

La Consejería de Digitalización invertirá más de 3,5 millones en los próximos cuatro años para implantar tecnología de vanguardia

La Comunidad de Madrid refuerza los sistemas informáticos sanitarios para protegerlos de ataques a la identidad de los usuarios

- Esta actuación permitirá mejorar los métodos de autenticación de 113.000 empleados del SERMAS monitorizando sus comportamientos en las aplicaciones
- El objetivo es poder anticiparse y neutralizar en tiempo real posibles amenazas procedentes de robos de contraseñas o ciberataques

11 de marzo de 2024.- La Comunidad de Madrid ha incorporado tecnología de vanguardia en materia de ciberseguridad destinada a blindar los sistemas informáticos de la sanidad pública y protegerlos de ataques, especialmente los que tratan de burlar los protocolos de autenticación para acceder a la identidad de los usuarios. El Gobierno regional invertirá más de 3,5 millones de euros en los próximos cuatro años para el desarrollo de un programa puntero cuyo principal objetivo es la tutela de los datos que maneja el Servicio Madrileño de Salud (SERMAS), reforzando los mecanismos de identificación de los empleados públicos.

El consejero de Digitalización, Miguel López-Valverde, ha explicado que esta actuación salvaguardará, por ejemplo, los métodos de bloqueo y acceso a recursos corporativos, así como de cambio de contraseña de 113.000 trabajadores que entran continuamente en las aplicaciones sanitarias. “A través de esta iniciativa, la Comunidad de Madrid implantará una red defensiva robusta que permitirá almacenar y acceder a los datos administrativos minimizando el riesgo de *hackeo*”, ha subrayado.

La información sanitaria se encuentra alojada en sistemas informáticos a los que médicos, enfermeros o administrativos se conectan diariamente para realizar consultas, introducir resultados o dar citas, entre otros trámites. Para evitar situaciones como robos de credenciales, la Administración autonómica ha invertido en la tecnología más puntera del mercado en *Identity Threat Protection* (protección contra amenazas de identidad), ideada para anticiparse y neutralizar en tiempo real posibles amenazas.

Esta solución se fundamenta en la monitorización constante del comportamiento de los usuarios del directorio informático de Sanidad, de sus accesos a las aplicaciones y de las incidencias que puedan ocurrir para así poder detectar, proteger y bloquear en tiempo real cualquier intento de agresión basado en vulnerabilidad de protocolos de autenticación.

PROTEGER LA RED ASISTENCIAL

A esta actuación en materia de ciberseguridad sanitaria se suma la aprobación en el último Consejo de Gobierno del año pasado de una inversión de 9,8 millones de euros para reforzar la Oficina de Seguridad de Sistemas de la Información (OSI), organismo responsable de prevenir, localizar y responder a las amenazas electrónicas que sufra el SERMAS.

La Oficina tiene ante sí el reto de dar soporte a una amplia red asistencial, que se caracteriza por una alta diversificación y heterogeneidad. Además, la creciente interacción de los productos sanitarios, la utilización de conexiones remotas para su mantenimiento, la necesidad de vigilar continuamente a los enfermos (incluso a los que no están ingresados en el hospital), o el uso de teléfonos inteligentes para que pacientes y médicos accedan a la información sobre la salud, son factores que hacen imprescindible disponer de mecanismos de protección adecuados en continua evolución.