SEGURIDAD DEL PACIENTE 2.0

Dr. Fabián Vítolo
Noble Compañía de Seguros

Las A 17 años de "*Errar es Humano*", el informe del Instituto de Medicina de los Estados Unidos que puso en el centro de escena la magnitud del problema de los errores y el daño evitable en la atención de la salud, los especialistas en seguridad del paciente de todo el mundo coinciden: pese a la enorme cantidad de conocimiento acumulado durante todos estos años, el progreso ha sido muy modesto y sobre áreas puntuales. Lejos estamos de la revolución en el cuidado que se imaginaba.

El movimiento por la seguridad de los pacientes ha realizado grandes aportes para comprender y abordar el problema, Se han creado agencias estatales y organizaciones no gubernamentales abocadas a este tema, definido objetivos y metas de seguridad, realizado campañas mundiales para salvar vidas (Ej; Manos Limpias; Cirugía Segura) y adoptado modelos de investigación de accidentes de la seguridad industrial, entre muchas otras medidas.

Sin embargo, sigue costando mucho pasar de las ideas a la acción y comienzan a aparecer los primeros síntomas de desánimo y estancamiento. La parálisis no parece ser la mejor opción: la mayor intensidad y complejidad de los servicios de salud, una población que envejece con múltiples comorbilidades y el potencial de daño de drogas y procedimientos cada vez más invasivos permiten aventurar que, si no se contiene, el problema del daño evitable a los pacientes crecerá.

En el mundo de la tecnología, el término 2.0 se utiliza para describir una nueva generación de herramientas superadoras de la generación anterior que enriquecen la experiencia y las posibilidades del usuario, modificando muchas veces paradigmas.

Y es precisamente un cambio de paradigma el que nos proponen los Profesores Erik Hollnagel (Dinamarca), Robert Wears (EE.UU) y Jeffrey Brairhwaite (Australia) en su documento *"From Safety-I to Safety II: A White Paper*" (2015) .

En la visión de estos especialistas, debemos replantearnos muchas de las técnicas y modelos propuestos en el abordaje ortodoxo de la seguridad (Seguridad I) y comenzar a mirar el problema desde otro ángulo. Según su propuesta, la gestión en seguridad debería avanzar desde "garantizar que la menor cantidad de cosas posibles salgan mal" a "garantizar que la mayor cantidad de cosas posibles salgan bien". A esta nueva perspectiva la denominan Seguridad II.

El futuro residiría en una combinación de las dos formas de pensamiento. Si bien muchos de los métodos y técnicas existentes pueden continuar utilizándose, la asimilación de la visón de la Seguridad- II requerirá de nuevas prácticas para estudiar lo que sale bien y concentrarse en eventos frecuentes, manteniendo una alta sensibilidad a la posibilidad de fallas y balanceando sabiamente la meticulosidad en el trabajo con la eficiencia. En este nuevo mundo, la inversión en seguridad debería ser considerada también una inversión en productividad.

A continuación, una traducción parcial libre y adaptación al español del texto original en inglés, al cual puede accederse ingresando en la siguiente dirección web: https://www.england.nhs.uk/signuptosafety/wp-content/uploads/sites/16/2015/10/safety-1-safety-2-whte-papr.pdf

SEGURIDAD 1,0: LA VISIÓN ORTODOXA

Para la mayoría de las personas, la seguridad consiste en la ausencia de evoluciones no deseadas, tales como incidentes o accidentes. Como el término "seguridad" es utilizado y reconocido por casi todo el mundo, damos por sentado que los otros entienden por seguridad lo mismo que nosotros, y por eso no nos preocupamos mayormente por definirla de manera más precisa. El propósito de este documento es justamente ese; busca además explorar las implicancias de dos interpretaciones distintas de la seguridad.

La seguridad generalmente se define como el sistema de calidad necesario y suficiente garantizar que el número de eventos potencialmente dañosos para los trabajadores, las personas y el ambiente sean aceptablemente bajos. La OMS, por ejemplo, define a la seguridad del paciente como "la reducción del riesgo de daño innecesario asociado a la atención sanitaria hasta un mínimo aceptable."

El interés por la seguridad surge históricamente a partir de la ocurrencia de accidentes (eventos adversos reales) o por el reconocimiento de ciertos riesgos (eventos adversos potenciales). Las cosas que salen mal son generalmente explicadas mediante la identificación de sus presuntas causas y la respuesta tradicional consiste en eliminar estas causas o al menos contenerlas. Los nuevos tipos de accidentes han sido de manera similar atribuidos a nuevos tipos de causas, relacionadas ya sea con la tecnología (ej. fatiga de materiales), con factores humanos (ej.: sobrecarga de trabajo; "error humano") o con la organización (ej.: "cultura de seguridad"). Como este abordaje ha sido efectivo para aportar soluciones de corto plazo, a lo largo de los siglos nos hemos acostumbrado a explicar los accidentes en términos de relaciones de causa-efecto. Tanto, que ya no nos damos cuenta de este proceso de pensamiento, a pesar de que el mismo raramente refleja la realidad de lo sucedido. Sin embargo, nos encontramos tenazmente aferrados a esta tradición. Desafortunadamente, la visión retrospectiva de las deficiencias no ayuda a explicar con claridad la generación ni la persistencia de estas deficiencias.

Para ilustrar las consecuencias de definir seguridad por lo que sale mal, consideremos la Figura 1. Aquí, la delgada línea roja representa el caso donde la probabilidad estadística de falla es de 1 en 10.000. Pero esto también significa que deberíamos esperar que las cosas salieran bien 9.999 veces de 10.000 (correspondiéndose con el área verde). En la atención de la salud la tasa de fallas (eventos adversos) en pacientes internados es más alta (en el orden del 10% -dependiendo de cómo se cuenten-), pero el principio es el mismo: las cosas salen bien con muchísima mayor frecuencia que mal.

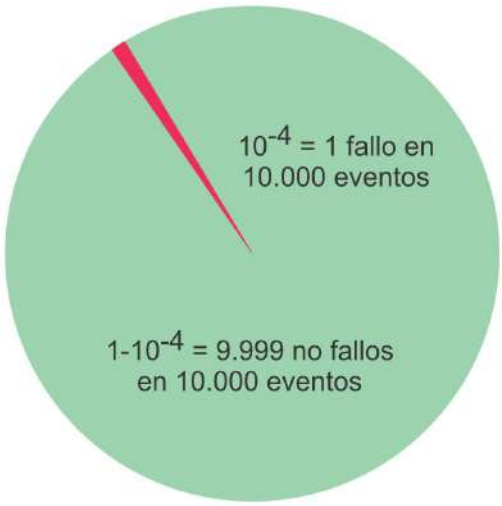


Figura1. El desbalance entre las cosas que salen bien y las que salen mal

En Seguridad 1,0, los esfuerzos se dirigen hacia lo que sale o puede salir mal, y este foco se refuerza de distintas maneras. Las autoridades y reguladores, por ejemplo, exigen reportes detallados en casos de accidentes, incidentes y eventos serios no intencionales. Existen agencias, departamentos y personas dentro las organizaciones especialmente destinadas a estudiar las evoluciones adversas. Numerosos modelos afirman poder explicar cómo pueden salir mal las cosas y ofrecen un considerable número de métodos para descubrir el componente defectuoso y sus causas. La información relativa a eventos adversos e incidentes es recogida en grandes bases de datos. Miles de trabajos científicos y libros describen y explican estas ocurrencias en detalle y el daño a los pacientes y los eventos adversos son debatidos en conferencias especializadas a

nivel nacional e internacional. El resultado final de esto es un diluvio de información, tanto acerca de las formas en las cuales las cosas pueden salir mal como de lo que debe hacerse para que estas cosas malas no ocurran. La solución general es del tipo "encuentre y repare": busque lo que está fallando o funcionando mal, trate de descubrir sus causas y, una vez descubiertas, elimínelas o introduzca barreras.

La situación es muy diferente con las cosas que salen bien. A pesar de su importancia crítica, los buenos resultados suelen recibir muy poca atención por parte de los responsables de gestionar los riesgos y promover la seguridad institucional. Como las autoridades y reguladores no piden mayores explicaciones sobre lo que sale bien ni por qué, son pocas las agencias o departamentos que se ocupan de profundizar en esto. Posibles excepciones podrían ser las auditorías, las encuestas (que pueden incluir un ítem sobre fortalezas) y las ocasionales buenas noticias o historias de éxito, que tanto agradan a los políticos o Directores Ejecutivos, ya que les sirven para gatillar noticias de prensa positivas. Sin embargo, en su conjunto, resulta muy difícil encontrar datos, hay pocos modelos, aún menos métodos y el vocabulario es muy escaso en comparación con los enormes glosarios de términos que se utilizan para definir lo que sale mal. Son muy pocos los libros y trabajos y prácticamente no se realizan conferencias. La búsqueda del cómo y el por qué las cosas salen bien choca con el foco tradicional sobre las fallas, y por eso recibe muy poco estímulo. Esto genera un serio problema, ya que no es posible garantizar que las cosas salgan bien sólo previniendo que salgan mal. Debemos también conocer cómo salen bien.

El abordaje ortodoxo de la seguridad (Seguridad – I), promueve una visión bimodal del trabajo y las actividades según la cual los resultados favorables y los desafortunados se deben a distintas formas de funcionamiento. Cuando las cosas salen bien se debe a que los sistemas funcionaron como debían y a que las personas realizaron su trabajo como fue imaginado; cuando las cosas salen mal es porque algo funcionó mal o falló. Se asume que los dos modos de funcionamiento son claramente diferentes, siendo el propósito de la gestión en seguridad garantizar que el sistema se mantenga en el primer modo y nunca se aventure en el segundo. (ver Figura 2.)

Figura 2. La Seguridad 1,0 asume que las cosas que salen bien y las que salen mal ocurren de diferentes maneras

La Seguridad 1,0 parte de la ocurrencia de eventos adversos (cosas que salieron mal) o bien de la identificación de potenciales riesgos. En ambos casos el abordaje suele ser del tipo "encuentre y repare". En el primer caso, encontrando las causas de los eventos adversos y desarrollando los cambios necesarios para que no se repitan. En el segundo, identificando la probable frecuencia e intensidad de los peligros en orden a eliminarlos o contenerlos. Otra solución consiste en prevenir la transición desde el estado de "funcionamiento normal" al de "funcionamiento anormal". Esto se consigue obligando a desempeñarse del modo normal, reforzando en cumplimiento de normas y estándares y eliminando la variabilidad (ver Figura 3.)

Figura:3 Seguridad mediante la eliminación y prevención

Resulta no sólo sabio sino también necesario reflexionar acerca de cuán efectivo ha sido este abordaje hacia la seguridad. Para ayudar a este propósito, describiremos a la Seguridad 1,0 a través de sus manifestaciones (fenomenología), sus mecanismos subyacentes (etiologia) y sus bases teóricas (ontología)

Las manifestaciones de la Seguridad 1.0: Fijarse en lo que salió mal

En el abordaje 1,0, la seguridad es definida por sus manifestaciones. Se dice que un sistema (ya sea un hospital, una farmacia o un centro de salud) es inseguro cuando produce muchos eventos adversos o afronta riesgos inaceptables. De manera similar, se dice que un lugar es seguro cuando los eventos adversos son muy infrecuentes o cuando gestiona sus riesgos de manera aceptable. Ésta, sin embargo, es una definición indirecta, ya que la seguridad es definida por su opuesto, más por lo que ocurre cuando está ausente que cuando está presente. La curiosa consecuencia de esto es que analizamos y tratamos de aprender sobre seguridad a partir de situaciones que se caracterizaron por su ausencia.

Otra consecuencia de esta visión es que el nivel de seguridad es inversamente proporcional al número de incidentes o eventos adversos. Si muchas cosas salen mal, se dice que el nivel de seguridad es bajo; pero si pocas cosas salen mal, el nivel de seguridad es alto. En otras palabras, cuantas más manifestaciones haya, menos seguro es el lugar y viceversa. Un nivel de seguridad perfecto e ideal sería aquel en el cual no ocurren eventos adversos y, por lo tanto, nada que medir. Desafortunadamente, es esto lo que determina que sea muy difícil, sino imposible, demostrar que los esfuerzos por mejorar la seguridad están funcionando y lo que resta argumentos para conseguir recursos para trabajar en seguridad.

Para ayudar a describir las manifestaciones de la falta de seguridad, se han descripto distintas tipologías de eventos adversos, en un rango que va desde lo simple (omisión-comisión) a lo más elaborado (distintas formas de errores cognitivos, violaciones o falta de cumplimiento). Obsérvese que estas tipologías a menudo esconden una problemática confusión entre error como resultado (manifestación) y error como causa.

Los “Mecanismos” de la Seguridad 1.0

Los mecanismos de la Seguridad 1.0 se basan en las suposiciones acerca de la forma en la que ocurrieron las cosas, las cuales son utilizadas para explicar o darle un sentido a las manifestaciones (eventos adversos). El mecanismo genérico de este modo de seguridad ha sido descripto como el “*credo de la causalidad”* – la creencia generalizada de que los malos resultados (accidentes, incidentes) ocurren porque algo se hizo mal -, por lo cual resulta factible encontrar y tratar sus causas. Y, si bien parece obvio y razonable asumir que las consecuencias están precedidas por las causas, sería una ingenuidad asumir que dichas causas son siempre fáciles de encontrar y de corregir.

A través de los años, este *credo de la causalidad* ha sido expresado mediante diferentes modelos de accidentes. Su versión más difundida asume que en todo accidente existen “causas raíces” que pueden ser descubiertas a través del análisis de lo sucedido. Si bien esta forma de pensamiento lineal resultaba probablemente adecuada en la primera mitad del siglo XX, la creciente complejidad de los sistemas socio-técnicos desarrollados durante la segunda mitad – especialmente a partir de la década del ’70- requiere de mecanismos más intrincados y poderosos. El mejor de ellos es el “Modelo del Queso Suizo, el cual explica que los eventos adversos son el resultado de una combinación de fallas activas y condiciones latentes. Otros ejemplos son TRIPOD (Reason et al, 1989), AcciMap (Rasmussen & Svedung, 2000) y STAMP (Leveson, 2004). En todos estos modelos el credo de la causalidad permite que el análisis se realice razonando “hacia atrás” desde las consecuencias hacia las causas subyacentes. Pero, como observó Reason (1997) “ El péndulo puede estar oscilando demasiado entre nuestros intentos por rastrear posibles errores y factores contribuyentes ligándolos a eventos adversos que se encuentran demasiado separados en tiempo y espacio de los mismos” . La creciente complejidad de estos modelos llevó incluso al mismo Reason a preguntarse si la fecha de vencimiento de su “queso suizo” no había expirado…

La bases de la Seguridad 1.0

La seguridad 1,0 se asienta en dos presunciones importantes. La primera es que los sistemas se pueden descomponer en sus partes constituyentes. La otra es que los sistemas y sus partes o bien funcionan correctamente o no, es decir que son bimodales.

“Los sistemas se pueden descomponer”

Sabemos que podemos crear sistemas juntando distintos componentes, como cuando se ensambla un

tomógrafo o un robot quirúrgico. También podemos generar complejos sistemas socio-técnicos como un hospital, -repleto de personas y tecnología- combinando y organizando cuidadosamente sus componentes. Esta es la forma natural en la que creamos sistemas,

La primera asunción es que este proceso puede ser revertido y que podemos comprender los sistemas descomponiéndolos en sus partes constituyentes más significativas. De hecho, solemos tener éxito cuando descomponemos los distintos elementos de un dispositivo tecnológico para descubrir las causas de ciertos accidentes (ej: equipos médicos que fallaron en quirófano). También asumimos que podemos descomponer "sistemas blandos" (las personas dentro de una organización) en sus distintas partes constituyentes (departamentos, servicios, roles, grupos equipos, etc). Y finalmente asumimos que podemos hacer lo mismo con las tareas y con los eventos, en parte por la seductora simplicidad que tiene la línea de tiempo (este evento ocurrió luego de aquel otro, y por lo tato el primer evento fue "la" causa. Pero solemos equivocarnos en todos los casos.

"El funcionamiento es bimodal"

También suele asumirse que los "componentes" de un sistema sólo pueden funcionar de dos modos: de manera correcta o de manera defectuosa, aceptando a veces distintos grados dentro de cada uno de estos modos. Los componentes del sistema se encuentran usualmente diseñados o pensados por ingenieros para cumplir una función específica y, cuando esto no ocurre, se dice que el componente falló, funcionó mal o se degradó. Si bien este razonamiento es válido para los sistemas tecnológicos y sus componentes, no resulta válido para los sistemas socio-técnicos y resulta definitivamente inapropiado para los componentes humanos y organizacionales, hasta el punto que no tendría sentido embarcarse en un análisis de este tipo.

Si bien las dos asunciones (posibilidad de descomponer el sistema y bimodalidad) son muy útiles para buscar causas y para responder "reparándolas", también nos llevan a descripciones del sistema y escenarios de una ilusoria trazabilidad y especificidad y a cuantificar también con una precisión ilusoria. Por eso, estas asunciones son insuficientes para sentar las bases de la gestión en seguridad en el mundo de hoy.

El mundo cambiante de la atención de la salud

Las crecientes demandas sobre el trabajo, la seguridad y la productividad

La visión 1.0 de la seguridad se desarrolló primero en la industria (aproximadamente entre los años 1965 y 1985), siendo unos años después importada al sector salud. Los sistemas industriales en la década del '70 eran relativamente simples cuando se los compara con el mundo de hoy. En esos años, la dependencia de las tecnologías de la información era muy limitada, en parte por la propia inmadurez de estas tecnologías, lo que hacía que las funciones de soporte fueran relativamente pocas, simples y mayormente independientes unas de otras. El nivel de integración (ej.: entre sub-sistemas y sectores) era bajo, y generalmente también era posible comprender y seguir lo que estaba pasando. Los sistemas de apoyo estaban pobremente acoplados (independientes), en contraposición con la gran interdependencia de nuestros días. El pensamiento en seguridad se desarrolló entonces sobre la base de las siguientes asunciones:

- Los sistemas y lugares de trabajo se encuentran bien diseñados y correctamente mantenidos.
- Los procesos son detallados, completos y correctos
- Las personas en el "extremo agudo" (en salud, aquellos que están en la primera línea de atención clínica) se comportan como se espera de ellos y como se los ha entrenado (trabajan como se supone o imagina que deben hacerlo)
- Los diseñadores han previsto cada contingencia y han dotado al sistema con una apropiada capacidad de respuesta. Si algo estuviera completamente mal, el sistema podría seguir funcionando porque el personal de la primera línea puede entender y manejar las contingencias, aún aquellas no previstas por los diseñadores.

Si bien estas asunciones probablemente nunca fueron correctas, se consideraban razonables en los '70s. Pero no resultan razonables hoy, y la seguridad basada en

estas premisas resulta inapropiada para el mundo que vivimos en la segunda década del siglo XXI.

Lamentablemente, desde la década del ’90 el sector salud adoptó estas asunciones de manera bastante acrítica, aún cuando el sector industrial se las estaba replanteando y cuando la atención de la salud de 1990 tenía muy poco que ver con los lugares de trabajo industrial de los 70’s. No puede decirse que esta situación haya mejorado, ya que incluso la atención del 2017 es muy distinta a lo que era en los ’90. Pese a ello, esta asunciones continúan siendo las bases de los actuales esfuerzos por mejorar la seguridad de los pacientes.

Desarrollo tecnológico frenético

Como la mayoría de las industrias, el sector salud se encuentra sometido a un tsunami de cambios y mejoras. Algunos cambios provienen de intentos bienintencionados que buscan reemplazar humanos “falibles” por tecnología “infalible”, mientras que otros responden a una mayor presión sobre el desempeño o a necesidades políticas. En muchos países, los gobiernos han establecido objetivos nacionales de seguridad con poco interés por analizar si esas metas tienen sentido o si son posibles de cumplir. El Presidente Clinton de los Estados Unidos, por ejemplo, respaldó el objetivo del Institute of Medicine (IOM) del año 2000 de reducir un 50% los errores en cinco años, afirmando que cualquier meta menor sería irresponsable (objetivos de seguridad como estos nos llevan a cuestionar nuevamente si se pueden medir mejoras en seguridad contando la forma en la que muy pocas cosas salieron mal)

Otra tendencia preocupante es que cada vez es más común que el problema de seguridad a tratar sea seleccionado en base a un solo criterio: si puede ser resuelto con alguna solución tecnológica atractiva y clara a nuestra disposición. Esto tiene dos consecuencias mayores. Una es que los problemas son abordados y resueltos uno por uno, como si pudieran ser tratados de manera aislada. La otra es que la solución preferida suele ser la meramente tecnológica y no socio-técnica, probablemente porque las soluciones socio-técnicas raramente son “atractivas y claras”.

A consecuencia del desarrollo tecnológico, hoy en día son muy pocas las actividades que son independientes unas de otras (en salud y en casi todos los campos), Las funciones, propósitos y servicios se encuentran íntimamente entrelazados y estos lazos serán aún mayores en el futuro. Consideremos, por ejemplo, algunas de las áreas de acción prioritarias para la seguridad de los pacientes establecidas por la OMS: higiene de manos y cirugía segura utilizando checklists; y otras, como los sistemas de reporte y aprendizaje, la implementación de “soluciones”; la difusión de las mejores prácticas, la gestión del conocimiento, la eliminación de las infecciones asociadas a las vías centrales y la implementación de “bundles” (paquetes de medidas). Si bien cada uno de estos objetivos puede aparecer plausible, su búsqueda a través de estrategias individuales conlleva el riesgo de consecuencias indeseadas. Los cambios en un sector pueden afectar a otros de manera significativa y no necesariamente beneficiosa, siendo por lo tanto muy difícil de que podamos comprender todas las implicancias que tienen las medidas que se proponen. De hecho cualquier solución basada en el pensamiento en seguridad 1.0 puede llegar a empeorar las cosas.

Dados los enormes desarrollos técnicos y científicos, la exagerada confianza en soluciones tecnológicas atractivas y la falta generalizada de voluntad para ser lo suficientemente exhaustivos hoy para ser eficientes después, nuestras ideas sobre la naturaleza del trabajo y la seguridad merecen ser revisadas. Debemos aceptar que los sistemas de hoy se vuelven cada vez más inextricables. Esto determina que los principios de su funcionamiento sean sólo son parcialmente conocidos (o en un creciente número de casos completamente desconocidos), que las descripciones deban ser elaboradas con infinidad de detalles y que sea muy probable que los mismos sistemas cambien antes de que hayamos terminado de describirlos, por lo cual nuestras descripciones serán siempre incompletas.

A consecuencia de esto, la predictibilidad se encuentra muy limitada, tanto durante la etapa de diseño como en la de las operaciones, y resulta casi imposible poder indicar o aún describir cómo debería realizarse el trabajo. Los sistemas puramente tecnológicos pueden funcionar de manera autónoma siempre y cuando su ámbito se encuentre completamente especificado y mientras no aparezca una variabilidad inesperada. Pero estas condiciones no pueden replicarse en los sistemas socio-técnicos. De hecho, para que la tecnología pueda funcionar, los seres humanos (y las organizaciones) deben funcionar como amortiguadores para absorber la

excesiva variabilidad. Las personas no son un problema a ser resuelto o a estandarizarse: son la solución adpatativa.

Las razones por las cuales las cosas funcionan (…de nuevo)

Como los sistemas de salud de hoy son cada vez más complejos e impredecibles, resulta imposible brindar una descripción completa de los mismos o especificar qué es lo que deberían hacer siempre los médicos, enfermeros y el resto del personal de salud, aún ante situaciones de ocurrencia frecuente. Como la tarea y el desempeño esperado no pueden ser completamente prescriptos, para que el sistema funcione se requiere de cierto grado de variabilidad, flexibilidad y adaptabilidad. Las personas contribuyen con tales "ajustes inteligentes", y son por lo tanto un activo sin el cual el funcionamiento adecuado del sistema sería imposible.

Los ajustes en el desempeño y la variabilidad son por lo tanto tan normales como necesarios, y son también las razones por las cuales las cosas tanto pueden salir bien como mal. Tratar de llegar a la seguridad restringiendo la variabilidad en el desempeño afectará inevitablemente nuestra capacidad para obtener los resultados deseados, pudiendo ser incluso contraproducente. La exigencia, por ejemplo, de que el médico lea, conozca y aplique al pie de la letra protocolos muy estandarizados de decenas de páginas para tratar a todos los pacientes que se presentan en la guardia con una cefalea o una crisis asmática no sólo resulta una tarea imposible, sino que puede quitar tiempo para brindar la atención propiamente dicha.

De manera similar, la existencia de más de 2.000 normas y protocolos de atención (números reales de varios sistemas de salud públicos) y la obligación de cumplir con estos procedimientos puede llevar a un colapso total del sistema. Por eso, más que preocuparnos por buscar las formas en las cuales algo puede fallar o funcionar mal y de establecer normas y procedimientos muy detallados, deberíamos tratar de comprender las características y el papel que tiene la variabilidad en el desempeño de todos los días.

El trabajo "como se lo imaginó" y "el trabajo como se realiza"

Una de las asunciones de las cuales poco se habla es la de que el trabajo perfectamente analizado y descripto en las normas y procedimientos ("el trabajo como se lo imaginó"") se corresponde con lo que la gente hace en la vida real. El trabajo imaginado termina siendo una visión idealizada de las tareas que ignora las distintas formas en las que estas tareas deben ser ajustadas para adaptarse a las siempre cambiantes condiciones de trabajo y del mundo. El "trabajo como se lo imaginó" describe lo que debería ocurrir bajo condiciones normales. El "trabajo como se realiza", en cambio, describe lo que realmente sucede, a medida que el trabajo se va desarrollando en contextos complejos.

Una razón de la popularidad del concepto del "trabajo como se lo imaginó" es el éxito indiscutible que tuvo la Teoría de la Administración Científica (Taylor, 1911). Introducida a principios del siglo XX, esta teoría había acumulado para la década del '30 suficientes estudios sobre tiempo-movilidad que demostraban de qué manera la descomposición de las tareas y actividades podía ser utilizada para mejorar la eficiencia del trabajo. Su punto culminante fue la línea de montaje de las fábricas.

La Administración Científica combinó estos estudios de tiempo/movilidad con el análisis racional y los sintetizó para encontrar la mejor forma de que los trabajadores pudieran realizar de manera mecánica y sin ninguna inducción especial cualquier tarea en particular. La Administración Científica sirvió así de fundamento teórico y práctico para la noción de que "el trabajo como se lo imaginó" era una condición necesaria y suficiente para el "trabajo como se realiza". Debemos destacar sin embargo, que la seguridad nunca fue un tema considerado por la teoría de la Administración Científica. Esta visión tuvo consecuencias tanto en la forma en que estudiamos los eventos adversos como en la que encaramos las mejoras en seguridad. Así, los eventos adversos podrían ser comprendidos observando los distintos componentes del sistema y encontrando aquellos que fallaron, como lo hacemos por ejemplo en el análisis de causa raíz. Y la seguridad podría ser mejorada mediante un cuidadoso trabajo de planificación en combinación con instrucciones detalladas y entrenamiento. Son estos principios los que nos llevan a confiar en la eficacia de las normas y a

poner énfasis sobre su cumplimiento. En resumen, la seguridad podría alcanzarse garantizando que el trabajo que se realiza sea idéntico al que se imaginó.

Pero en los ambientes complejos en los que se ejerce la medicina en nuestros días, el trabajo real puede ser muy distinto al trabajo descripto en las normas y procedimientos ("como se lo imaginó"), lo que lleva a preguntarnos la verdadera utilidad de describir tan minuciosamente lo que se debe hacer. Esta misma pregunta implica un cambio de paradigma que cuestiona los modelos y métodos que han constituido el núcleo central de la ingeniería de los sistemas, de los factores humanos y de la ergonomía. También desafía el concepto clásico de la autoridad de los jefes y gerentes. La implicancia práctica de todo esto es sólo podremos mejorar la seguridad si salimos de nuestros escritorios y salas de reuniones para pasar más tiempo en los ambientes clínicos y operativos con las personas de la primera línea de atención.

La complejidad actual de la atención de la salud nos obliga abordar el trabajo de todos los días como realmente es y no como debería ser, ya que los sistemas son reales y no ideales. Los sistemas terminan siendo confiables no porque se los haya pensado o diseñado de manera perfecta, ni porque las personas hagan exactamente los que está indicado en el manual, sino porque esas mismas personas son flexibles y se adaptan a circunstancias cambiantes.

Los humanos, por lo tanto, no son un lastre y la variación en el desempeño no representa una amenaza. Por el contrario, la variabilidad en el trabajo de todos los días es necesaria para que el sistema funcione, y es también la causa tanto de las evoluciones aceptables como de los eventos adversos. Entonces, como todos los resultados (los buenos y los malos) dependen de la variabilidad en el desempeño, las fallas no pueden prevenirse eliminándola; en otras palabras, la seguridad no puede ser buscada imponiendo restricciones sobre el trabajo normal.

El abordaje ortodoxo de la seguridad (seguridad 1.0) comienza preguntándose por qué las cosas salieron mal, intentando luego buscar las causas presuntas para asegurarse que el episodio no vuelva a ocurrir. Es decir que busca restituir el trabajo al modo en que se lo imaginó. La alternativa sería preguntarse por qué las cosas salieron bien (o por qué nada salió mal), y tratar luego de asegurarnos que esto suceda siempre. Es ahí donde entramos en el terreno de la Seguridad 2.0.

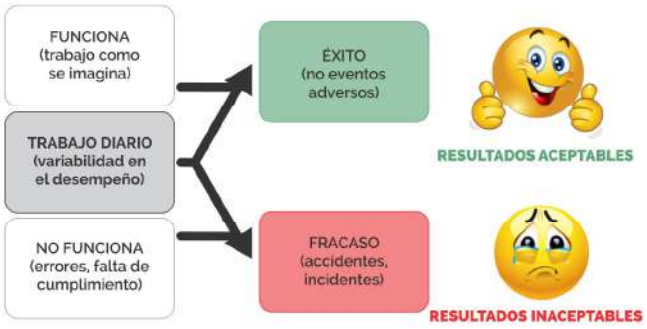
SEGURIDAD 2.0: UNA NUEVA VISIÓN

Durante el curso normal del trabajo clínico, los médicos, enfermeros y personal auxiliar se desempeñan con seguridad porque son capaces de ajustar su trabajo a las distintas condiciones que se les presentan. En sistemas más manejables y con buena ingeniería (como la aviación, la industria minera y las manufacturas, pero también por ej. en la producción farmacéutica) la necesidad de ajustes será muy pequeña. En muchos casos también existe la opción de detener o diferir las operaciones hasta que las circunstancias sean más favorables, como cuando se cancelan vuelos por malas condiciones climáticas o por problemas mecánicos. Algunas compañías industriales incluso cierran temporalmente sus plantas hasta solucionar el problema.

Sin embargo, la naturaleza misma de la atención médica hace que la misma se vuelva a menudo inmanejable, obligando, para que el sistema funcione, a realizar ajustes sobre la marcha. En muchas circunstancias, la precariedad de las circunstancias hace también imposible que se pueda detener o diferir el tratamiento de un paciente, aún cuando las condiciones de trabajo sean malas.

Dada la incertidumbre, intratabilidad y complejidad del trabajo médico, lo que sorprende no es que las cosas salgan ocasionalmente mal, sino que salgan bien tan a menudo. Sin embargo, como hemos visto, cuando tratamos de mejorar la seguridad, nos focalizamos en las pocas cosas que salen mal en vez de hacerlo sobre las muchas cosas que salen bien. Sin embargo, nuestra atención a los raros casos de fallas atribuibles al "error humano" no nos permite explicar por qué el desempeño humano prácticamente siempre obtiene buenos resultados ni cómo ayuda a cumplir con los objetivos de la atención en salud. El foco sobre la falta de seguridad no nos indica la dirección en la que debemos ir para mejorar la seguridad.

La solución a esto sería sorprendentemente simple: en vez de fijarnos solo en los pocos casos que salieron mal, deberíamos también atender los muchos casos que salen bien y tratar de entender por qué. Deberíamos también reconocer que las cosas salen bien porque los médicos y el resto del personal de salud son capaces de ajustar su trabajo a las distintas condiciones y no porque trabajan como se lo imaginó. La ingeniería de la resiliencia reconoce que los buenos resultados y los eventos adversos tienen una misma base común: los ajustes en el desempeño de todos los días. (ver Figura 4.)



Como muchas situaciones del trabajo médico resultan intratables (difíciles de seguir o de conocer cómo funcionan), es prácticamente imposible detallar minuciosamente qué es lo que siempre debería hacerse, excepto para cosas muy simples. La razón por las cual las personas trabajan efectivamente bajo condiciones cambiantes es su constante adaptación a lo que otras personas hacen o es probable que hagan. A medida que los sistemas de salud continúen expandiéndose, tanto de manera vertical como horizontal y su intratabilidad siga creciendo, estos ajustes serán cada vez más importantes y necesarios para un desempeño efectivo. Las adaptaciones sobre la marcha representan por ende tanto un desafío como una oportunidad para la gestión en seguridad.

De acuerdo a esta visión, deberíamos dejar de tratar las fallas como eventos únicos e individuales y empezar a verlas como una expresión de la variabilidad en el desempeño de todos los días. Excluyendo algunas actividades excepcionales, es casi seguro que algo que salió mal había salido bien muchísimas veces antes y que volverá a salir bien en el futuro. Entender el por qué de los buenos resultados es la base necesaria para comprender cómo ocurren los eventos adversos. En otras palabras, cuando algo sale mal, deberíamos comenzar el análisis comprendiendo cómo usualmente sale bien, en vez de buscar causas específicas que sólo explican la falla. Los eventos adversos se deben más a combinaciones de variabilidades en el desempeño bien conocidas que a distintas fallas o malfuncionamiento de los procesos.

Pese a los constantes esfuerzos para manejar las distintas variables y normatizar, las distintas situaciones que presenta la atención de la salud se vuelven cada vez más inabarcables. Irónicamente, una de las razones de esto es nuestra limitada capacidad para prever las consecuencias de los cambios en el diseño de los procesos (tanto de las consecuencias buscadas como de los efectos adversos). Este problema fue abordado hace muchos años en una discusión sobre la automatización, donde Bainbridge (1983) puntualizó que "*el diseñador que busca eliminar al operador, aún deja que este último realice las tareas que el propio diseñador no sabe cómo automatizar.*". Este argumento aplica no sólo al diseño en automatización sino también a las especificaciones y el diseño del lugar de trabajo de la atención de salud en general. Cuanto más complicada sea una situación de trabajo, mayor será la incertidumbre acerca de los detalles. Y el trabajo clínico es extremadamente complejo, requiriendo altos niveles de criterio y juicio profesional para que la atención se adecue a las distintas circunstancias de pacientes con múltiples morbilidades.

Las premisas para la gestión en seguridad en la actualidad podrían entonces ser resumidas de la siguiente manera:

- El trabajo clínico y los sistemas no pueden ser descompuestos de una manera significativa (no tienen "elementos" o "componentes" naturales)

- El funcionamiento de los sistemas no es bimodal, pudiendo clasificarlos en "funciona" o "no funciona". El desempeño de todos los días es –y debe ser- flexible y variable.

- Los resultados emergen de la variabilidad del desempeño humano, que es a su vez la fuente tanto de las buenas evoluciones como de los eventos adversos.

- Mientras que algunos eventos adversos pueden ser atribuidos a fallas y mal funcionamiento, otros son el resultado de la variabilidad en la ejecución de procesos entrelazados.

A consecuencia de todo esto, la definición de seguridad debería pasar de "evitar que algo salga mal" a "asegurar que todo salga bien". La seguridad 2,0 consiste en la capacidad del sistema para funcionar como debe bajo condiciones variables, de manera tal que el número de resultados buscados y aceptables sea lo más alto posible. La base de la gestión en seguridad debe ser por lo tanto la comprensión de por qué las cosas salen bien, lo que implica comprender las prácticas habituales reales de todos los días.
Garantizar que tanto como sea posible salga bien, en el sentido de que el trabajo clínico diario cumpla con sus propósitos, no puede depender exclusivamente de la respuesta ante las fallas, ya que de esta manera sólo podríamos corregir la recurrencia de algo que ya pasó. La gestión de la seguridad debe también ser proactiva, de forma tal que las intervenciones sean realizadas antes de que algo ocurra. Una gran ventaja de esto es que las acciones anticipadas, en general, requieren menos esfuerzos porque en caso de haberse producido el evento sus consecuencias dejarían menos tiempo para desarrollar y difundir las mejoras. Las respuestas tempranas ahorran también mucho tiempo. A continuación, describimos las características de la seguridad 2,0 con más detalle, profundizando sobre sus bases teóricas, sus mecanismos subyacentes y sus manifestaciones.

Las bases de la seguridad 2,0: Variabilidad en el desempeño en vez de bimodalidad

A diferencia de la Seguridad 1,0, la Seguridad 2,0 se basa en el principio de que los ajustes en el desempeño son la norma general y que este desempeño no sólo ***es*** variable sino que también ***debe*** serlo. Esto es así porque resulta imposible y no tiene mayor sentido caracterizar a los componentes de un sistema socio-técnico en términos de éxito/ fracaso o de buen/mal funcionamiento. Esta variabilidad, sin embargo, no debería ser interpretada negativamente como "desvíos de las normas", "violaciones al procedimiento" o "no cumplimiento". Por el contrario, la capacidad de hacer ajustes en las tareas es la principal contribución de los humanos al trabajo, sin la cual no se podrían realizar siquiera las tareas más sencillas.

Los "Mecanismos de la Seguridad 2,0: fenómenos emergentes en vez de causalidad

Como los ajustes y la variabilidad en el desempeño constituyen la base de la Seguridad 2.0, la primera conclusión lógica a la que se arriba es que los mecanismos no pueden depender de la causalidad y de la propagación lineal de causas y efectos. Si bien todavía es común atribuir la mayoría de los eventos adversos desperfectos o mal funcionamiento de componentes o funciones normales del sistema, cada vez son más los casos donde esto no es posible. En estos casos el resultado termina siendo un emergente y no un resultante. No por esto resulta imposible explicar qué es lo que pasó, pero las explicaciones serán de una naturaleza diferente. Por emergente no debe entenderse que algo ocurrió "mágicamente", sino que ocurrió de una manera que no puede ser explicada utilizando los principios de la descomposición y la causalidad. Este es típicamente el caso de los sistemas que son parcial o totalmente intratables.

La forma en la que usualmente explicamos cómo ocurrieron las cosas es rastreando hacia atrás los efectos a partir de sus causas, hasta que encontramos una causa raíz (o nos quedamos sin tiempo o dinero). Este abordaje es típicamente representado por los diagramas tipo "espina de pescado" (ver Fig. 5)

Figura. 5. Diagrama de espina de pescado utilizando una lógica lineal para rastrear un evento adverso

Según este modelo, cuando algo sale mal, existirá un cambio observable en algo (caso contrario no podríamos enterarnos de su ocurrencia). El resultado visible puede ser un error de lado quirúrgico, una infección o una falla diagnóstica. La Seguridad 1,0 asume que las causas de estos eventos son reales, siendo el propósito de la investigación de accidentes rastrear su desarrollo hacia atrás, desde el resultado observable hacia la causa eficiente. Estas causas también son "reales" en el sentido de que pueden ser asociadas a componentes o funciones que "fallaron" de alguna forma, donde esta falla puede hacerse visible post-facto o bien puede deducirse de los hechos. De manera similar, los proyectos de gestión de riesgos proyectan los posibles desarrollos futuros partiendo de la/s causas eficientes de posibles resultados. Estos proyectos generalmente comienzan con una base de datos de incidentes pasados y evalúan el riesgo de que ocurra algo similar en el presente o futuro.

En el caso de los fenómenos emergentes, en cambio, el resultado final también es por supuesto "observable" y "real", no siendo tan fácil de determinar las razones por las cuales aparecieron. El resultado final puede deberse, por ejemplo, a una condición o fenómeno transitorio que sólo existió en un punto particular del tiempo y del espacio: la enfermera tenía cefalea; el médico a cargo tuvo que ausentarse por un familiar enfermo; era el casamiento de la hija del jefe de servicio y todos estaban celebrando el evento; Estas condiciones pueden, a su vez, emerger de otros fenómenos transitorios (Ver Figura 6.)

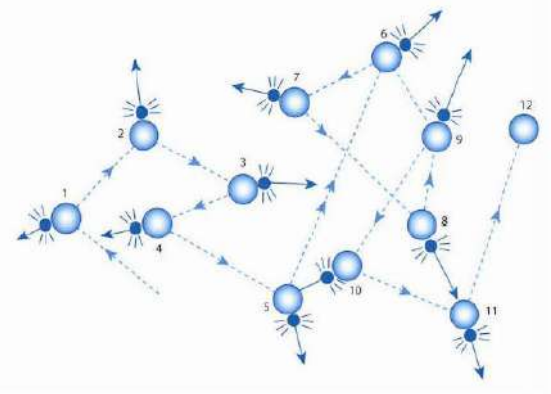


Figura 6: Fenómenos transitorios y emergentes

Las causas son por lo tanto reconstruidas (o inferidas) más que encontradas, y por lo tanto puede ser muy difícil eliminarlas o contenerlas de la manera usual; sin embargo sigue siendo posible controlar las condiciones que las llevaron a existir, siempre y cuando comprendamos cómo se trabaja normalmente.

Las manifestaciones de la Seguridad 2.0: Las cosas que salen bien

Las manifestaciones de la Seguridad 2.0 no son los eventos adversos sino todas las posibles evoluciones (ver Figura 7), especialmente aquellos resultados típicos o de alta frecuencia que son generalmente ignorados por la gestión de seguridad. El sistema continúa considerándose inseguro y peligroso si la frecuencia de eventos adversos es alta, pero resulta más importante comprender por qué es seguro cuando estos eventos adversos no ocurren. La seguridad es entonces definida por lo que sucede cuando está presente más que por lo que ocurre cuando está ausente, estando directamente relacionada con los resultados buenos y frecuentes. Cuanto más de estas manifestaciones haya, mayor será la seguridad del sistema, y viceversa. Esta visión permite demostrar que los esfuerzos por mejorar la seguridad redundan en beneficios, facilitando el argumento por más recursos humanos y financieros.

Existen pocas tipologías disponibles para ayudar a describir las manifestaciones de la Seguridad 2.0. A pesar de que las cosas salen mayoritariamente bien todo el tiempo, no tomamos conciencia de esto porque nos acostumbramos. Psicológicamente damos la seguridad por sentada. Pero como el trabajo diario no tiene nada de excepcional, puede ser explicado en términos relativamente sencillos. El desempeño de todos los días puede ser definido, por ejemplo, como aquellos ajustes que sirven para crear o mantener las condiciones de trabajo requeridas, que compensan la falta de tiempo, materiales, información, etc., y que tratan de evitar condiciones que se sabe perjudican la tarea. Y, como la variabilidad en el desempeño es ubicua, es más fácil de monitorear y manejar.

El camino hacia adelante

La Seguridad 1,0 y la 2,0 no son mutuamente excluyentes y ambos abordajes deben yuxtaponerse. Basar la gestión en seguridad en una u otra visión puede tener consecuencias indeseadas. Las principales diferencias se encuentran resumidas en la Tabla 1.

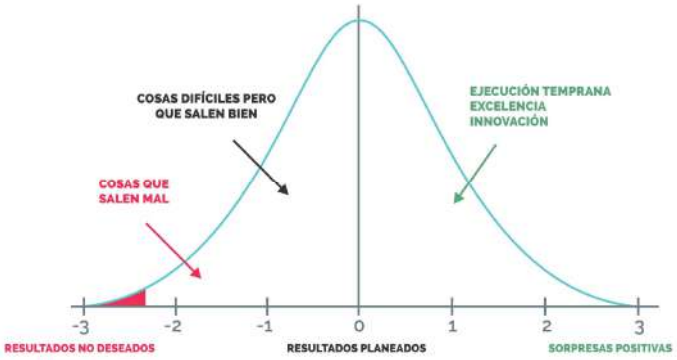


Figura 7: Probabilidad de eventos y foco de la seguridad

Lo que los médicos, enfermeros y resto del personal de salud hacen todos los días es generalmente una combinación de Seguridad 1.0 y Seguridad 2.0. El equilibrio depende de muchos factores, tales como la naturaleza del trabajo, la experiencia de las personas, el clima de la organización, las presiones por parte de las autoridades o de los pacientes y las distintas enfermedades, entre otros. Todos sabemos que es mejor prevenir que curar, pero las condiciones no siempre permiten que la prevención tenga el rol que merece.

Cuando se analizan las prioridades de quienes diseñan las políticas sanitarias, los reguladores y las autoridades de las instituciones, la visión que predomina es la de Seguridad 1,0. Una razón es que su objetivo primario ha sido históricamente garantizar que los pacientes o la población no estén expuestos a daños.

Cuando quienes diseñan las políticas sanitarias (autoridades, reguladores y directores de las instituciones) analizan sus prioridades, la visión que predomina es la de Seguridad 1.0. Una de las razones de esto es que el objetivo primario de estas personas ha sido históricamente garantizar que los pacientes o la población no estén expuestos a daños innecesarios. Otra razón es que estos niveles de decisión suelen encontrarse muy lejos en tiempo y espacio de las operaciones de la primera línea de atención, teniendo por lo tanto limitadas sus posibilidades de observar o experimentar cómo se trabaja realmente. Una tercera razón es que les resulta mucho más sencillo (o por lo menos así lo asumen) contar los pocos eventos que salieron mal que los muchos que evolucionaron favorablemente.

El personal de salud recibe muchas más presiones para ser eficientes ("hay que sacar las cosas") que para ser meticulosos en el trabajo diario. Este fenómeno determina que aparezca como menos legítimo destinar tiempo y esfuerzo para digerir y comunicar experiencias, ya que esto suele ser visto como no productivo, al menos en el corto plazo. Una gestión efectiva en seguridad requiere, sin embargo, cierto esfuerzo para pensar acerca de la forma en la que se trabaja, para brindar los recursos necesarios y para prepararse para lo inesperado. La presión por la eficiencia –que se manifiesta por ejemplo en el objetivo típico de ver cada vez más pacientes en el mismo tiempo, en la estandarización de los tratamientos en módulos o paquetes y en el acortamiento en los días de internación -, hace que esto sea muy difícil.

Puede ser también muy difícil gestionar la seguridad de manera proactiva para la miríada de eventos a pequeña escala que constituyen las distintas situaciones del trabajo diario. Las cosas pueden desarrollarse de manera rápida e inesperada, hay pocos indicadores y los recursos a menudo suelen ser escasos. El ritmo de las tareas deja muy pocas oportunidades para reflexionar sobre lo que está pasando y para actuar estratégicamente. De hecho, las presiones del trabajo y las demandas externas a menudo necesitan soluciones oportunistas que fuerzan al sistema a trabajar de modo reactivo. Para salir de esta trampa y pasar del modo reactivo al proactivo se requiere de un esfuerzo deliberado. Y, si bien esto puede parecer una pérdida de recursos en el corto plazo, es sin duda una sabia inversión en el largo.

Por otra parte, puede llegar a ser relativamente sencillo preparase proactivamente para garantizar la seguridad ante eventos a gran escala porque se desarrollan de una manera relativamente lenta, aún cuando pueden empezar de manera abrupta. Un ejemplo podría ser una huracán o una tormenta mayor que pueda causar destrozos materiales y víctimas fatales o una pandemia), Existen en estos casos claros indicadores de cuándo se necesita la respuesta y de cómo debe ser la misma. Es por lo tanto más fácil estar preparado de manera anticipada.

Como ya dijimos, resulta importante destacar que la Seguridad 1.0 y la Seguridad 2.0 representan dos visiones complementarias de la seguridad más que dos abordajes incompatibles o en conflicto. Muchas de las

prácticas actuales pueden por lo tanto continuar utilizándose, aunque tal vez con distinto énfasis. Pero la transición desde la Seguridad 1.0 a la Seguridad 2.0 requiere también del desarrollo de nuevas prácticas, algunas de las cuales se describen a continuación.

La transición: De Seguridad 1.0 a la Seguridad 2.0

Fijarse en lo que sale bien

Un mensaje clave: Estudie tanto lo que sale bien como lo que sale mal y aprenda tanto de lo que funciona como de lo que falló. De hecho, no deberíamos esperar a que algo malo suceda para tratar de comprender qué es lo que realmente ocurre en situaciones comunes y rutinarias. Las cosas no salen bien simplemente porque las personas cumplan al pie de la letra las normas y procedimientos o porque trabajen como se lmaginó al diseñar los procesos. Las cosas salen bien porque las personas hacen ajustes razonables de acuerdo a lo que demandan las distintas situaciones que se les presentan. Descubrir cuáles son estos ajustes y tratar de aprender de ellos es al menos tan importante como encontrar las causas de los eventos adversos.

Las cosas que salen mal, como podría ser un brote infeccioso, un quiebre en la comunicación, un error de medicación o un error de sitio quirúrgico, generalmente no surgen de circunstancias únicas o extraordinarias. Lo más probable es que bajo esas mismas circunstancias las cosas se vinieran haciendo muy bien y que se sigan haciendo bien en el futuro. Por eso es necesario comprender cómo las actividades del día a día salen bien – la forma en la que tienen éxito-, para poder comprender cómo podrían fallar. Desde la perspectiva de la seguridad 2.0, las fallas no se deben a errores o mal funcionamiento, sino a combinaciones inesperadas que surgen a partir del desempeño variable de todos los días.

La diferencia entre la visión de la seguridad 1.0 y la de la seguridad 2.0 se ilustra en la Figura 8. La seguridad 1.0 se focaliza en eventos que ocurren en la cola de la distribución normal, y especialmente en la zona dentro de ese desvío estándar que representan accidentes. Estos eventos son fáciles de ver porque son excepcionales y porque los resultados difieren mucho de lo habitual. Son, sin embargo, difíciles de explicar, más allá del atractivo que tienen los análisis de causa raíz y los modelos de análisis lineales. Como son excepcionales y como son difíciles de comprender, son también difíciles de cambiar y manejar.

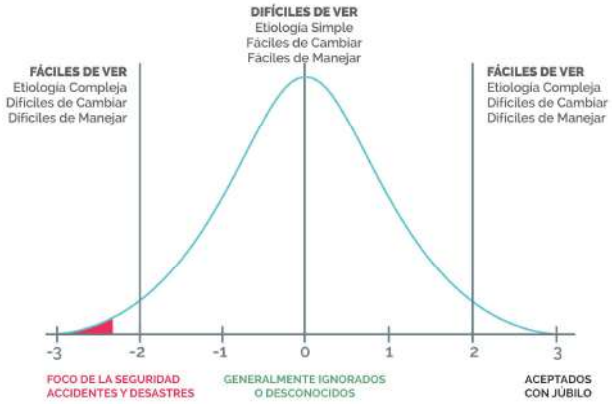


Figura 8. : Relación entre la probabilidad de los eventos y la facilidad de precepción

La Seguridad 2.0 se focaliza en los eventos en la mitad de la distribución. Estos son "difíciles" de ver, pero sólo porque habitualmente los tenemos automatizados y los ignoramos en nuestras actividades diarias. La "lógica" sería que no tiene mayor sentido perder tiempo para analizar las cosas que funcionan. Pero el núcleo del problema es que las cosas generalmente no funcionan de la forma que pensamos y asumimos, y el trabajo real puede diferir de manera significativa del trabajo como está planeado. Estos eventos en la mitad de la campana de Gauss pueden ser comprendidos y explicados en términos de ajustes mutuos en las tareas que terminan siendo la base del trabajo diario. Como estas acciones son frecuentes, como son de de pequeña escala y porque podemos comprender más fácilmente cómo y por qué ocurren, son fáciles de monitorear y de manejar. Las intervenciones entonces son muy focalizadas y de un alcance limitado (porque el problema en cuestión suele no ser complicado), resultando por lo tanto más fácil – aunque no necesariamente siempre- anticiparse a los efectos principales y secundarios de estas actividades.

Por supuesto que parece beneficioso no prestarle demasiada atención a las tareas rutinarias mientras las mismas no tengan la posibilidad de dañar o mientras el ambiente de trabajo se mantenga estable. Pero en

nuestra sociedad, el ambiente de trabajo ya no es más estable y por lo tanto dicho beneficio es ilusorio.

El ambiente de trabajo, y por lo tanto el trabajo en sí mismo es cada vez más impredecible. Esto determina que las rutinas que funcionan bien hoy pueden no funcionar mañana, y por lo tanto es importante saber cómo funcionan. Esta exhaustividad en el análisis de lo que funciona bien es el que nos permitirá ser eficientes cuando llegue el tiempo de hacer cambios y de realizarlos de manera rápida.

Foco en eventos frecuentes

Un segundo mensaje: fíjese en lo que ocurre habitualmente y focalícese en los eventos basándose en su frecuencia más que en su severidad. Muchas pequeñas mejoras en las tareas diarias pueden ser más efectivas que una gran mejora a partir de un hecho aislado y excepcional.

La investigación de los incidentes generalmente se encuentra muy limitada por tiempo y recursos. Por la tanto, existe la tendencia a estudiar los incidentes que han tenido serias consecuencias y dejar el resto para otro momento, que nunca llega. Se asume tácitamente que el potencial de aprendizaje es proporcional a la severidad del incidente o accidente.

Esto es un error. Si bien es cierto que se ahorra más dinero evitando un accidente de gran escala que uno pequeño, eso no significa que el potencial de aprendizaje sea mayor en el primer caso. Además, el costo acumulado de incidentes frecuentes y de pequeña escala puede ser igual o mayor al del gran accidente. Y como los eventos pequeños pero frecuentes son más fáciles de comprender y de manejar, tiene mayor sentido concentrarnos en ellos más que en eventos excepcionales de grandes consecuencias.

Permanecer alerta a la posibilidad de fallas

Un tercer mensaje es: si bien la Seguridad 2.0 se focaliza en las cosas que salen bien, aún resulta necesario recordar siempre que las cosas pueden salir mal y mantener una alta sensibilidad a la posibilidad de fallas. La “falla posible” en este casono es tan solo algo que pueda funcionar mal, como en la visión de la Seguridad 1.0, sino también que no se obtengan los resultados deseados (que fallemos para garantizar que las cosas salgan bien)

Asegurarse que las cosas salgan bien requiere una preocupación constante por estudiar cualquier cosa que funcione bien, no solo para garantizar que continúe haciéndolo sino también para contrarrestar la tendencia a favorecer, buscar, interpretar y recordar la información que confirma las propias creencias o hipótesis, dando desproporcionadamente menos consideración a posibles alternativas (sesgo de confirmación)

Para permanecer sensibles a la posibilidad de fallas, es necesario crear y mantener una visión abarcadora del trabajo como se realiza, tanto en el corto como en el largo plazo. Esto permitirá anticiparse y por lo tanto prevenir la combinación de pequeños problemas o fallas, apuntando a los pequeños ajustes que pueden reducir combinaciones potencialmente peligrosas en la variabilidad de las tareas. Muchos eventos adversos sobrevienen del agregado oportunista de atajos en combinación con inadecuados procesos de supervisión o de identificación de peligros. Permanecer sensible a lo que ocurre, tanto a las formas en las cuales se puede tener éxito o fracasar, resulta importante en la visión de la Seguridad 2.0

Ser tan exhaustivo como eficiente

Un cuarto mensaje: no privilegie la eficiencia por sobre la meticulosidad, o al menos no lo haga exageradamente. Si la mayoría del tiempo se utiliza para ver “cómo se llega a fin de mes” , habrá nulo o poco tiempo para consolidar experiencias o para comprender el trabajo como realmente se realiza. Debe ser bien visto dentro de la cultura organizacional destinar recursos, especialmente tiempo, para reflexionar, compartir experiencias y aprender. Si ese no es el caso, ¿cómo puede pretenderse que algo mejore?
La eficiencia del presente no pudo ser alcanzada sin exhaustividad en el pasado. Y de la misma manera, la eficiencia en el futuro no puede ser alcanzada sin exhaustividad en el presente (es decir, sin planificación y preparación). Si bien la meticulosidad puede ser vista en el presente como una pérdida de productividad (eficiencia), es una condición necesaria para la eficiencia en el futuro. Para poder sobrevivir a largo plazo resulta por lo tanto esencial conseguir algún tipo de equilibrio.

Invertir en seguridad para ganar

Un quinto y último mensaje: hacer que las cosas salgan bien no solo es una inversión en seguridad sino también en productividad. El tiempo destinado a aprender, pensar y comunicarse es habitualmente percibido como un costo. Esto refleja la visión de la Seguridad 1.0, donde las inversiones en seguridad se hacen para prevenir que algo malo ocurra. Sabemos los costos, como cuando compramos un seguro. Pero no sabemos a ciencia cierta cuánto es lo que hemos ahorrado, ya que el potencial evento es incierto y desconocemos su eventual magnitud.

En el negocio del riesgo, existe un adagio común que sostiene *"si usted piensa que la seguridad es cara, pruebe con un accidente".* Y si calculamos los costos de un accidente mayor, como el de Betsy Lehman, una paciente con cáncer que falleció luego de recibir cuatro veces la dosis de quimioterapia o de Willie King, un paciente diabético de 51 años al cual se la amputó el miembro equivocado, casi cualquier inversión en seguridad aparecerá como costo-efectiva. Sin embargo, como no podemos probar que las actuales precauciones de seguridad son o fueron las razones por las cuales los accidentes no ocurrieron en nuestras instituciones, y como no podemos precisar cuándo es probable que estos accidentes ocurran, se termina reduciendo la inversión en seguridad, sobre todo en tiempos duros con bajos márgenes de rentabilidad.

En el mundo de la Seguridad 1.0, las inversiones en seguridad son vistas como un gasto no productivo. Entonces, si se realizó una inversión y no hubo ningún finalmente ningún accidente, se lo termina considerando como un gasto probablemente innecesario. Si hay o hubo accidentes, es vista como una inversión justificada. Si no se realiza ninguna inversión, pero tampoco se registran accidentes, es la decisión es vista como un ahorro justificado. Por último, si no se invirtió y finalmente ocurren los accidentes, se considera que se tuvo mala suerte o que hubo un error en la toma de decisiones ("deberíamos haber invertido…").

En la Seguridad 2.0, en cambio, la inversión en seguridad es vista también como una inversión en la productividad, ya que la definición – y el propósito- de la Seguridad 2.0 es hacer que la mayor cantidad de cosas posibles salgan bien. Entonces, si se realiza la inversión y no se producen accidentes, aún así se continuará mejorando el desempeño de todos los días. Si ocurren accidentes, la inversión volverá a aparecer como plenamente justificada. Si no se invierte y no ocurren accidentes, el desempeño continuará siendo aceptable pero no mejorará, mientras que si los accidentes ocurren, la falta de inversión será vista como una mala decisión.

Conclusión

Como la atención de la salud depende de sistemas socio-técnicos cada vez más complejos, comienza a ser claro que el abordaje 1.0 a la seguridad puede resultar inadecuado, tanto en el corto como en el largo plazo. La decisión de optar por un abordaje tipo Seguridad 2.0 no debería resultar difícil.

Sin embargo, el futuro no consistiría en reemplazar un abordaje por otro, sino en combinar las dos formas de pensamiento (ver Figura 9.). Es todavía cierto que la mayoría de los eventos adversos son relativamente simples (o pueden ser tratados de manera simple sin consecuencias serias) y que podemos lidiar con ellos de una manera que nos resulta familiar. Pero hay un creciente número de casos en los cuales esa forma de abordaje no funciona. Para estos, es necesario adoptar la visión de la seguridad 2.0, lo que esencialmente significa adoptar una visión resiliente de la atención.

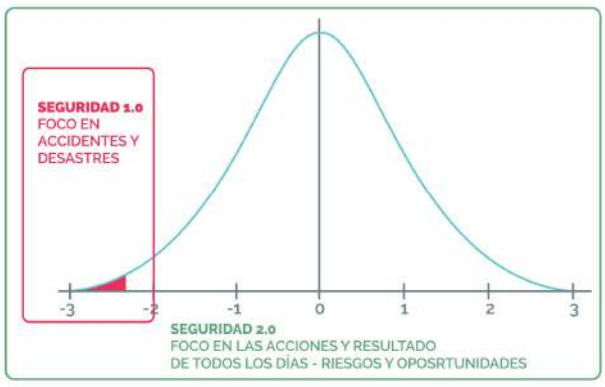


Figura 9. : Foco en Seguridad 1.0 y Seguridad 2.0

La Seguridad 2.0 es ante todo una forma diferente de mirar a la seguridad, en donde también se aplican de manera diferente muchos de los métodos y técnicas más familiares de la Seguridad 1.0. Sin embargo, la

Seguridad 2.0 deberá a su vez desarrollar sus propios métodos para observar y saber cómo funcionan las cosas que salen bien y para manejar la variabilidad en el desempeño, más que restringirla.

Epílogo

La introducción de una comprensión distinta del mundo en el que vivimos, trabajamos y del cual dependemos requiere de algo parecido a un cambio de paradigma. Los estudiosos de la seguridad han desarrollado un consenso acerca de cómo funcionan las cosas y cómo puede garantizarse la seguridad, pero el aumento de conocimientos parece estar llegando a una meseta y el problema de los eventos adversos ha continuado creciendo. Debemos afrontar el hecho de que el mundo no puede ser explicado sólo por modelos de causa-efecto. Los incidentes y accidentes no sólo ocurren de manera lineal, sino que en su génesis influyen fenómenos emergentes que provienen de la complejidad del sistema de atención de la salud en general. Preguntarse por qué una cosa generó otra no termina siendo suficiente para explicar el sistema en uso y no lleva a mejorar la seguridad.

Este cambio de paradigma obligará a los expertos en seguridad a salir de su "zona de confort" y explorar nuevas oportunidades. En ese nuevo mundo, tanto los gerentes como los profesionales asistenciales deberán buscar los modelos y métodos a utilizar. Algunos métodos ya se encuentran disponibles y han sido aplicados en diferentes ámbitos. Por ejemplo, el Functional Resonance Analysis Method (FRAM; Hollangel 2012, busca identificar y describir las funciones esenciales de un sistema, caracterizando la potencial variabilidad de estas funciones y definiendo su resonancia sobre el sistema basándose en las interrelaciones y dependencias entre las funciones. Se buscan luego formas de monitorear el desarrollo de la resonancia, ya sea para favorecer las variabilidades deseadas y amortiguar el efecto de las variabilidades que pueden desembocar en eventos adversos (www.functionalresonance.com)

El nuevo paradigma también implica que las prioridades de la gestión en seguridad también deben cambiar. En vez de conducir las investigaciones luego de del evento o de esforzarse solo por reducir eventos adversos, la gestión en seguridad debería destinar algunos recursos al estudio de los eventos que salen bien y tratar de aprender de ellos. En lugar de aprender de los eventos más severos, deberíamos tratar de aprender de los más frecuentes. Y en lugar de analizar un solo evento grave en profundidad, deberíamos explorar la regularidad del abanico de muchos eventos frecuentes para comprender los patrones que determinan el desempeño del sistema. Una buena forma de empezar sería comenzar a reducir la dependencia del "error humano" como la causa casi universal de los incidentes y comprender en cambio la necesidad de la variabilidad en el desempeño.

Agradecimiento

Al Dr. Pablo Lemos, Jefe de Internación Clínica del Hospital Privado de Córdoba y gran estudioso de la seguridad de los pacientes, quien me introdujera en esta nueva visión y compartiera conmigo el artículo original

Aclaración

Los autores del artículo original en inglés en ningún momento hacen referencia a los términos 1.0 o 2.0. Siempre hablan de Safety-I y Safety-II. Opté por utilizar esta terminología tan en boga en el mundo de la tecnología porque me parece que refleja muy bien el concepto de una nueva generación de conceptos y herramientas.

Bibliografía

Este artículo resulta de traducir de manera libre al español el núcleo del siguiente documento:

- Hollnagel E, Wears R.L and Braithwaite J. *"From Safety-I to Safety-II: A White Paper."* The Resilient Health Care Net: Published simultaneously by the University of Southern Denmark; University of Florida, USA, an Macquirie University, Australia. (2015)

Si bien se respeta el sentido del texto, no sigue fielmente la forma de expresión de la obra original.

A continuación las referencias citadas en el artículo

- Altman, L. (1995). 'Big doses of chemotherapy drug killed patient, hurt 2d'. The New York Times, 24 March.
- Bainbridge, L. (1983). Ironies of automation. Automatica, 19(6), 775-779.
- Clary, M. (1995). 'String of Errors Put Florida Hospital on the Critical List'. Los AngelesTimes, 14 April.: http://articles.latimes.com/1995-04-14/news/mn-54645_1_american-hospital.
- EUROCONTROL (2009). A white paper on resilience engineering for ATM. Brussels: EUROCONTROL.
- Finkel, M. (2011). On Flexibility: Recovery from Technological and Doctrinal Surprise on the Battlefield. Stanford, CA: Stanford University Press.
- Heinrich, H. W. (1931). Industrial accident prevention: A scientific approach. New York: McGraw-Hill.
- Hollnagel, E. (2009). The ETTO principle: Efficiency-thoroughness trade-off. Why things that go right sometimes go wrong. Farnham, UK: Ashgate.
- Hollnagel, E. (2012). FRAM: The Functional Resonance Analysis Method. Farnham, UK: Ashgate.
- Hollnagel, E., Braithwaite, J. & Wears, R. L. (2013) Resilient health care. Farnham, UK: Ashgate.
- Hollnagel, E., Woods, D. D. & Leveson, N. G. (2006). Resilience engineering: Concepts and precepts. Aldershot, UK: Ashgate.
- Leveson, N. G. (2004). A new accident model for engineering safer systems. Safety Science, 42(4), 237-270.
- Rasmussen, J. & Svedung, I. (2000). Proactive risk management in a dynamic society. Karlstad, Sweden: Swedish Rescue Services Agency.
- Reason, J., Shotton, R., Wagenaar, W. A., Hudson, P. T. W. & Groeneweg, J. (1989). Tripod: A principled basis for safer operations. The Hague: Shell Internationale Petroleum Maatschappij.
- Reason, J. T. (1997). Managing the risks of organizational accidents. Aldershot, UK: Ashgate Publishing Limited.
- Reason, J., Hollnagel, E., & Paries, J. (2006). *Revisiting the Swiss Cheese Model of Accidents*. EUROCONTROL. Brétigny-sur-Orge, FR. Retrieved 6 October 2008, from http://www.eurocontrol.int/eec/gallery/content/public/documents/EEC_notes/2006/EEC_note_2006_13.pdf.
- Shorrock, S. and Licu, T. (2013). Target culture: lessons in unintended consequences. HindSight 17. Brussels: EUROCONTROL.
- Taylor, F. W. (1911). The principles of scientific management. New York: Harper.
- Wears, R. L. and S. J. Perry (2006). Free fall - a case study of resilience, its degradation, and recovery, in an emergency department. 2nd International Symposium on ResilienceEngineering, Juan-les-Pins, France, Mines Paris Les Presses.

- Wears, R. L., Hollnagel, E. & Braithwaite, J. (2015) The resilience of everyday clinical work. Farnham, UK: Ashgate.

- WHO (2014). NCD* death rate, age standardized (per 100 0000 population, 200-2012. http://gamapserver.who.int/gho/interactive_charts/ncd/mortality/total/atlas.html.

Tabla 1: Resumen de la Seguridad 1,0 y la Seguridad 2,0

	Seguridad 1.0	Seguridad 2.0
Definición de Seguridad	Que la menor cantidad de cosas posibles salgan mal	Que la mayor cantidad de cosas posibles salgan bien
Forma de abordaje	Reactivo, respondiendo cuando algo ocurre o es categorizado como un riesgo inaceptable	Proactivo, buscando continuamente anticiparse a los desarrollos y eventos
Visión del factor humano	Los humanos son vistos predominantemente como una carga o peligro. Son un problema a resolver	Los humanos son vistos como un recurso necesario para la flexibilidad y resiliencia del sistema. Brindan soluciones flexibles a muchos problemas potenciales
Investigación de accidentes	Los accidentes son causados por fallas y mal funcionamiento. El propósito de la investigación es identificar las causas	Las cosas ocurren básicamente de la misma manera, más allá del resultado. El propósito de la investigación es comprender cómo las cosas generalmente salen bien como base para explicar cómo pueden ocasionalmente salir mal
Evaluación de riesgos	Los accidentes son causados por fallas y mal funcionamiento. El propósito de la investigación es identificar las causas y los factores contribuyentes	Comprender las condiciones por las cuales puede llegar a ser muy difícil o imposible el monitoreo y control de la variabilidad en el desempeño