¿Por qué y cómo generar contraseñas seguras?

Cada día se usa más servicios online y se necesita un perfil o una cuenta en un sitio web, aplicación o portal, ante esta realidad es muy complicado gestionar todas las contraseñas y nombres de usuario que se tenga, tanto es así que la tendencia habitual es ***usar siempre la misma contraseña o poner una contraseña fácil de recordar y muy corta para evitar olvidarlas***, pero, si bien nos ayuda a recordarlas, también puede causar problemas al dejar nuestra información expuesta a terceros, sobre todo ante los delincuentes cibernéticos.

Al no utilizar una contraseña segura, aumenta el riesgo que alguien puede descubrir con más facilidad las credenciales (usuario y contraseña) que se han usado, por ejemplo: para ingresar al correo electrónico y acceder a él sin autorización, si esto sucede, tendrá control y podrá ver los correos de amigos, del trabajo o del banco, con el acceso al correo podrá acceder también a las redes sociales con solo solicitar recuperar la contraseña. Y no solo eso, también podría acceder a las cuentas bancarias o cualquier otro sitio al que se acceda usando la cuenta de email comprometida.

Los riesgos son claros si no se usan contraseñas elaboradas y robustas, se corre el peligro de que algún día alguien las descubra y haga mal uso de ellas, por tal razón tener **contraseñas seguras es fundamental** para estar protegidos de ataques y robos de datos personales, y de esta manera mantener nuestra intimidad e información a salvo.

Recomendaciones para crear una contraseña segura:

Una contraseña segura debe ser fácil de recordar para el propietario de la cuenta, pero prácticamente imposible de adivinar para otra persona, a continuación se detalla algunos consejos para crear una contraseña robusta:

- **Tiene que ser única,** cada cuenta debe tener su propia contraseña.
- **Debe ser larga,** el largo mínimo recomendado es de ocho caracteres con una combinación entre: números, letras mayúsculas y minúsculas, mientras más larga sea la contraseña, mejor.
- **Como puede ser difícil de recordar**, conviene usar una frase de contraseña, es decir, una oración breve o una abreviatura (con la primera letra de cada palabra) de la letra de una canción o un poema que sea fácil de recordar.
- **Remplazar** algunas de las letras por caracteres especiales (@, #, $, etc.) o por números para que sea más difícil de adivinar.
- **No utilizar nombres o números asociados**, como fecha de nacimiento, el nombre de los hijos, padres, hermanos o mascotas, que a menudo se puede encontrar en las redes sociales.
- **Evitar usar** caracteres repetitivos y secuenciales, como "1111", "1234" o "abab".
- **Actualice las contraseñas,** es muy recomendable cambiarlas cada cierto tiempo las contraseñas, como, por ejemplo cada 3 meses; o cuando el dispositivo electrónico ha sido infectado por algún virus informático, luego de la limpieza completa del dispositivo se debería cambiar las contraseñas.
- **Es secreta**, no se debe compartir nunca las contraseñas con nadie, porque ya no importará cuán robusta sea, si se comparte ***<<En ese momento dejará de ser segura>>.***

Referencias:

- https://www.lastpass.com/es/features/password-generator#:~:text=Las%20contrase%C3%B1as%20deben%20tener%20como,contrase%C3%B1as%20reutilizadas%20o%20poco%20seguras.
- https://www.acelerapyme.gob.es/recursos/infografia/consejos-para-crear-contrasenas-seguras
- https://www.reparacionordenadoresmadrid.org/como-elegir-una-contrasena-fuerte-y-segura.html
- https://aplimedia.com/guia-contrasenas-seguras/