiente: Una persona no autorizada accede a los resultados de un informe clínico antes de que el personal médico informe sobre éste al paciente. Esta persona resulta ser próxima al paciente y le informa sobre estos

resultados, pudiendo entonces el paciente tomar decisiones sin esperar a conocer de primera mano la opinión del profesional sanitario. Estas decisiones precipitadas pueden afectar a su seguridad clínica sin saberlo. Si se hubiese controlado el perfil de acceso de la persona que accedió, se podría haber evitado esa situación y evitar riesgos para la seguridad del paciente.

Otro caso donde se debe garantizar la máxima protección de datos es el de los sistemas que almacenan información sanitaria en la nube. Cada vez es más habitual que la industria farmacéutica cuente con soluciones de este tipo aplicadas a sus productos para controlar la adherencia de los pacientes. En principio, es una buena idea para garantizar la seguridad clínica de los pacientes, pero dichos laboratorios deberían someterse a auditorías externas que garanticen que los datos que se almacenan se usan exclusivamente para el objetivo mencionado y no para otros.

Lo mismo ocurre con el Internet de las cosas, que poco a poco se está extendiendo también al ámbito sanitario porque cada vez es más habitual su uso en la monitorización remota de pacientes. La Unión Europea está potenciando el uso de la herramienta FIWARE<sup>36</sup>, una plataforma para el desarrollo y el despliegue de aplicaciones en este entorno para distintos sectores, entre ellos la sanidad. Sus especificaciones se adaptan a la filosofía de código abierto. Su desarrollo en el ámbito sanitario se encuentra en sus fases preliminares, y se debe vigilar si los estándares utilizados en la comunicación entre distintos dispositivos, que transmiten y reciben datos asociados a la salud de las personas, cumplen con las normas de protección de datos.

¡Y qué decir de la expansión que están teniendo las aplicaciones para dispositivos móviles y su conexión con distintos accesorios o dispositivos inteligentes! Se han desarrollado con tanta rapidez por ver quien tomaba posiciones primero en el mercado, que no se ha incorporado en muchos casos el marcado CE<sup>37</sup>, que certifica que los productos se han probado y que cumplen, entre otros, con los requisitos de seguridad y sanidad exigidos por la Unión Europea para su fabricación y comercialización.

---

<sup>36</sup> <https://www.fiware.org/>

<sup>37</sup> Unión Europea. Marcado CE: [http://europa.eu/youreurope/business/product/ce-mark/index\\_es.htm](http://europa.eu/youreurope/business/product/ce-mark/index_es.htm)

El big data ya se trató en el apartado de integridad, pero en este también tiene cabida. Es tentador para cualquier organización sanitaria poder sacar partido de los miles de datos sanitarios con los que cuenta, y una solución para ello es utilizar esta tecnología. Se debe remarcar que aunque la información se anonimice, siempre se puede intentar obtener la identidad de las personas a través de técnicas informáticas, por lo que es vital asegurarse que la protección de datos se garantiza en estos sistemas.

La confidencialidad también puede condicionar la seguridad clínica de los pacientes en algunos casos, en caso de que el personal clínico no cuente con un sistema sencillo y fluido para el acceso a la información. Se debe buscar un compromiso entre la confidencialidad y la facilidad de acceso. En muchos casos no siempre es así, ya que se diseñan sistemas tan complejos que penalizan la rapidez de acceso.

Está claro que, por muchas medidas de seguridad que se dispongan, siempre se va a contar con casos en los que por diferentes motivos no se pueda garantizar la confidencialidad, por lo que en este sentido siempre se debe trabajar previendo los posibles fallos y defectos que nos podemos encontrar, con una actitud proactiva y no reactiva.

## Aspectos normativos de la seguridad de la información

Como ya se ha dejado entrever, la tecnología va por delante del desarrollo normativo. Esto también ocurre en el caso concreto de la seguridad, provocando en muchos casos vacíos legales.

No se van a describir todos los aspectos normativos de la seguridad de la información en España, sino sólo los de más actualidad y los que influyen en el ámbito sanitario. Todas estas normativas, que se enumeran en orden inverso a su publicación, persiguen la garantía de la seguridad de la información y por tanto son importantes en la seguridad clínica de los pacientes.

## Ley de protección de las infraestructuras críticas

La ley de protección de las infraestructuras críticas (PIC) y su reglamento<sup>38</sup>, que transponen la directiva europea 2008/114/CE<sup>39</sup>, tienen como objetivo catalogar el conjunto de infraestructuras que prestan servicios esenciales a la sociedad y diseñar medidas de prevención y protección eficaces contra las posibles amenazas, tanto en la seguridad física como en la lógica de las tecnologías de la información.

Entre los sectores que se definen como esenciales se encuentra el de la sanidad, incluyendo a los centros sanitarios, hospitales y laboratorios. En algunos sectores, como el eléctrico y el del gas, ya se han redactado los planes estratégicos sectoriales correspondientes, pero en el sector de la sanidad esta labor se encuentra aún pendiente de realización. Estos planes están compuestos por varios documentos que incluyen la normativa de aplicación, estructura del sector, estudio de impacto, análisis general de riesgos y propuesta de medidas estratégicas. El desarrollo de este tipo de planes permite conocer cuáles son los servicios esenciales proporcionados a la sociedad y su funcionamiento general, las infraestructuras estratégicas sobre las que se asientan estos servicios esenciales, las vulnerabilidades del sistema, las consecuencias potenciales de su inactividad y las medidas estratégicas necesarias para su mantenimiento [5].

En este sentido, la principal vulnerabilidad y amenaza en la seguridad lógica de las tecnologías de la información radica en los ataques cibernéticos. Hasta ahora estos ataques han estado dirigidos a otros sectores pero, como los datos clínicos de las personas son altamente sensibles y “suculentos”, su valor en el “mercado negro” es elevado y

<sup>38</sup> Boletín Oficial del Estado:

- Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas: BOE N° 102, 29 de abril de 2011. Disponible en: <http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630>
- Real Decreto 704/2011, de 20 de mayo, por el que se aprueba el Reglamento de protección de las infraestructuras críticas. BOE N° 103, 21 de mayo de 2011. Disponible en: [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2011-8849](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2011-8849)

<sup>39</sup> Boletín Oficial del Estado. Directiva 2008/114/CE del Consejo, de 8 de diciembre de 2008, sobre la identificación y designación de infraestructuras críticas europeas y la evaluación de la necesidad de mejorar su protección: BOE N° 345, de 23 de diciembre de 2008. Disponible en: [https://www.boe.es/diario\\_boe/txt.php?id=DOUE-L-2008-82589](https://www.boe.es/diario_boe/txt.php?id=DOUE-L-2008-82589)

por lo tanto es un sector que también está en el punto de mira de estos ataques. La ciberseguridad, que se engloba dentro de la seguridad de la información, se ocupa de dar soluciones para evitar estos ataques.

### Esquema Nacional de Seguridad

Por la necesidad de dar respuesta a la protección de la información y a los medios usados en el derecho de los ciudadanos a comunicarse electrónicamente con la administración, como se recoge en la Ley 11/2007, surge el Esquema Nacional de Seguridad (ENS), regulado por el Real Decreto 3/2010<sup>40</sup>, de 8 de enero, que concreta la política de seguridad que se debe aplicar en la utilización de los medios electrónicos, en cuanto a las medidas de seguridad técnicas y organizativas que sean precisas.

Algunas instituciones, como la Consejería de Sanidad de la Comunidad de Madrid (orden 491/2013, de 27 de junio<sup>41</sup>) y el Ministerio de Sanidad (Orden SSI/321/2014<sup>42</sup>, de 26 de febrero) ya han aprobado la publicación de su plan de seguridad de la información en el ámbito de la administración pública.

Es importante resaltar que el ENS es de obligado cumplimiento para las administraciones públicas y no lo es para el ámbito privado. Asimismo, la implantación de la norma ISO 27001 permite cumplir con los requerimientos del ENS.

Otro aspecto a destacar en la redacción del ENS es que se debe diferenciar al prestador de servicios de la implantación de la

---

<sup>40</sup> Boletín Oficial del Estado:

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos: BOE N° 150, de 23 de junio de 2007. Disponible en: [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2007-12352](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-12352)
- Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. BOE N° 25, de 29 de enero de 2010. Disponible en: <http://www.boe.es/buscar/doc.php?id=BOE-A-2010-1330>

<sup>41</sup> Orden 491/2013, de 27 de junio, de la Consejería de Sanidad, por la que se aprueba la política de seguridad de la información en el ámbito de la Administración Electrónica y de los sistemas de información de la Consejería de Sanidad de la Comunidad de Madrid. Disponible en: <http://www.madrid.org/wleg/servlet/Servidor?opcion=VerHtml&idnorma=9364&word=S&wordperfect=N&pdf=S>

<sup>42</sup> Orden SSI/321/2014, de 26 de febrero, por la que se aprueba la política de seguridad de la información en el ámbito de la administración electrónica del Ministerio de Sanidad, Servicios Sociales e Igualdad: BOE N° 55, de 5 de marzo de 2014. Disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2014-2378>

administración electrónica con el del ENS, es decir, debe existir en los departamentos de tecnologías de la información una estructura independiente pero transversal al resto, encargada de la seguridad. Con esto queda claro que no es coherente que un mismo servicio se audite a sí mismo.

Sistemas de información sanitarios típicos que deben adecuarse al ENS por ser parte de la administración electrónica de los servicios de salud son: receta electrónica, cita web e historia clínica del paciente.

### LOPD

La ley 15/1999 Orgánica de Protección de Datos (LOPD) y su reglamento de medidas de seguridad<sup>43</sup>, actualizado en 2010, clasifican la información relacionada con la salud como de nivel alto. Esto quiere decir que se le deben aplicar las máximas medidas de protección a esta información.

Entre las medidas obligatorias a adoptar está la redacción de un documento de seguridad que recoge las medidas de índole técnica y organizativa necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados según lo dispuesto en el citado reglamento y en la LOPD.

Uno de los riesgos que existe en la aplicación de la LOPD en las administraciones públicas es la falta de sanciones económicas en este ámbito, ya que sólo se contemplan la posibilidad de que sean administrativas.

La Unión Europea ha aprobado la constitución de un nuevo reglamento de protección de datos de carácter personal que sustituye a la directiva actualmente vigente. Su propósito es adaptarse a la nueva era digital y mejorar la protección de datos de los ciudadanos europeos.

---

<sup>43</sup> Boletín Oficial del Estado:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal: BOE Nº 298, de 14 de diciembre de 1999. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-1999-23750>
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal: BOE Nº 17, de 19 de enero de 2008. Disponible en: <https://www.boe.es/buscar/act.php?id=BOE-A-2008-979>

## Protección datos versus seguridad clínica

Antes de entrar a detallar posibles casos donde se pone en duda el aspecto de la confidencialidad en la seguridad clínica, es importante dejar claro que la seguridad de la información es un elemento vital para todos y todo en general, pero si se lleva al extremo la normativa pueden producirse situaciones como las que se van a comentar a continuación, que pueden generar un debate o al menos una reflexión sobre qué debe primar, si los aspectos clínicos, entre los que se encuentra la seguridad del paciente, o la confidencialidad. La respuesta adecuada es que siempre debe haber un equilibrio entre ambas.

El primer caso que se analiza es el de los derechos ARCO (acceso, rectificación, cancelación y oposición) que incluye la LOPD, merced a los cuales los ciudadanos pueden ejercer su derecho a recibir información sobre los accesos a sus datos personales, solicitar la rectificación y cancelación de los datos por ser incompletos, inexactos o excesivos, y comunicar su oposición al tratamiento de su información personal.

La solicitud de la cancelación de datos sanitarios, por ejemplo en un hospital, se contradice con el deber de la conservación del historial clínico que recoge la ley 41/2002 de autonomía del paciente<sup>44</sup>, ya que es necesaria para la práctica clínica. En este caso, si se aplicase la LOPD se penalizaría la seguridad clínica del paciente.

La Agencia Española de Protección de Datos ha resuelto sobre estos asuntos en varias ocasiones, concluyendo que en este caso prima lo recogido en la ley 41/2002 para garantizar la correcta asistencia sanitaria<sup>45</sup>.

---

<sup>44</sup> Ley 41/2002, de 14 de noviembre, básica reguladora de la autonomía del paciente y de derechos y obligaciones en materia de información y documentación clínica: BOE Nº 274, de 15 de noviembre de 2002. Disponible en: [https://www.boe.es/diario\\_boe/txt.php?id=BOE-A-2002-22188](https://www.boe.es/diario_boe/txt.php?id=BOE-A-2002-22188)

<sup>45</sup> Agencia Española de Protección de Datos. Derecho de cancelación sobre los datos de un paciente. Informe 0049/2005. [https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes\\_juridicos/derecho\\_acceso\\_rectificacion\\_cancelacion\\_oposicion/common/pdfs/2005-0049\\_Derecho-de-cancelaci-oo-n-sobre-los-datos-de-un-paciente.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/derecho_acceso_rectificacion_cancelacion_oposicion/common/pdfs/2005-0049_Derecho-de-cancelaci-oo-n-sobre-los-datos-de-un-paciente.pdf)

Un segundo caso es el acceso al historial clínico de los pacientes desde los servicios de salud pública e investigación biomédica. La Unión Europea ha estado preparando desde hace bastante tiempo un nuevo reglamento de protección de datos que está creando mucha polémica por los cambios introducidos en los artículos 81 (tratamiento de datos personales relativos a la salud) y 83 (tratamiento para fines de investigación histórica, estadística o científica) mediante las enmiendas del Parlamento Europeo aprobadas en abril de 2014<sup>46</sup>. La versión inicial había logrado conseguir un equilibrio entre la protección de la intimidad y la investigación biomédica. Por una parte establecía los requisitos del consentimiento informado específico y explícito o la completa anonimización para el uso y almacenamiento de datos de carácter personal; pero por otro establecía excepciones en el campo de la investigación sujetas a una serie de garantías, reflejadas en el artículo 83. Las enmiendas que se introdujeron redujeron mucho el alcance de esas excepciones. En definitiva, el uso de datos de carácter personal en esos campos sin el consentimiento informado de los sujetos o sin datos anonimizados por completo, quedaría prohibido o sería prácticamente imposible. No se tendrían en cuenta medidas que se aplican ya con éxito para la investigación con datos personales y sin consentimiento informado, como son la autorización previa por un comité de ética de investigación clínica, la codificación de la identidad de los sujetos y la adopción de estrictas garantías de confidencialidad para los responsables de los ficheros.

Un tercer último caso sería la constitución de los perfiles de acceso del personal que accede a la historia clínica electrónica. La normativa no zanja claramente cuál es el acceso que debe tener el personal sanitario. El límite de permisos debe definirse sobre la base de lograr la mejor asistencia sanitaria para el paciente<sup>47</sup>, y siempre debe ser aprobado por los servicios de documentación clínica, que son sus responsables últimos. Un ejemplo clásico de confrontación es el de personal de enfermería, y más en concreto el de consultas y hospitalización; en ambos casos se debe dar acceso a todo lo relativo del

---

<sup>46</sup> Sociedad Española de Epidemiología. Grupo de Trabajo sobre Confidencialidad y Protección de Datos. <http://www.seepidemiologia.es/gruposdetrabajophp?contenido=gruposdetrabajosub10>

<sup>47</sup> Agencia Española de Protección de Datos. Criterio de acceso del personal de enfermería. Informe 656/2008. [https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes\\_juridicos/datos\\_esp\\_protégidos/common/pdfs/2008-0656\\_Acceso-a-historia-cl-ii-nica-por-personal-de-enfermer-ii-a.pdf](https://www.agpd.es/portalwebAGPD/canaldocumentacion/informes_juridicos/datos_esp_protégidos/common/pdfs/2008-0656_Acceso-a-historia-cl-ii-nica-por-personal-de-enfermer-ii-a.pdf)

episodio en cuestión y a todo lo anterior que sea considerado relevante para dar una buena asistencia. Si el personal sanitario no cuenta con toda la información posible puede ponerse en riesgo la seguridad clínica de los pacientes.

La última valoración sobre este apartado es que la protección de datos debe superar aspectos técnicos como la unificación, caducidad y complejidad de las contraseñas, e incluso el bloqueo de acceso por número de intentos erróneos de ingreso en aquellos sistemas que todavía cuentan con esta técnica de identificación, ya que provocan una percepción de lentitud y poca usabilidad, y por consiguiente un sentimiento de rechazo, en los usuarios finales de la historia clínica electrónica.

Se debe alcanzar un equilibrio entre las medidas de seguridad y la disponibilidad. Un exceso en las medidas para garantizar la confidencialidad puede suponer colapsar los sistemas [6].

## Conclusiones

Como se ha visto a lo largo del capítulo, los pilares de la seguridad de la información (integridad, disponibilidad y confidencialidad) son condición necesaria pero no suficiente para garantizar la seguridad de los pacientes, ya que ésta depende también de otros factores.

Una organización que tenga bien desarrollada su política de seguridad y la ponga en práctica no tendrá problemas derivados de la seguridad de la información en la seguridad clínica del paciente. Eso sí, si no se desarrolla o se hace parcialmente, se corre el riesgo de sufrir incidentes en la seguridad de la información y por tanto en la seguridad del paciente.

También se ha mostrado que la protección de datos llevada al extremo puede provocar problemas en la accesibilidad de los sistemas de información, y por tanto condicionar la seguridad clínica al no contar con la información necesaria para realizar la asistencia.

Finalmente, las guías de seguridad clínica ya incluyen aspectos de la seguridad de la información como claves en las recomendaciones que realizan, por lo que se reconocen y valoran la importancia de este tema para el paciente.

## Bibliografía

- [1] Reyes J.F., Bermúdez M.J. Conceptos básicos sobre seguridad clínica. *Enfermería del Trabajo* 2011; 1:221-8.
- [2] Reason J. Human error: models and management. *BMJ* 2000; 320:768-70.
- [3] Schneier B. Semantic Attacks: The Third Wave of Network Attacks. *Schneier on Security*, Octubre 2001. Disponible en: <https://www.schneier.com/crypto-gram/archives/2000/1015.html#1>
- [4] Martínez R. y Rojas D. Gestión de la seguridad de la información en atención primaria y uso responsable de Internet y de las redes sociales. En: Carnicero J., Fernández A. y Rojas D. (coordinadores). *Manual de salud electrónica para directivos de servicios y sistemas de salud (II). Aplicaciones de las TIC a la atención primaria de salud. Informes SEIS (10)*. Comisión Económica para América Latina y el Caribe (CEPAL), Sociedad Española de Informática de la Salud (SEIS); 2014. 255-78. Disponible en: <http://82.98.165.8/documentos/informes/secciones/adjunto1/X%20Informe%20SEIS%20-%2010%20-%20Seguridad%20de%20la%20informaci%C3%B3n,%20Internet%20y%20redes%20sociales.pdf>
- [5] Sánchez F. Entrevista al Director del Centro Nacional para la Protección de las Infraestructuras Críticas. *Revista Securitecnia*. Número 417. Abril 2014. Disponible en: <http://www.seguritecnia.es/seguridad-publica/administraciones-publicas/el-cnpic-sera-flexible-en-la-implantacion-de-los-pso-y-los-ppe-por-parte-de-los-operadores>
- [6] Garbayo J, Carnicero J, Sánchez C. La seguridad, confidencialidad y disponibilidad de la información clínica. En: Carnicero J. (coordinador). *De la historia clínica a la historia de salud electrónica. Informes SEIS (5)*. Sociedad Española de Informática de la Salud (SEIS); 2003. 255-86. Disponible en: <http://82.98.165.8/documentos/informes/secciones/adjunto1/CAPITULO9.pdf>



## Los autores



**Sonia Elizabeth Benítez (Argentina).** Médica especialista en Medicina Interna de la Universidad de Buenos Aires. MSc en Informática Médica por la Oregon Health & Science University. Médica de Planta del Departamento de Informática en Salud del Hospital Italiano de Buenos Aires.

**Nereo Norberto Candenas (Argentina).** Desarrollador Universitario de la Universidad de Belgrano. Analista del Instituto Ort de Argentina. Coordinador de Tecnología y Desarrollos del Laboratorio Central del Hospital Italiano de Buenos Aires.

**Javier Carnicero Giménez de Azcárate (España).** Licenciado en Medicina y Cirugía por la Universidad de Zaragoza. Doctor por la Universidad de Valladolid. Máster en Dirección de Servicios de Salud por la Universidad Pública de Navarra. Jefe del Servicio de Gestión de Prestaciones y Conciertos del Servicio Navarro de Salud. Revisor de Applied Clinical Informatics (ACI), revista electrónica oficial de la Asociación Internacional de Informática Médica (IMIA). Miembro de la Junta Directiva de la Sociedad Española de Informática de la Salud. Coordinador de los Informes SEIS.

**Miguel Ángel de Cristóforo (Argentina).** Bioquímico especialista en Análisis Clínicos orientación Microbiología de la Universidad de Buenos Aires. Coordinador de los Sistemas de Información y Jefe de la sección Virología del Laboratorio Central del Hospital Italiano de Buenos Aires. Coordinador de las carreras de Farmacia y de Bioquímica y Docente del Instituto Universitario del Hospital Italiano.

**Carlos Emparán García de Salazar (España).** Cirujano General y del Aparato Digestivo. MBA en Dirección Hospitalaria Internacional. Director Médico del Burjeel Hospital (Abu Dhabi, Emiratos Árabes Unidos). Profesor Asociado de Cirugía. Vocal de la Sección de Calidad y Gestión de la Asociación Española de Cirujanos. Fellow del Colegio Americano de Cirujanos. Miembro de la Sociedad Alemana de Cirugía.

**Matías Gastón Dombald (Argentina).** Bioquímico asociado - Sistemas de Información del Laboratorio Central del Hospital Italiano de Buenos Aires. Postgrado en Gerenciamiento en Sistemas de Salud – Instituto Universitario Hospital Italiano de Buenos Aires. Miembro del Comité de Seguridad del Paciente - Hospital Italiano de Buenos Aires. Miembro de la Comisión Directiva del Colegio Oficial de Farmacéuticos y Bioquímicos de la Capital Federal - Argentina. Docente - Instituto Universitario Hospital Italiano de Buenos Aires.

**Selene Indarte (Uruguay).** Doctora en Medicina (Universidad de la República, Uruguay). Posgrado en Administración de Empresas de Salud (Universidad de la Empresa, Uruguay), en Habilidades Gerenciales (Universidad de la Empresa, Uruguay), y en Informática Biomédica (Hospital Italiano de Buenos Aires, Argentina). Miembro de la Directiva de SUEIIDISS (HL7 Uruguay). Docente asociado de la Facultad de Ingeniería en el tema “Sistemas de Información en Salud”. (Universidad de la República, Uruguay). Docente de la Facultad de Ingeniería en el Diploma de Informática Médica (Universidad de la Empresa).

**Daniel Luna (Argentina).** Médico Internista, Magíster en Ingeniería de Sistemas de Información y Doctorando en Ingeniería Informática. Jefe del Departamento de Informática en Salud del Hospital Italiano. Titular de la Cátedra de Informática Médica y la Maestría de Informática en Salud del Instituto Universitario del Hospital Italiano. Editor Asociado de Journal of Health Informatics in Developing Countries, Applied Clinical Informatics Journal y el Healthcare Informatics Research.

**Humberto Fernán Mandirola Brioux (Argentina).** Médico Doctorado en Medicina Interna de la Universidad de Buenos Aires, Especialista en Medicina Interna y Terapia Intensiva, Asociado al Departamento de Informática Médica del Hospital Italiano de Buenos Aires, Director de la Carrera de Post Grado de la UBA de Medicina Interna, Miembro de la Comisión directiva de HL7 Argentina.

**Raúl Martínez Santiago (España).** Licenciado en Ciencias Físicas por la Universidad de Cantabria. Máster en Dirección y Gestión de Servicios Sanitarios y Sociales por la Universidad de Cantabria. Coordinador de Sistemas y Tecnologías de la Información del Servicio Cántabro de Salud. Miembro de la Sociedad Española de Informática de la Salud.

**Carlos Otero (Argentina).** Informático Médico en el Hospital Italiano de Buenos Aires. MSc en Informática Médica por la Oregon Health & Science University. Médico de Planta del Departamento de Informática en Salud del Hospital Italiano de Buenos Aires. Chair IMIA working group for development.

**Pedro Parra Hidalgo (España).** Médico Especialista en Medicina Preventiva y Salud Pública. Doctor en Medicina por la Universidad de Murcia. Subdirector General de Calidad Asistencial, Seguridad y Evaluación del Servicio Murciano de Salud. Profesor del Máster para la Gestión de la Calidad en los Servicios de Salud de la Universidad de Murcia. Evaluador acreditado EFQM. Miembro de la Sociedad Española de Informática de la Salud (SEIS). Revisor de la Revista de Calidad Asistencial y de Anales de Pediatría. Expresidente de la Sociedad Española de Calidad Asistencial (SECA).

**Arturo Pereira Saavedra (España).** Doctor en Medicina por la Universidad de Barcelona y Especialista en Hematología y Hemoterapia. Consultor senior del Servicio de Hemoterapia y Hemostasia del Hospital Clínic de Barcelona.

**Fernán González Bernaldo de Quirós (Argentina).** Médico especialista en Medicina Interna de la Universidad de Buenos Aires. MSc en Gobierno y Dirección de Sistemas de Salud. Universidad Oberta de Cataluña. Vicedirector Médico Planeamiento Estratégico. Hospital Italiano de Buenos Aires. Jefe De Área Sección Investigación en Medicina Interna. Director de la Maestría de Informática en Salud. Instituto Universitario Hospital Italiano. Profesor Titular de Fisiología Humana - Instituto Universitario Hospital Italiano.

**David Rojas de la Escalera (España)**. Ingeniero de Telecomunicación (especialidad telemática) por la Universidad de Cantabria. Business Development Senior Consultant en Sistemas Avanzados de Tecnología, S.A. (SATEC). Miembro de la Sociedad Española de Informática de la Salud. Revisor de Applied Clinical Informatics (ACI), revista electrónica oficial de la Asociación Internacional de Informática Médica (IMIA) y de la Asociación de Directores Médicos de Sistemas de Información (AMDIS). Referee del Consejo Editorial de la revista Gestión y Evaluación de Costes Sanitarios de la Fundación Signo.

## Notas























El Informe SEIS, “Las TIC y la seguridad de los pacientes” destaca la contribución de las Tecnologías de la Información y de la Comunicación (TIC) a la calidad y eficiencia de la actividad asistencial. Entre sus aportaciones al sistema de salud se encuentra la mejora de la seguridad de los pacientes. Sin embargo, y a pesar de sus efectos positivos, las TIC también pueden suponer nuevos riesgos para los pacientes.

La seguridad de los pacientes es un objetivo que goza de la máxima prioridad, por lo que cualquier tecnología, incluso las TIC, que se incorpore al sistema de salud, debe considerar tanto su contribución como los riesgos para alcanzar ese objetivo. Como las TIC son también un instrumento clínico, deben tratarse de la misma forma que cualquier tecnología de la salud, evaluándose su eficacia (¿cumple el objetivo previsto?); su seguridad (¿tiene efectos adversos o secundarios que impidan o desaconsejen su utilización? ¿tiene riesgos para la seguridad de los pacientes?); su efectividad (¿cumple sus objetivos en condiciones reales?); y su coste, de forma que se pueda calcular su relación coste-efectividad.

Este Informe SEIS pretende sensibilizar, contribuir a generar conocimiento y comprometer a todos los involucrados, para que los objetivos de seguridad de los pacientes se incorporen desde el primer momento a todos y cada uno de los proyectos de sistemas TIC en el sector de salud.

ISBN 978-84-617-4024-3



9 788461 740246