



# Automatización de procesos de seguridad, **una tendencia imparable en el sector**

Tras un año de pandemia, muchas organizaciones han acelerado su transformación digital para seguir siendo competitivas en el mercado. Aprovechando esta necesidad, los departamentos de Seguridad también han de impulsar la digitalización automatizada de sus procesos; aunque, en ocasiones, esto puede resultar complicado, tal y como se puso de manifiesto en este desayuno de trabajo que organizó la revista *Seguritecnia* con el patrocinio de RKL.

Por David Marchal

**D**igitalizar la automatización de procesos consiste en usar la tecnología para realizar tareas sin necesidad de intervención humana o con el mínimo control indispensable. Esto permite agilizar los procedimientos, crear mejores flujos de trabajo y optimizar la productividad.

Por supuesto, esa automatización puede estar presente en mayor o menor medida en distintas áreas y actividades que llevan a cabo las organizaciones. Pero, ¿hasta qué punto es posible llevar la digitalización automatizada de procesos al ámbito de la seguridad? Esa es, precisamente, la pregunta que dio pie al desayuno de trabajo que organizó la revista *Seguritecnia*, con la colaboración

de la compañía **RKL**. En él participaron distintos expertos del sector: **Alfonso José Ruiz**, jefe de Sección del Servicio de Planes y Seguridad del CNPIC; **Gabriel Sevilla**, director de Seguridad de Cellnex Telecom; **Óscar Benítez**, director de Seguridad en Transports de Barcelona (TMB); **Santiago García**, director de Seguridad del Hospital Gregorio Marañón de Madrid; **José María Rico**, jefe del departamento de Seguridad Corporativa de Red Eléctrica de España (REE); **Aitor Villa**, director de Seguridad de EITB; **Antonio Ponce**, director de Seguridad del Hospital Son Espases de Palma de Mallorca; **Antonio Jesús Martín**, director de Seguridad del Hospital Clínico de Madrid; **José Luis Fernández**, técnico superior de Sistemas y Tecnologías de la Información del Hospital Clínico de Madrid; y **José María Sanz**, CEO de RKL.

Para comenzar, este último quiso matizar lo que, a su juicio, diferencia a la digitalización y la automatización en este ámbito. “Una cosa es automatizar, que es lo que todos estamos haciendo en mayor o menor grado, aunque sea en analógico; y otra es digitalizar. El paso importante es ver cómo se puede digitalizar esa automatización, porque eso ayuda a evitar errores humanos”, explicó.

Al respecto se pronunció Sevilla, de Cellnex Telecom: “Con las operaciones manuales, la detección y la resolución de problemas son más lentas, hay errores en la configuración de los recursos y no hay uniformidad en la aplicación de políticas, lo cual genera que los sistemas queden expuestos a problemas de cumplimiento y ataques”. Por eso, en su opinión, “hay que partir de la premisa de que todo lo susceptible de digitalizar lo será”.



## Alfonso José Ruiz

Jefe de Sección del Servicio de Planes y Seguridad del CNPIC

**“Una buena solución para facilitar procesos relacionados con la seguridad con la Administración es la creación de una ventanilla única”**

En el caso concreto de la seguridad, añadió: “La automatización puede ayudar a optimizar las operaciones cotidianas y a integrar la seguridad con los procesos, las aplicaciones y las infraestructuras desde el comienzo. Automatizar los procesos de seguridad por com-



## Gabriel Sevilla

Director de Seguridad de Cellnex Telecom

**“La automatización ayuda a optimizar las operaciones cotidianas y a integrar la seguridad con procesos, aplicaciones e infraestructuras”**

pleto puede reducir el coste promedio en un 95 por ciento”, sentenció Sevilla.

Se trata, por tanto, según Rico, de REE, de “optimizar los procesos para que sean más sencillos y ágiles”. “Ahora lo que nos toca a todos es gestionar la seguridad con una visión integral”, añadió.



## Óscar Benítez

Director de Seguridad en Transports de Barcelona (TMB)

**“Estamos desarrollando una gran cochera que está digitalizada y automatizada al cien por cien. Con ella, estamos diseñando la seguridad del futuro”**

En este sentido, hay organizaciones que ya están dando pasos en ese camino como es el caso de EITB. “En el ámbito de la digitalización de procesos estamos muy avanzados, por ejemplo, con la presentación digitalizada de planes de seguridad, la implementación de herra-

## » RKL: un servicio de Safety & Security completo y personalizado

RKL nace para cubrir la necesidad que observan en el mercado sus fundadores de analizar riesgos y enfocar los esfuerzos de las empresas. Desde el Safety & Security se deben analizar y enfocar las soluciones globales, de manera convergente e integral, desde el punto de vista físico y lógico. Todo ello, por supuesto, en base a una relación de total confianza y el mayor compromiso de confidencialidad.

Bajo este prisma, RKL aporta un servicio 360° a sus clientes, empezando por el análisis de la mejor estrategia y servicio para cada caso de uso, siguiendo con el resto de actividades hasta que el cliente dispone de un servicio de Safety & Security completo y personalizado. Este servicio integral aporta un valor diferencial a RKL, alejándose de las soluciones de seguridad genéricas, en la que su aportación en las tareas de ingeniería de sistemas permite adaptar su solución a cualquier cliente, un valor añadido único en el sector.

La compañía busca la confianza de sus clientes para transformar digitalmente sus modelos de gestión de la seguridad, creando un nuevo entorno donde el “dato” derivado de las operaciones físicas y lógicas pasa a ser la clave.

Gracias a este enfoque, y una importante inversión en I+D+i, la empresa ha desarrollado Virtual Ecosystem for Safety & Security (VES PaaS), una plataforma como servicio (PaaS) que gestiona y opera riesgos físicos/cibernéticos en infraestructuras críticas; integrando las personas, los bienes y los procesos digitales y físicos.

En esa misma línea, y gracias a acuerdos importantes con empresas como Veoci, SITUM y 3D Vista, también ha implementado soluciones SaaS que permiten la digitalización de los modelos de seguridad. Este es el caso de PAU SaaS, que logra operar los Planes de Autoprotección y Emergencia de las organizaciones.





## Santiago García

Director de Seguridad del Hospital Gregorio Marañón de Madrid

**“El hándicap que tenemos todos los hospitales es que el trabajo ha de ser presencial, y esto a veces complica la digitalización de procesos en el ámbito de la seguridad”**

mientas de simulacros de evacuación, realizados con RKL, o los planes de protección contra incendios”, apuntó Vila.

Sin embargo, hay otras instituciones que no lo tienen tan fácil. Por ejemplo, Ruiz, del CNPIC, reconoció que los procesos de digitalización ayudarían a agilizar su día a día. “Sin embargo, a nosotros nos cuesta por la gran cantidad de normativas, protección de datos, custodia de documentos y burocracia que manejamos habitualmente”.

Y lo mismo sucede en el ámbito hospitalario, cuya digitalización de procesos, por su propia idiosincrasia, puede resultar más complicada. “El hándicap que tenemos todos los hospitales es que el trabajo ha de ser presencial, y esto a veces complica la digitalización de procesos, aunque hemos avanzado bastante en este aspecto desde el comienzo de la pandemia”, explicó García, del Hospital Gregorio Marañón.

Esta opinión la compartieron también Ponce, del Hospital Son Espases; y Marfín, del Hospital Clínico. En el caso del primero, explicó que han invertido mu-



## José María Rico

Jefe del departamento de Seguridad Corporativa de Red Eléctrica de España

**“Tenemos que rodearnos de profesionales que estén cualificados para la gestión de la ciberseguridad, que es una carencia demandada por organismos de todo el mundo”**

cho “en potenciar la automatización de sistemas asistenciales; pero el ámbito de la seguridad se ha dejado un poco de lado. Hemos hecho lo que hemos podido. Por ejemplo, hemos automatizado los partes de incidencia”.

Por su parte, en opinión del segundo, “vivimos un uso masivo de nuevas herramientas tecnológicas que están transformando la sociedad, pero estas todavía no han llegado a la mayor parte de los departamentos de Seguridad del ámbito sanitario, más allá de la digitalización documental y las aplicaciones de mensajería instantánea”, manifestó. “Los departamentos de Seguridad nos encontramos con la difícil tarea de hacer valer necesidades en un entorno donde priman otros objetivos más importantes”, añadió.

Precisamente, su compañero en el hospital confirmó este hecho: “No podemos abordar la seguridad a fondo para controlar y automatizar todo lo que nos gustaría por un tema de recursos”, apuntó Fernández. “Durante la pandemia, hemos tenido que invertir mucho



## Aitor Villa

Director de Seguridad de EITB

**“Es importante automatizar procesos para tener estadísticas e información sobre determinados procedimientos. Ahora bien, esa automatización la tiene que manejar personas que estén bien preparadas”**

tiempo en automatizar procesos para enviar información a Salud Pública. Eso nos impide tratar otros aspectos, como los relacionados con la seguridad, que nos gustaría automatizar en el hospital”.

Sin embargo, no todas las organizaciones participantes en el desayuno de trabajo han tenido esos inconvenientes. “Tengo la suerte de contar con un departamento de Seguridad bastante bien estructurado, en el que ya hemos superado ciertos aspectos en el ámbito de la digitalización”, aseguró Benítez, de TMB, quien puso un ejemplo. “Estamos desarrollando una gran cochera para los autobuses que está digitalizada y automatizada al cien por cien. Con ella, estamos diseñando la seguridad del futuro”, confirmó.

## Necesidades de automatización

A continuación, y relacionado con todo lo expuesto hasta aquí, el debate giró en torno a las principales necesidades que tienen todas estas empresas al abordar la digitalización de sus procesos de seguridad. Por ejemplo, Marfín, del Hospital Clínico, expuso los que, a su juicio,



# Los riesgos ciber físicos de tu empresa son una prioridad.

Te ayudamos a identificar, proteger, detectar, responder y recuperar desde una perspectiva global de las amenazas físicas y lógicas que pueden impactar en tu empresa, profundizando en las Tecnologías de la Operación (OT).



Consultoría



Ingeniería



Automatización de Procesos



VES PaaS



+34 946 40 10 11  
contacta@rklintegral.com  
rklintegral.com

**Safety&Security**  
Cyber Physical  
Threat Management





## Antonio Ponce

Director de Seguridad del Hospital Son Espases de Palma de Mallorca

**“En general, en el ámbito sanitario, se ha invertido mucho en potenciar la automatización de sistemas asistenciales; pero la seguridad se ha dejado un poco de lado”**

hay algunos requerimientos globales. “Necesitamos herramientas analíticas para la gestión y manejo de los datos, de manera que nos permitan conocer y entender la actividad y extraer conclusiones de lo sucedido durante un periodo de tiempo. Por ejemplo, situaciones de emergencia, conatos de incendio, análisis de riesgos, intervenciones realizadas por el equipo de vigilancia el año anterior...”. Y al mismo tiempo, prosiguió, “es necesaria la identificación de tendencias basándose en estadísticas para establecer patrones que permitan pronosticar lo que puede suceder en un futuro y actuar preventivamente”.

Por su parte, Fernández, del Hospital Clínico, hizo hincapié en las necesidades de seguridad aplicada al entorno clínico, que es en lo que más están avanzando en su centro sanitario. “La información que tenemos sobre los pacientes es ingente, y podemos almacenarla o utilizarla. En nuestro caso, la estamos usando de ayuda a la toma de decisiones, mediante sistemas de alarma para la seguridad del paciente o detección temprana

de urgencias. Ahora bien, lo que se necesita para seguir avanzando en este ámbito es inversión, tanto en recursos como monetaria”, apuntó.

Con todo ello se mostró de acuerdo Vila, de EITB, quien, además, sacó a colación un aspecto fundamental para él. “Es importante automatizar procesos para tener estadísticas e información sobre determinados procedimientos. Ahora bien, esa automatización la tienen que manejar personas que realmente estén preparadas y tengan los conocimientos para ello”.

Así también se pronunció Rico, de REE, para quien esa necesaria digitalización y automatización de procesos de seguridad también “abre nuevas brechas de ataque” desde el punto de vista de la ciberseguridad. “Hay que ser conscientes de que tenemos que rodearnos de profesionales que estén cualificados para la gestión de la ciberseguridad, que es una carencia demandada por organismos de todo el mundo. Debemos, por tanto, seguir apostando por la concienciación, la formación continua y la capacitación”.

En este punto, Martín, del Hospital Clínico, también opinó al respecto: “Los sistemas a desarrollar deben tener en cuenta el índice de madurez digital de los profesionales del sector, por lo que, para su implantación, hay que tener presente el desarrollo de aplicaciones para la formación y evaluación online que permitan mejorar la experiencia del usuario y fomentar su incorporación sin necesidad de ser expertos informáticos”.

Ahora bien, esas necesidades de automatización en ocasiones pueden chocar con la realidad, tal y como apuntó Benítez, de TMB: “El tema es cómo integrar los sistemas de seguridad y de tecnología en una misma plataforma; es decir, cómo consigo, por ejemplo, que SCADA hable con la videovigilancia”. A su juicio, el objetivo es cómo relacionar *safety* con



## Antonio Jesús Martín

Director de Seguridad del Hospital Clínico de Madrid

**“Los departamentos de Seguridad nos encontramos con la difícil tarea de hacer valer necesidades en un entorno donde priman otros objetivos más importantes”**

*security* para “reducir los tiempos de respuesta y conseguir enterarnos de que pasa algo”. Siguiendo con el ejemplo, “el sistema SCADA da la alarma, y el de videoconferencia se conecta automáticamente para ver qué ha pasado; y, a partir de ahí, se pone en marcha el plan de emergencia. El problema es cómo digitalizo y automatizo todo esto”.

Es algo, precisamente, en lo que ya están trabajando en el Hospital San Espases, según contó Ponce: “Hay algunos procesos que se pueden automatizar. Por ejemplo, estamos trabajando en digitalizar las videocámaras para hacerlas más inteligentes y que, cuando detecten movimiento, puedan establecer automáticamente unos procesos”, apuntó.

## Procesos automatizables

Y ahí, precisamente, es donde se encuentra la clave de todo, según Sanz, de RKL. “Hay que buscar la manera de automatizar los procesos de forma digital, algo imprescindible si tenemos en cuenta la inmensa cantidad de datos que manejamos todos los días. Si a



## José Luis Fernández

Técnico Superior de Sistemas y Tecnologías de la Información del Hospital Clínico de Madrid

**“No podemos abordar la seguridad a fondo para controlar y automatizar todo lo que nos gustaría por un tema de recursos”**

esto, además, le añadimos los enormes requerimientos legales existentes, puede convertirse en algo ingobernable”, apuntó. Por eso, a continuación, el directivo enumeró tres aspectos por los que, en su opinión, hay que digitalizar la automatización de procesos: “ahorro de tiempo, toma de decisiones para evitar errores humanos y retorno de la inversión cuantitativa y cualitativa”.

El problema es que esto, a veces, puede chocar con la realidad, tal y como apuntó García, del Hospital Gregorio Marañón: “En el caso de los hospitales tenemos el inconveniente de que somos organizaciones muy anárquicas, a las que nos cuesta imponer a los sanitarios cualquier medida de seguridad. Si queremos activar recursos en casos de emergencia mediante automatización no tenemos el detalle exacto para llegar al último efectivo al que nos gustaría llegar”, apuntó. Y a ello tampoco ayuda, según el directivo, la diferenciación tan marcada que tienen en el hospital entre seguridad lógica y física y cómo la digitalización puede afectar a una y a otra área.

Claro que eso no ocurre en el departamento de Seguridad de REE, donde tienen un enfoque más integral, lo que les permite concentrarse en digitalizar ciertos procedimientos en el ámbito de la gestión de la seguridad. “Estamos automatizando muchos procesos como el Plan de Seguridad del Operador, la identificación del personal crítico o la implementación de sistemas que soportan procesos”. Y advirtió: “o todo esto se automatiza para tenerlo actualizado permanentemente o vamos al fracaso”.

Por su parte, Ruiz, del CNPIC, estuvo de acuerdo con estas afirmaciones confirmando que “la digitalización ha llegado para quedarse”, y apuntó la necesidad de poner en marcha “una ventanilla única para facilitar la interlocución con la Administración en procesos de seguridad”.

Y en esa relación entre los operadores y la Administración, según Ruiz, también se debería avanzar en el ámbito de la certificación, que es un proyecto piloto que se está desarrollando, pero que, según confirmó el directivo, “actualmente no es prioritario”.

Sin embargo, cuando se desarrolle va a permitir establecer un sistema sencillo y eficaz de presentación de documentación y distintos planes de seguridad a organismos como el CNPIC. “Y a esto le debería acompañar también un sistema de auditoría e inspecciones de operadores críticos y esenciales para comprobar que las medidas de seguridad se llevan a cabo y también profundizar en el sistema de certificación. Y en todo ello la digitalización sería muy importante”, añadió.

El resto de participantes en el debate también compartieron ese deseo de digitalizar las notificaciones y planes que se han de comunicar a las Administraciones. Y es que, en opinión de Sevilla, de Cellnex Telecom, “los procesos



## José María Sanz

CEO de RKL

**“Tenemos que buscar cómo automatizar los procesos de forma digital, algo imprescindible si tenemos en cuenta la inmensa cantidad de datos que manejamos cada día”**

manuales pueden retrasar la identificación de amenazas en entornos de TI complejos y generar puntos vulnerables en la empresa”. Por eso, continuó, “al automatizar los procesos de seguridad, se podrá identificar, validar y remitir las amenazas con mayor rapidez y sin intervención manual”.

## Conclusión

De esta forma se llegó al final del desayuno de trabajo. Y para terminar, Sanz, de RKL, animó a todas las empresas a digitalizar la automatización y, de esa forma, empoderar al sector de la seguridad. “Hemos de demostrar que somos capaces de hacer cosas innovadoras y que aporten valor”.

Precisamente, recordó la existencia de una nueva ley de modernización de las Administraciones Públicas con 14.000 millones de euros de ayudas para digitalizar estas instituciones en colaboraciones público-privadas. “Ahora solo hay que tener ganas para empezar a avanzar en la digitalización”, concluyó el directivo. **S**