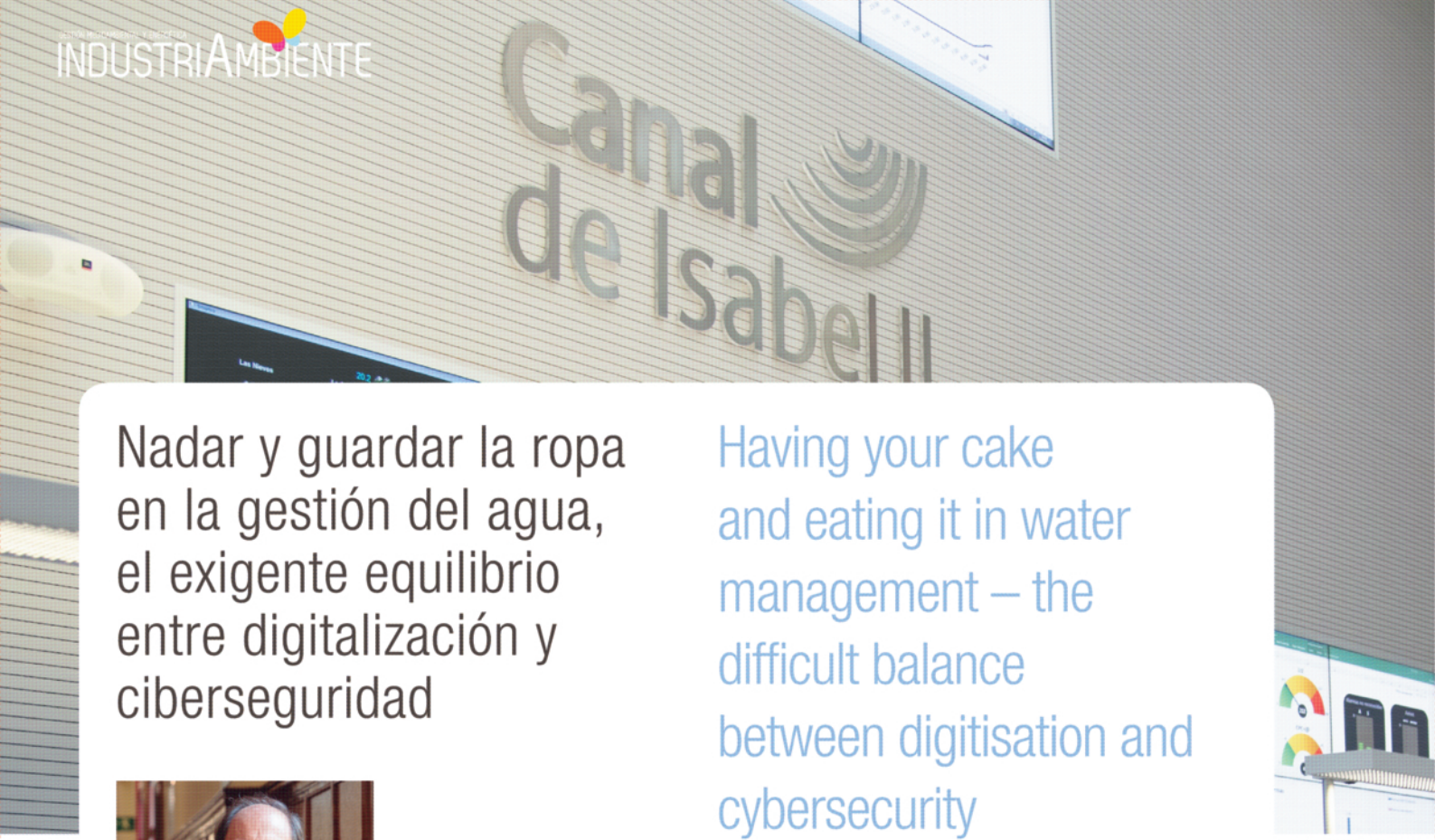


Nadar y guardar la ropa en la gestión del agua, el exigente equilibrio entre digitalización y ciberseguridad

Having your cake and eating it in water management – the difficult balance between digitisation and cybersecurity

Mariano González Sáez – CEO at Canal de Isabel II

En el sector del agua, la seguridad digital es hoy tanto o más importante que la seguridad física de las infraestructuras para garantizar la continuidad, cantidad y calidad de una sustancia que, según la Directiva 2008/114 de la Unión Europea, "es esencial para el mantenimiento de funciones sociales vitales, la salud, la integridad física, la seguridad, y el bienestar de la población".

"Porque tuve hambre, y me disteis de comer; tuve sed, y me disteis de beber". La cita bíblica del Evangelio según Mateo deja en evidencia el valor, ya en el siglo I de nuestra era, de que haya alguien que se responsabilice de proporcionarnos agua.

Pero, entre el buen samaritano que atiende la necesidad de un peregrino, y la empresa pública que responde de la de más de 6,5 millones de personas, hay 1800 años de historia, década más, década menos.

Computación, digitalización, recogida y procesamiento de datos, son procesos normalizados en todas las empresas, también en las que gestionan un bien

In the water sector, digital security is now as or more important than the physical security of infrastructures in terms of ensuring the continuity, quantity and quality of a substance that, according to EU Directive 2008/114, "is essential for the maintenance of vital societal functions, health, physical integrity, safety, security, and well-being of the population".

"For I was hungry and you gave me something to eat, I was thirsty and you gave me something to drink". The quotation from the Gospel according to Matthew shows the value, back in the 1st century AD, of someone who takes responsibility for providing us with water.

But, between the good Samaritan who attends to the needs of a pilgrim, and the public utility that responds to the needs of over 6.5 million people, there is 1800 years of history, give or take a decade or two. Computing, digitisation, and data collection and processing are standard processes in all com-

Charles Clifford - obras de construcción del Canal de Isabel II
Charles Clifford - obras de construcción del Canal de Isabel II/ Canal de Isabel II construction works

finito, globalmente escaso, imprescindible para la vida y fácilmente contaminable como es el agua.

Cuando en 1851 la reina Isabel II promovió la construcción de un canal derivado del río Lozoya, que conduciría el agua hasta Madrid, la cima de la tecnología era la regla de cálculo, pero la calidad y exigencia del conocimiento permitió la construcción de unas infraestructuras hidráulicas sin precedentes, algunas de las cuales todavía siguen en funcionamiento 173 años después.

La industria del agua en la Comunidad de Madrid tiene nombre propio, Canal de Isabel II, y una historia cargada de retos y desafíos a los que siempre se ha dado respuesta, siendo el más reciente el de la gestión del dato, la digitalización y automatización de procesos y, consecuentemente, la necesidad de un estricto protocolo de ciberseguridad y protección de datos.

En Canal, como en el resto de las empresas de agua urbana, nuestras instalaciones han ido incorporando desde modernos sistemas de información y comunicación hasta complejos elementos de automatización que posibilitan, incluso, la operación a distancia de las distintas infraestructuras del ciclo del agua.

Paralelamente, la imparable conectividad de nuestros días no solo ha permitido integrar los sistemas directamente relacionados con la operación (OT), sino también aquellos en los que residen los datos de miles de clientes (IT).

En este sentido, en Canal de Isabel II hemos instalado ya cerca de 400.000 contadores inteligentes conectados con tecnología NB-IoT, que envían 24 lecturas diarias, una cada hora, lo que supone multiplicar por 1.400 la información disponible sobre consumos de agua. Esto último, unido a que el 60 % de nuestros clientes recibe su factura por vía electrónica, hace que

panies, including those that manage water, a finite, globally scarce resource that is easily contaminated. In 1851, when Queen Isabel II promoted the construction of a canal from the river Lozoya to carry water to Madrid, the slide rule was the pinnacle of technology, but quality and the demand for knowledge allowed the construction of unprecedented water infrastructures, some of which are still in operation 173 years later.

The water industry in the Autonomous Community of Madrid is synonymous with Canal de Isabel II and has a history replete with challenges to which it has always responded. The most recent has been data management, digitisation and the automation of processes and, consequently, the meeting the need for a strict cybersecurity and data protection protocol.

As at other urban water companies, modern information and communication systems have been incorporated into the facilities at Canal, along with complex automation elements that even enable remote operation of the different infrastructures associated with the urban water cycle.

At the same time, the unstoppable current trend of connectivity has made it possible to integrate not only the systems directly related to operation (OT), but also those in which the data of thousands of customers reside (IT).

At Canal de Isabel II, we have installed close to 400,000 smart meters connected with NB-IoT technology, which send 24 daily readings, one per hour, thus multiplying the water consumption information available to us by 1,400. This, coupled with the fact that 60% of our customers receive their bills electronically, makes it critical for us to maintain the security and integrity of the information we share with our

para nosotros resulte crítico mantener la seguridad e integridad de la información que compartimos con los usuarios. Y es que no podemos negar que, así como todos estos avances tecnológicos se traducen en palpables ventajas, también entrañan nuevos riesgos asociados a la interconexión de infraestructuras y dispositivos, la introducción del internet de las cosas y el telecontrol de instalaciones clave.

LAS GUERRAS DEL SIGLO XXI

"Creo que el próximo Pearl Harbor o el próximo 11 de septiembre será cibernético" declaró recientemente Angus King durante una audiencia en el Senado de Estados Unidos.

Los países de la Unión Europea también lo creen y, por ello, con fecha 8 de diciembre de 2008, aprobaron la Directiva 2008/114/CE que, en el caso de España, se concretó en la creación del Centro Nacional de Protección de Infraestructuras Críticas, acompañado de la Ley 8/2011 de 28 de abril, y el Real Decreto 704/2011 de 20 de mayo, ambos textos dirigidos a la catalogación y protección de las infraestructuras críticas, entre las que están las del agua.

Se podría decir que la batería normativa llegaba casi una década tarde, porque el primer ciberataque a una infraestructura hídrica se produjo en el año 2000. Un exempleado tomó el control de la compañía de agua en la que había trabajado y provocó un importante vertido de aguas residuales a parques y ríos del condado de Maroochy, en Australia.

En 2018, la Autoridad de Actividad de Agua y Alcantarillado de Onslow en Carolina del Norte tuvo que cerrar su red tras dos ataques consecutivos de ransomware que pusieron en peligro la seguridad de los datos y la infraestructura de servicio.

En 2019, un joven de 22 años pirateó de forma remota la red del Distrito de Agua Rural del Condado de Ellsworth, en Kansas. El hacker intentó alterar los niveles de desinfectante en la planta de tratamiento de agua, pero el ataque pudo detenerse antes de causar daños.

En 2021, ciberataques gemelos lograron acceder al servicio de agua de San Francisco, California y Oldsmar, Florida. Ambos ataques tuvieron como aliado un aparentemente inocente programa de acceso remoto llamado TeamViewer.

Aunque en estos casos más recientes se logró frustrar las intenciones de los hackers, su enumeración nos permite percibir las dimensiones que pueden adquirir las amenazas digitales en un momento en que tanto la industria como los hogares están más conectados que nunca.

Un informe reciente de la compañía Check Point alertaba de que en España se producen, de media, 1.250 ataques cibernéticos por semana.

customers.

While all these technological advances bring tangible benefits, it cannot be denied that they also entail new risks associated with the interconnection of infrastructures and devices, the introduction of the internet of things and the remote control of key installations.

THE WARS OF THE 21ST CENTURY

"I believe that the next Pearl Harbor, the next 9/11 will be cyber", Angus King recently stated during a US Senate hearing.

European Union countries also believe this and, therefore, December 8, 2008, saw the passing of Directive 2008/114/EC. This led to the creation of the National Critical Infrastructure Protection Centre in Spain, accompanied by Act 8/2011 of April 28 and Royal Decree 704/2011 of May 20, both of which seek to catalogue and protect critical infrastructures, including water infrastructures.

This battery of legislation was arguably almost a decade too late, because the first cyber-attack on a water infrastructure occurred in the year 2000, when a former employee took control of the water company where he had worked and caused a major sewage spill into parks and rivers in Maroochy County, Australia.

In 2018, the Onslow Water and Sewer Authority in North Carolina had to shut down its network following two consecutive ransomware attacks that compromised data security and service infrastructure.

In 2019, a 22-year-old remotely hacked into the Ellsworth County Rural Water District's network in Kansas. The hacker attempted to alter disinfectant levels at the water treatment plant, but the attack was stopped before any damage was done.

In 2021, twin cyber-attacks gained access to water services in San Francisco, California and Oldsmar, Florida. Both attacks were allied with a seemingly innocent remote access programme called TeamViewer.

While in these more recent cases, the hackers' intentions were thwarted, citing them as examples them gives us a sense of the potential dimension of digital threats at a time when both industry and households are more connected than ever before.

A recent Check Point report warned that there are, on average, 1,250 cyber-attacks per week in Spain.
An opening paradigm, which could almost serve as a mantra, is that digitisation and cybersecurity must go hand in hand. We should not go too far down one road without going down the other at the same time. If we progress along the path of digitisation whilst neglecting cybersecurity, we increase the risk of cyber-attacks with no guarantee of being able to stop them.The opposite could also happen: if we focus all our efforts on cybersecurity, we may slow down progress in digitisation and fall into the trap of

Un primer paradigma, que prácticamente podría servir como mantra, es que digitalización y ciberseguridad deben caminar de la mano. No deberíamos avanzar mucho en una dirección sin hacerlo al mismo tiempo en la otra. Si progresamos en el camino de la digitalización descuidando la ciberseguridad, incrementamos el riesgo de ciberataques sin garantías de poder frenarlos.

También puede ocurrir lo contrario, si centramos todos los esfuerzos en ciberseguridad, frenamos el progreso en digitalización, cayendo en la obsolescencia. Las empresas hemos explorado y analizado con detalle las posibles amenazas cibernéticas, como pueden ser los ataques masivos, las intrusiones en los sistemas de control industrial o las vulnerabilidades de los sistemas de supervisión, por poner algunos ejemplos. Pese a ello, debemos recordar que no existe el riesgo cero; por muy robustos que sean nuestros escudos de protección, siempre debemos permanecer vigilantes.

UNA RESPONSABILIDAD ACEPTADA

Como máximos responsables del ciclo urbano del agua en la Comunidad de Madrid, debemos cumplir con tres premisas fundamentales que marcan la prestación de nuestro servicio: calidad, cantidad y continuidad.

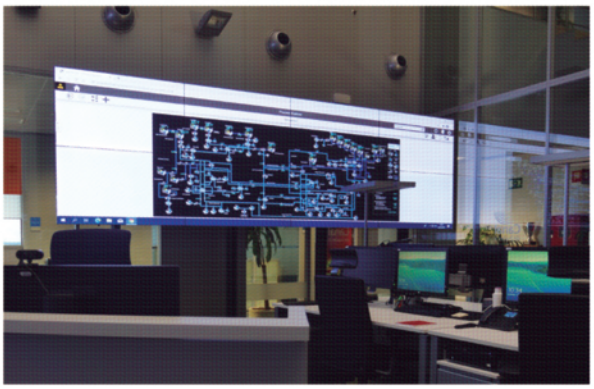
Para conseguirlo es tan importante la seguridad física de las infraestructuras como la seguridad digital, ya que, en la actualidad, ambas son esenciales para asegurar el servicio.

En esta línea, resulta esencial implementar medidas sólidas de ciberseguridad como la segmentación de redes, la autenticación de múltiples factores, la detección de intrusiones en tiempo real, la monitorización de variaciones en el transcurso de las operaciones y la formación continua del personal, sin descuidar las auditorías permanentes a sistemas y aplicaciones.

El volumen de datos que hoy somos capaces de procesar nos permite dibujar con precisión el consumo de agua que realizamos y desgranarlo, lo que ayuda a una mejor gestión y protección del recurso. Bajo este enfoque, quizá se haya perdido una buena oportunidad para destinar fondos europeos y del PERTE, no solo a la digitalización del sector sino también a su hermana siamesa: la ciberseguridad.

Los datos masivos que recolectamos no generan por si solos conocimiento, ni nos permiten avanzar hacia la igualdad y el bienestar, pero es nuestra responsabilidad poner todo de nuestra parte para salvaguardar nuestros activos de información, proteger la privacidad de nuestros clientes y garantizar la continuidad de los servicios que prestamos que nos exigen disponer de casi 500 millones de metros cúbicos cada año para atender las necesidades individuales, industriales, agrícolas y municipales de más de 6,5 millones de madrileños.

obsolescence. Companies have explored and analysed potential cyber threats in detail, including massive cyber-attacks, intrusions in industrial control systems and vulnerabilities in monitoring systems, to give just a few examples. However, we must remember that there is no such thing as zero risk; no matter how robust our protective shields are, we must always remain vigilant.



A RESPONSIBILITY ASSUMED

Being at the helm of the urban water cycle in the Autonomous Community of Madrid, our duty is to comply with three fundamental premises that underpin the provision of our service: quality, quantity and continuity.

To achieve this, the digital security of infrastructures is just as important as the physical security. Both are now vital to guarantee the service. It is essential to implement robust cybersecurity measures such as network segmentation, multi-factor authentication, real-time intrusion detection, monitoring of variations in the course of operations and continuous staff training, without neglecting ongoing audits of systems and applications.

The volume of data we can now process allows us to accurately map our water consumption and break it down, enabling enhanced management and protection of the resource. Given this fact, perhaps a good opportunity has been missed to allocate European and PERTE funds, not only to the digitisation of the sector but also to its Siamese twin: cybersecurity.

The massive data we collect does not in itself generate knowledge, nor does it allow us to advance towards equality and well-being, but it is our responsibility to do our part to safeguard our information assets, protect the privacy of our customers and guarantee the continuity of the services we provide, which require us to make almost 500 million cubic metres of water available each year to meet the individual, industrial, agricultural and municipal needs of over 6.5 million residents of Madrid.