Revista Cubana de Tecnología de la Salud

Revista Cubana de Tecnología de la Salud
ISSN: **2218 – 6719** RNPS: **2252**

Abril - Junio 2023; 14(2):e4075
URL: http://www.revtecnologia.sld.cu/index.php/tec/article/view/4075

Editorial

El usuario: una vulnerabilidad inevitable en la seguridad de la información en salud

The user: an unavoidable vulnerability in health information security

María del Carmen Roche Madrigal [1] *

[1] Universidad de Ciencias Médicas de La Habana. Facultad de Tecnología de la Salud. La Habana, Cuba.

***Autor para la correspondencia:**
marycarmen@infomed.sld.cu

Recibido: 16 de abril del 2023
Aceptado: 17 de mayo del 2023

Citar como:
Roche-Madrigal MC. El usuario: una vulnerabilidad inevitable en la seguridad de la información en salud. Revista Cubana de Tecnología de la Salud [Internet]. 2023 [citado:]; 14(2):e4075. Disponible en: http://www.revtecnologia.sld.cu/index.php/tec/article/view/4075

El mundo es un lugar frenético, y la velocidad a la que cambia crece exponencialmente. La información es el rey. Proteger esa información, sea personal o de negocios, se ha convertido en uno de los mayores retos de la vida.

La seguridad de la información, la seguridad informática y la ciberseguridad pueden parecer lo mismo. En la actualidad, prima el modelo de digitalizar y gestionar cualquier tipo de información mediante un sistema informático.

Sin embargo, son tres áreas del conocimiento que, aunque deben trabajar en armonía y de forma conjunta, y fueron concebidas para proteger los activos o bienes informativos. En especial: la información, la infraestructura que la soporta y los usuarios que la utilizan cada una tiene objetivos y actividades diferentes.

La seguridad de la Información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Se refiere a la protección de los activos de información imprescindibles para el éxito de cualquier organización.

Es la encargada de regular y establecer las normas a seguir para la protección de la información. Tiene el propósito de proteger la información registrada, independiente del lugar donde se localice: impresa en papel, en los discos duros de las computadoras o incluso en la memoria de las personas.

Mientras que la seguridad de la información es la línea estratégica; la seguridad informática describe la distinción táctica y operacional de la seguridad y la ciberseguridad. Es el proceso de proteger las redes, los sistemas y los datos del acceso no autorizado, la modificación y la destrucción.

Existe un axioma de seguridad: ningún sistema de información es seguro, es decir, la medida no puede garantizar un ambiente libre de amenazas o riesgos para la información y las organizaciones o los usuarios que la requieren. ¿Por qué? porque hay personas implicadas en la gestión del sistema, y cometen errores o equivocaciones. Por lo tanto, el ser humano, que es parte de cualquier sistema, siempre lo hará vulnerable.

Algunos autores consideran que la implantación de adecuadas medidas de seguridad para la protección de la información, exige contemplar aspectos técnicos y legales. No obstante, en muchas ocasiones, se presta muy poca atención a la importancia del factor humano en la protección de la información. Las personas representan el eslabón más débil dentro de la seguridad de la información. [1]

Es fundamental tener en cuenta el papel del ser humano y la relación con los sistemas y redes informáticas de la organización. Un principio básico que se debe priorizar desde el punto de vista de la seguridad de la información, es que todas las soluciones tecnológicas implantadas por la organización pueden resultar inútiles ante el desconocimiento, falta de información, desinterés o ánimos de causar daño de algún empleado.

El nivel de seguridad de un sistema de información es efectivo si el nivel de seguridad del eslabón más débil también lo es. Se puede tener la mejor tecnología, cortafuegos, sistemas de detección de ataques, dispositivos biométricos. Lo único que se necesita es una llamada a un empleado desprevenido y se accede al sistema sin más. Tienen todo en las manos. [2]

Si se piensa que la tecnología puede resolver los problemas de seguridad, entonces no entiende ni el problema ni la tecnología. La seguridad de la información se debe afrontar a nivel global. Una puerta blindada no sirve para proteger un edificio si se dejan las ventanas abiertas.[3]

Los usuarios no son conscientes del papel que poseen en la pérdida de confidencialidad, integridad y disponibilidad de los datos, pueden ignorar errores y no repararlos. Por eso la formación de los usuarios es la clave para reparar el factor humano. Las personas pueden ser descuidadas y cometer errores, pero con una formación adecuada, se les puede enseñar a evitarlos y a mantener los datos seguros.

La necesidad de proteger la información y el sistema debe convertirse en una cultura de trabajo. Hay que enseñar a los usuarios a identificar y evitar los errores humanos que pueden conducir a incidentes o violaciones de seguridad. Deben identificar las estafas de ingeniería social, los correos electrónicos *spam*, los mensajes *Hoax*. Asimismo proteger las credenciales de acceso y tener cuidado al revelarlas a otros.

La Facultad de Tecnología de la Salud no está exenta de la necesidad de educar a los usuarios de la red. La carrera de Sistemas de Información en Salud (SIS) tiene dentro del currículo base la asignatura Seguridad de la Información en Salud, donde se tratan los temas referentes a la guarda y custodia de los recursos de información y de la ética en la gestión. Estos temas están presentes en todas las asignaturas de la carrera.

Por tanto, en el contexto de la gestión de información en salud, los profesionales de SIS deben implementar medidas efectivas de seguridad de la información, estar actualizados en las últimas tendencias y amenazas. Dado que la seguridad de la información no es solo una cuestión técnica, sino también ética y legal, es imprescindible que exista la conciencia del factor humano en este ámbito.

Palabras clave: *Seguridad de la Información, Seguridad Informática, Ciberseguridad, Usuario de la información.*

Keywords: *Information Security, Information Security, Cybersecurity, Information User*

REFERENCIAS BIBLIOGRÁFICAS

1. Bogantes A. El rol de la seguridad informática en el ámbito académico y los sistemas de información asociados. Sistemas, Cibernética e Informática. 2020;17(1):24-29
2. Alabdan R. Phishing attacks survey: Types, vectors, and technical aproaches. Future internet. 2020; 12(10):e168.
3. Almanza AR. XIX Encuesta Nacional de Seguridad Informática. Evolución del perfil del profesional de seguridad digital. Revista Sistemas [Internet]. 2020 [citado 12 Ene 2023]. Disponible en: https://doi.org/10.29236/sistemas.n151a3