RAYENSALUD

UNA MIRADA AL USO Y CUIDADOS DE SISTEMAS CRÍTICOS: REGISTRO CLÍNICO ELECTRÓNICO

CONDICIONES HABILITANTES PARA EL BUEN DESEMPEÑO DE LAS SOLUCIONES TECNOLÓGICAS QUE SE UTILIZAN EN LOS ESTABLECIMIENTOS DE SALUD

RAYEN SALUD, empresa chilena de desarrollo e implementación de soluciones tecnológicas para el sector Salud, en su permanente compromiso por acompañar el significativo quehacer de las Redes de Salud y el despliegue de sus funcionarios por entregar una atención más oportuna, segura y de calidad para las personas, elaboró el presente documento, como aporte a los ámbitos de soporte y mantenimiento de sistemas de carácter crítico que llevan a cabo los profesionales y técnicos informáticos de los Establecimiento de Salud.

Esto, además, como un marco teórico en materia de condiciones habilitantes para que las soluciones tecnológicas que se utilizan en los Establecimientos de Salud se constituyan como importantes aliadas en la entrega de una mejor atención en salud para las personas.

RAYENSALUD

UNA MIRADA AL USO Y CUIDADOS DE SISTEMAS CRÍTICOS: REGISTRO CLÍNICO ELECTRÓNICO

Más allá de los Sistemas de Información, el uso de herramientas tecnológicas de carácter crítico en los Establecimientos de Salud -que apoyan la gestión sanitaria y que abordan integralmente los procesos clínicos y administrativos en la atención a las personas- requiere que los equipos informáticos locales configuren y mantengan los perímetros de seguridad y habilitantes tecnológicos adecuados, para asegurar su buen funcionamiento.

En la misma línea, se requiere tener en cuenta la dinámica y evolución permanente de las funcionalidades de las distintas soluciones tecnológicas, junto a sus integraciones, como parte fundamental del proceso integral de Transformación Digital de los Establecimientos de Salud y, por tanto, de las Redes Asistenciales, puesto el cambio y actualización constantes también demandan recursos, ajustes y habilitantes tecnológicos adicionales.

En ese sentido, es importante entender que el desempeño de los sistemas altamente interoperables, como el Registro Clínico Electrónico, depende del buen ejercicio del ecosistema tecnológico que lo habilita, como el sistema eléctrico, los puntos de red, navegadores vigentes; entre otros.

Por ello, con el objeto de colaborar en este ámbito, a continuación sugerimos algunas condiciones de fácil incorporación y seguimiento, que permiten mejorar el desempeño de las herramientas disponibles y robustecer el ecosistema tecnológico habilitante de los Establecimientos de Salud para su Transformación Digital:

RAYENSALUD

1. **Asegurar la disponibilidad de electricidad:**

   En lo posible y ante eventuales cortes de energía, se sugiere contar con una **red de fuerza alternativa,** como generadores o UPS (Sistema de Fuerza Ininterrumpible), para mantener el suministro eléctrico.

2. **Resguardar tecnológicamente las estaciones de trabajo:**

   El equipamiento tecnológico de las estaciones de trabajo debe estar actualizado con sistemas operativos que tengan **respaldo y soporte del fabricante**. Esto es sumamente necesario, dado que permite tener acceso a las actualizaciones recurrentes de seguridad y estabilidad por parte del proveedor.

   Del mismo modo, el equipamiento debe contar con -al menos- recursos equivalentes a un **procesador Intel i5 de sexta generación y 4GB de memoria**. Además, se le debe incorporar un sistema de **antivirus y antimalware**, actualizados y de fabricantes conocidos, que den un nivel de seguridad aceptable.

   En algunos casos, los sistemas ofrecen opciones de cortafuego, filtro de contenido y análisis de correos, los cuales son buenas opciones de protección global. En caso de tenerlos, se recomienda **identificar y tener cuidado con los filtros de contenido**, dado que la información clínica puede ser interpretada por ellos como “no apropiada” y, por consiguiente, bloqueada por el sistema de antivirus. Por ello, se deben agregar las excepciones del caso, para no presentar inconvenientes en la operación de los Sistemas de Información Clínica.

   Para mayor resguardo, es recomendable el respaldo y cifrado de la información sensible contenida en las estaciones de trabajo. Para ello, existen herramientas propias del sistema operativo, tales como, Windows Backup y Bitlocker.

3. **Configurar las Redes de Datos:**

   Una red en buenas condiciones permite una buena gestión y velocidad en la transmisión de datos. En lo posible, se sugiere contar con e**quipos de comunicaciones modernos y actualizados, de no más de 5 años, en una estructura de estrella** -que es la más recomendada- en la que los nodos superiores en jerarquía sean de mayor capacidad que los inferiores, con el fin de evitar “cuellos de botella”.

   Otro ámbito relevante es que la habilitación de los puntos de red sea certificada, es decir, que sean revisados y validados, utilizando herramientas de medición. Esto asegura que la transmisión de datos sea óptima y sin pérdidas.

Es importante considerar en la topología y/o disposición de la red, **enrutadores de buena capacidad**, acordes al volumen de datos a intercambiar e interconectar, como también, al número de estaciones de trabajo y sistemas que se quieran gestionar.

Por otro lado, es fundamental no olvidar **tener un buen firewall**, de capacidades y controles de seguridad idóneos para el resguardo de la información clínica, que permitan priorizar servicios por sobre otros y definir reglas de acceso, para controlar el tráfico y uso de los recursos de red y enlaces de comunicaciones, gestionando y habilitando los accesos requeridos a través de solicitudes específicas y no genéricas. Además, es recomendable implementar un **procedimiento para la gestión de accesos**.

También se deben **mantener en constante revisión las capacidades de los equipos de comunicaciones con sus firmwares actualizados**.

Todos los días aparecen nuevas vulnerabilidades, que vienen abordadas y corregidas en las actualizaciones de los equipos de comunicaciones.

Finalmente, es altamente recomendable **definir segmentación de redes, aplicado a los roles y actividad de los usuarios, con reglas de acceso entre cada segmento**, acorde a las funciones de las personas que utilizarán las estaciones de trabajo y al acceso a la información que se les desea dar. Esto permite tener un control más fino de lo que puede hacer cada uno y hasta dónde puede tener acceso, con el propósito de resguardar y controlar el acceso a la información crítica.

4. **Asegurar la disponibilidad del acceso a Internet:**

   En lo posible, contar con enlaces a internet redundantes y controlados, es decir, que los sistemas críticos de apoyo a la atención clínica tengan prioridad por sobre otros sistemas, como sitios de ocio y servicios de streaming de audio y video, tales como Facebook, YouTube y Spotify; entre otros.

   Del mismo modo, es importante contar con un nivel de enlace acorde a la cantidad de equipos y que asegure un tiempo de respuesta mínimo, es decir, con la menor latencia posible. Esto es crucial para un buen funcionamiento de los sistemas de información y el tiempo de respuesta de las peticiones que se realizan a través de ellos. Hay que considerar que un valor "aceptable" de latencia es de 40ms o menor, mientras que lo óptimo se encuentra por debajo de los 20ms.

   En la misma línea, debe ser una tarea permanente el monitorear el uso y consumo de los enlaces, estableciendo umbrales de intercambio y definiendo alertas en casos de desbordes, en cuanto a tamaño de paquetes y cantidad de accesos. Asimismo, establecer umbrales de consumo que se escapan a las actividades usuales, por ejemplo, la detección de uso de protocolos P2P para descarga (bitorrent u otros).

   También se sugiere habilitar filtro de contenidos, que controle los accesos a sitios permitidos (en lista blanca) y prohibidos y/o maliciosos (en lista negra), manteniendo un control y monitoreo de dichas listas.

   Finalmente, es significativo para un mejor desempeño de los sistemas el utilizar la Ruta 5D MINSAL, que es la red privada que tiene cobertura sobre todos los Establecimientos de Salud del país.

5. **Mantener los navegadores actualizados**

   Los sistemas web están en constante evolución, por tanto, el navegador o browser tiene una responsabilidad importante en el funcionamiento de un sistema y debe estar siempre actualizado a su última versión disponible.

   Estas actualizaciones están disponibles siempre y cuando el navegador esté corriendo en un sistema operativo vigente y con soporte por parte del fabricante.

   La importancia de su actualización y correcta configuración se debe a que día a día se encuentran nuevas amenazas de seguridad en los navegadores, las que ponen en riesgo a los sistemas web.

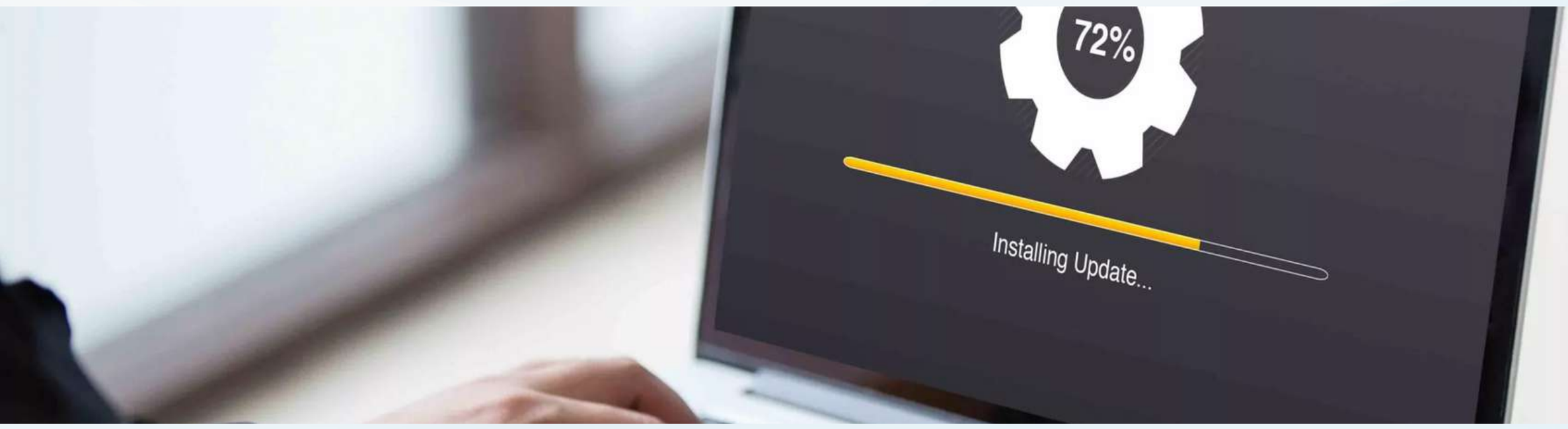
   Por ello, es recomendable deshabilitar versiones de navegadores declaradas como vulnerables y migrar a versiones más estables y seguras.

6. **Contar con un marco de ciberseguridad adecuado:**

   Para tener una visión completa de las vulnerabilidades y amenazas que corren los activos de información del Establecimiento de Salud, se deben tener en cuenta los tres pilares fundamentales de la Seguridad de la Información: Integridad, Disponibilidad y Confidencialidad. Esto permitirá gestionar y mitigar de mejor modo los riesgos a los que se enfrentan.

   Para esto, es ampliamente recomendable guiarse por un Sistema de Seguridad certificado bajo una norma y/o estándar internacional, como la ISO 27.001 (de Seguridad de la Información), la ISO 31.000 (de Gestión de Riesgos) o la ISO 22.301 (de Continuidad del Negocio); entre otras. Estas facilitarán el entendimiento sobre el alcance de lo que se debe evaluar y cómo hacerlo, como también, adelantarse a los riesgos, comprenderlos y abordarlos.

   Por otro lado, es muy importante contar con procesos de Gestión de Incidentes y protocolos de Escalamiento documentados, como también, cumplir con la legislación y regulaciones vigentes en el país.



Por lo general, los procesos de certificación bajo alguno de los estándares previamente mencionados, contemplan el análisis y cumplimiento de las normativas legales y de negocio, que deben ser revisadas, documentadas y controladas.

También es recomendable **realizar Pruebas de Penetración y/o Hacking Ético,** para evaluar los mecanismos de seguridad de los Sistemas de Información Clínica en uso. Estas son realizadas en ambientes y tiempos controlados, buscando y probando vulnerabilidades de los sistemas en sus capas de seguridad, desde un catálogo de posibilidades de fallas conocidas.

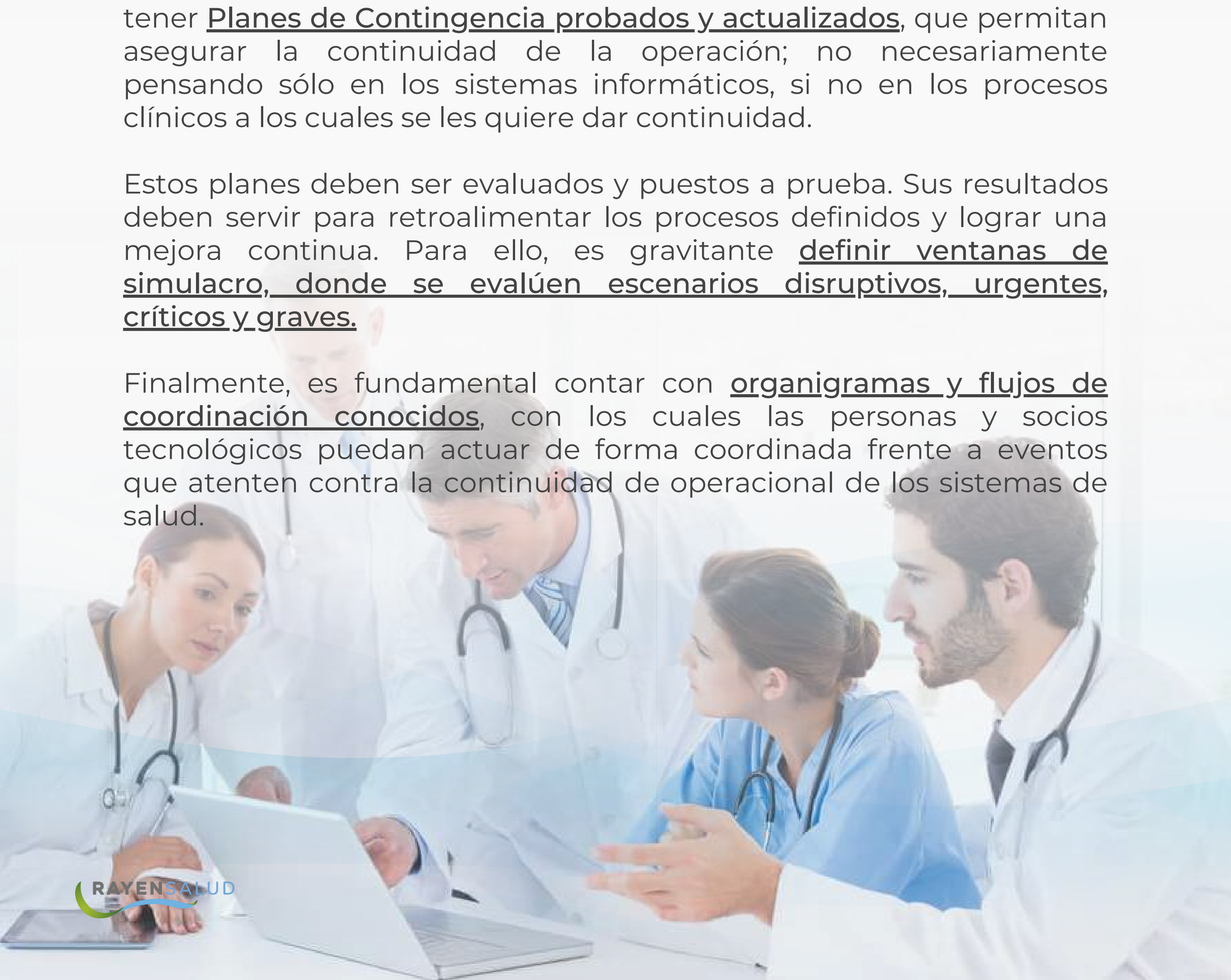
Finalmente, entendiendo que el eslabón más débil en materia de Seguridad de la Información son las personas, es recomendable **contar con un proceso periódico de capacitación sobre riesgos y vulnerabilidades de seguridad para quienes utilizan, administran y gestionan los sistemas de información crítica**, con educación que trascienda a lo netamente funcional o tecnológico, añadiendo buenas prácticas desde su rol como usuarios de los sistemas, generando una cultura de seguridad.

7. **Contar con planes de contingencia:**

   La tecnología no es infalible y el costo de implementar y mantener un sistema es exponencial en la medida que se aplican y requieren más niveles de seguridad y disponibilidad. Por tanto, es recomendable tener **Planes de Contingencia probados y actualizados**, que permitan asegurar la continuidad de la operación; no necesariamente pensando sólo en los sistemas informáticos, si no en los procesos clínicos a los cuales se les quiere dar continuidad.

   Estos planes deben ser evaluados y puestos a prueba. Sus resultados deben servir para retroalimentar los procesos definidos y lograr una mejora continua. Para ello, es gravitante **definir ventanas de simulacro, donde se evalúen escenarios disruptivos, urgentes, críticos y graves.**

   Finalmente, es fundamental contar con **organigramas y flujos de coordinación conocidos**, con los cuales las personas y socios tecnológicos puedan actuar de forma coordinada frente a eventos que atenten contra la continuidad de operacional de los sistemas de salud.



Mejorando directamente los niveles de ciberseguridad

La aplicación de estas sugerencias, además de optimizar la performance de los aplicativos, permite otorgar un mayor marco de seguridad a la gestión de la información de los pacientes, teniendo en cuenta el importante incremento en materia de ciberdelincuencia que se ha visto en los últimos años, especialmente de los ataques dirigidos hacia Establecimientos de Salud, en un contexto en que ocurren más de 4 mil ataques de ransomware por día, según el último comunicado emitido por el FBI al respecto, y en el que más del 90% de las Organizaciones de Salud han reportado -al menos- una brecha de ciberseguridad en los últimos tres años, según el informe de Frost Radar 2020.

En ese sentido, estas 7 recomendaciones van en directa colaboración con asegurar la disponibilidad, integridad y confidencialidad de los datos clínicos registrados, en ocasión a las atenciones en salud.

RAYENSALUD