

Cómo se elabora una buena contraseña

Por Arnoldo Moreno Pérez

"Un password debe ser como un cepillo de dientes. Úsalo cada día; cámbialo regularmente; y NO lo compartas con tus amigos." Cristian F. Borghello.

Uno de los métodos más comunes y certeros para controlar el acceso a información en los sistemas es usar contraseñas. En Seguridad Informática, corresponde al concepto de identificar a un usuario mediante algo que sólo él sabe y, este mismo criterio se aplica cuando asignamos una clave a algún archivo creado en cualquier programa.

Cabe señalar la importancia de fortalecer nuestras contraseñas y asegurarnos de mantenerlas siempre como algo verdaderamente confidencial. Uno de los errores más comunes es elaborar una clave que sea fácil de recordar (con la intención de no olvidarla), pero no es recomendable basarnos en datos personales (teléfono, número de cartilla, fecha de cumpleaños, etc.), palabras de diccionario (en ningún idioma), nombres de nuestras mascotas, aficiones o gustos.

Si una contraseña se adivina fácilmente, pierde su validez para proteger el acceso a información que se quiere mantener de manera confidencial o reservada. La contraseña ideal es la que usted como usuario puede recordar con facilidad, pero que nadie más pueda dar con ella.

Antes de sugerir reglas para elaborar buenas contraseñas, asegurémonos de poner énfasis en el aspecto de preservar la confidencialidad. Para ello: No comparta sus contraseñas, cámbielas con frecuencia, no las repita en diferentes sistemas, no las almacene por comodidad en su computadora, no la envíe por correo electrónico ni por mensajero instantáneo y, en caso de que intuya que alguien más ya las sabe, proceda a cambiarlas de inmediato.

Además, las contraseñas son vulnerables al robo por tres factores: primero, porque los usuarios acostumbran a ser descuidados, de forma que a menudo escogen contraseñas fáciles de adivinar, segundo, por la forma en que los sistemas operativos guardan, codifican y transmiten las contraseñas y, tercero, los ataques que se pueden realizar a un archivo con contraseña a fin de dar con ella valiéndose de varios recursos. Puntualizamos que, para proporcionar servicios de autenticación, un sistema operativo debe almacenar las contraseñas de manera que pueda compararlas con las que introducen los usuarios en la pantalla de inicio de sesión. Además, un sistema operativo debe transmitir a una computadora remota algo parecido a una clave o código descifrable cuando autentifica una petición de conexión de un usuario remoto. La autenticación deja abierta la posibilidad de que un intruso pueda recuperar las contraseñas de los usuarios al acceder al archivo de contraseñas o intervenir los canales de comunicación.

Ahora bien, después de haber señalado todo lo anterior, pasemos a señalar varias reglas y sugerencias que los expertos han recomendado en los últimos años para elaborar una buena contraseña (decidimos aquí caminar sobre hombros de gigantes). A saber:

- 1.- Debe contener al menos 8 caracteres y no más de 64. Se recomienda combinar números y letras en mayúscula y minúscula, de preferencia no repetir los mismos caracteres. La contraseña distingue mayúsculas y minúsculas, por ello deberá de

recordar las letras que escribe en mayúscula. En caso de incluir caracteres que no sean alfa-numéricos hay que averiguar primero cuáles son los que el sistema permite.

2.- Nunca utilice una contraseña que resulte fácil de averiguar como su fecha de nacimiento o el nombre de sus hijos. Su contraseña no debe contener su nombre de correo electrónico, sus apellidos o la respuesta a su pregunta secreta. Tampoco se deben de utilizar derivados de estos, ni datos personales que se puedan llegar a indagar fácilmente.

3.- Nunca escriba su contraseña en papel. Elija una contraseña que pueda recordar (la contraseña debe de ser fácil de recordar para no tener que escribirla y también es deseable que se pueda escribir rápidamente sin necesariamente tener que mirar el teclado, o bien, no tener que depender demasiado de este hecho).

4.- No utilice palabras de diccionario en ningún idioma. En la actualidad existen muchos programas para tratar de develar claves que basan su ataque en técnicas de diccionario y de fuerza bruta.

5.- Nunca envíe su contraseña por correo electrónico o en un mensaje instantáneo (obviamente tampoco mencionarla en una conversación telefónica, ni faltar a la discreción de manera alguna).

6.- No se recomienda poner la misma contraseña en todas partes. Esto es, evite usar exactamente la misma clave en distintos sistemas y archivos.

7.- Procure no mantener sus contraseñas indefinidamente. Trate de cambiarlas con cierta regularidad.

8.- Existen varias maneras de plantear una contraseña que no sea débil. Por ejemplo, utilice las primeras letras de una frase u oración que no sea tan conocida (puede combinarla con números o letras), o bien, se puede elegir palabras sin sentido pero que sean pronunciables, etc.

9.- Si se trata de una contraseña para acceder a un sistema procure que esta solamente admita un número limitado de intentos y se bloquee. En caso de que esto suceda frecuentemente, que también pueda enviar un aviso al administrador.

Todas las recomendaciones anteriores van más bien orientadas a los usuarios promedio. En lo que concierne a los administradores de sistemas, considero que ellos están obligados tanto al sentido común como a la preparación necesaria antes de adquirir la responsabilidad de administrar algo y, a la disposición para aprender cada día cosas nuevas e ir las implementando.

Este artículo queda íntegramente dedicado a Aurora López Carmona, quien me sugirió la idea de hacerlo y también gracias a ella tuve la motivación de estructurarlo como lo hice.

Si tienes alguna duda o comentario, puedes enviarme un correo electrónico a arnoldo@microasist.com.mx.