La formación en el ámbito digital, clave para evitar ciberataques en los centros sanitarios

- **"Cualquier profesional, además de su formación relacionada con la enfermería, también debería tener unos mínimos conocimientos para utilizar ordenadores y cualquier otro tipo de tecnología de carácter digital", destaca Marco Lozano (INCIBE).**

- **"Una de las principales amenazas a las que se enfrenta el sector sanitario es la paralización de las redes informáticas de un centro sanitario y la consiguiente extorsión; lo que buscan es monetizar el ataque informático". "No son riesgos potenciales, sino hechos reales, que ya se han producido". Así de contundente se ha mostrado Juan Antonio Rodríguez Álvarez de Sotomayor, teniente coronel de la Guardia Civil y jefe del departamento contra el Cibercrimen de la UCO.**

- **"El derecho al olvido es una respuesta a un problema que genera el almacenamiento de información personal en la red, que no tiene límites temporales. Todo aquello que se publica en Internet es algo que queda en Internet de forma permanente. Lo que se produce es un conflicto entre la protección de datos y la intimidad, que es un derecho de la persona, y el derecho a la libertad de información", subraya el magistrado Fernando Ruiz Piñeiro.**

Madrid, 2 de junio de 2022.- Sólo en 2020, las Fuerzas y Cuerpos de Seguridad del Estado registraron 287.963 ciberdelitos, según el último informe sobre Cibercriminalidad de la Secretaría de Estado de Seguridad, cifras que se incrementan año a año. Así se ha puesto de manifiesto en el webinar "Amenazas en la Red: los riesgos para el profesional sanitario" que han organizado el Consejo General de Enfermería y su Instituto Superior

de Formación Sanitaria (ISFOS). "La tecnología, a día de hoy, está muy presente en nuestras vidas, a todos los niveles, en nuestra vida personal y también en la laboral. Es muy habitual el uso de teléfonos, ordenadores, redes sociales y de distintas aplicaciones y programas que empleamos en hospitales y consultas, por lo que hay que saber utilizarlos de forma segura", ha destacado Florentino Pérez Raya, presidente del Consejo General de Enfermería.

Como ha explicado Pilar Fernández, vicepresidenta del Consejo General de Enfermería y directora de ISFOS, "el evitar ser víctimas de uno de estos delitos, mucho más frecuentes de lo que podemos pensar, está en nuestras manos, primero conociendo de qué hablamos y después sabiendo cómo debemos protegernos para evitar que nos roben nuestros datos e incluso nuestra identidad".

Saber cuáles son las amenazas que deben afrontar los enfermeros por su puesto de trabajo y cómo combatirlas es el objetivo que se han marcado en este webinar y para ello han contado con los mayores expertos en ciberseguridad de nuestro país, incluyendo representantes del Instituto Nacional de Ciberseguridad (INCIBE), la Guardia Civil y la Audiencia Nacional.

Principales riesgos

Como ha explicado Marco Lozano, responsable de Ciberseguridad para Empresas del INCIBE, "compartir las contraseñas entre compañeros puede dar acceso a servicios o datos para los que esa persona no tiene permisos. Además, muchas organizaciones de ámbito sanitario tienen sistemas obsoletos, desactualizados, equipos que están ya sin soporte por parte del fabricante, una situación que provoca vulnerabilidad de esas organizaciones que pueden ser susceptibles de acceder a las extorsiones, pagos y demás peticiones relacionadas con cualquier tipo de ataque que llevan a cabo los ciberdelincuentes".

Existen múltiples posibilidades de que un enfermero pueda poner en riesgo la organización si no lleva a cabo las conductas adecuadas de utilización de servicios. Para evitarlos "cualquier profesional, además de su formación relacionada con la enfermería, también debería tener una mínima formación para utilizar ordenadores y cualquier otro tipo de tecnología de carácter digital, para que adquieran los conocimientos mínimos que le permitan ser capaz de identificar algún tipo de amenaza que llega a través del correo electrónico, por ejemplo, pues suele ser el canal más habitual que utilizan los atacantes. Se debe evitar visitar páginas de internet de dudosa reputación o que no sepamos que son seguras y no acceder a servicios para los que no se está autorizado, no instalar aplicaciones para las que no tiene autorización, así como limitar la mayor

cantidad de exposición de información, tanto privada como profesional", ha destacado el experto del INCIBE.

Así, a este respecto, ha recordado que el INCIBE tiene a disposición de todos los profesionales una línea de ayuda a la seguridad a través del número de marcación corta, el 017, donde cualquier autónomo o empleado puede ponerse en contacto con el Departamento Especializado de Protección a Empresas, donde técnicos altamente cualificados, le darán respuesta a cualquier duda o problema relacionado con la ciberseguridad. Se trata de una línea completamente gratuita y confidencial que está disponible los 365 días del año.

Ciberdelincuencia

"La ciberseguridad es un ámbito que afecta a todo el mundo, incluido al ámbito sanitario. Los datos nos demuestran que el crecimiento es imparable y que afecta en todos los sectores". Así de contundente se ha mostrado Juan Antonio Rodríguez Álvarez de Sotomayor, teniente coronel de la Guardia Civil y jefe del departamento contra el Cibercrimen de la Unidad Central Operativa de Policía Judicial (UCO).

Así, ha explicado que "una de las principales amenazas a las que se enfrenta el sector sanitario es la paralización de las redes informáticas de un centro sanitario y la consiguiente extorsión; lo que buscan es monetizar el ataque informático". "No son riesgos potenciales, sino hechos reales, que ya se han producido". De tal forma que "cualquier centro sanitario, del tamaño que sea, tiene que estar preparado para que el mundo digital desaparezca y volvamos otra vez al papel y al boli para poder atender a los pacientes", ha comentado el teniente coronel de la UCO.

A su juicio, "la gran mayoría de los ciberataques que conocemos se dan porque se explotan vulnerabilidades que son conocidas con anterioridad y que no se habían parcheado o actualizado". De ahí que una de las principales acciones de prevención sea tener actualizado el software de todos los dispositivos. Para aquellos que no están conectados a Internet "el mejor antivirus o el mejor software de protección es el sentido común y avisar si se observa a cualquier persona ajena al sistema que pueda estar manipulando un dispositivo o conexión en el propio centro sanitario", ha subrayado el jefe del departamento contra el Cibercrimen de la UCO.

Derecho al olvido

Otro de los temas que se ha debatido en el webinar ha sido el derecho al olvido en Internet. Como ha explicado el magistrado de la Audiencia Nacional, Fernando Ruiz Piñeiro "el derecho al olvido es una respuesta a un problema que genera el

almacenamiento de información personal en la red, que no tiene límites temporales. Todo aquello que se publica en Internet es algo que queda en Internet de forma permanente. Lo que se produce es un conflicto entre la protección de datos y la intimidad, que es un derecho de la persona, y el derecho a la libertad de información".

Como ha señalado el presidente de la sección octava de la sala de lo Contencioso-Administrativo de la Audiencia Nacional, "al igual que no podemos borrar la historia, la historia personal tampoco desaparece. Lo que se intenta es que la persona sufra los mejores perjuicios posibles en relación con lo ocurrido en su vida pasada", y eso es algo que se valora caso por caso.

Con respecto a los enfermeros, Ruiz Piñeiro también ha recordado que en su caso también tienen la obligación de respetar el secreto profesional y el derecho a la intimidad de los pacientes. "Deben tener especial cuidado con las cosas que hacen en su trabajo y lo que puedan difundir, especialmente en redes sociales, porque lo que se escribe, lo que se comparte queda escrito y siempre estará ahí. No hay quien lo borre", ha concluido.