Día Mundial de la Contraseña, nuestra primera barrera de defensa

Image

El Día Mundial de la Contraseña se celebra cada año el primer jueves del mes de mayo. Aprovechando esta efeméride, queremos **recordarte la gran importancia** que tiene hacer un **uso adecuado** de esta medida de acceso para que la seguridad de nuestra organización no se vea comprometida.

Para desarrollar nuestro trabajo diario en el SAS tenemos que acceder a diferentes servicios (inicio del PC, correo electrónico, etc.) y aplicaciones (Diraya, Siglo, Intranet, etc.) que **requieren de unas credenciales de autenticación** basadas en un nombre de usuario y una clave.

La contraseña es la primera barrera de defensa, ya que impide que alguien no autorizado pueda acceder a un servicio o a una aplicación. Por ello, hoy nos centraremos en explicar la manera de generar **una contraseña fuerte y fácil de recordar**.

¿Cómo conseguirla?

Una forma de medir la seguridad de nuestra contraseña es calcular cuánto tiempo tardaría un ciberdelincuente en adivinarla. Cuanto **mayor sea la longitud de la contraseña**, más segura será. Por lo tanto, se recomienda hacer uso de una frase, y no de una palabra del diccionario, lo que aumentaría la complejidad del descifrado:

- El número mínimo de caracteres obligatorios que debe tener nuestra contraseña es 8, pero **recomendamos que sean 12** para incrementar su robustez.

Vamos a tomar como ejemplo una frase de más de 12 caracteres, como por ejemplo “en un lugar de la mancha”.

Al tratarse de una frase hecha, en menos de 5 minutos y con un ordenador convencional, haciendo uso de una de las múltiples herramientas que hay por el mercado, la contraseña podría ser descifrada. Por tanto, necesitamos añadir más dificultad al descifrado, y para conseguirlo:

- Utiliza tanto letras **mayúsculas**, como **minúsculas**

En el caso de nuestro ejemplo, probamos a poner en mayúsculas las primeras letras de la primera y la última palabra de nuestra frase: “En un lugar de la Mancha”.

A pesar de este cambio, en tan solo un par de días, nuestra contraseña estaría en manos de ciberdelincuentes. Necesitamos aumentar más la seguridad. Vamos a probar añadiendo otro tipo de caracteres:

- **Añade números y símbolos**

Ponemos un número y un símbolo al final: “En un lugar de la Mancha 2019!”

Con esta combinación, el tiempo de descifrado sería de varios años, pero aun así, no hemos conseguido que la contraseña sea lo más robusta posible. Para ello, podemos añadir complejidad inventando palabras:

- **Comprime la contraseña** para que sea más fácil de recordar

Lo podemos hacer utilizando, por ejemplo, la primera letra de cada palabra, de tal forma que quedara: “EuldlM2019!”.

Además de implementar todas estas medidas:

- **Cámbiala con frecuencia**

Al menos cada 6 meses, antes de que caduque. Además, si sospechas que alguien se ha podido apropiar de ella, notifícalo a través de ayudaDIGITAL para restablecerla y recuperar el control cuanto antes.

- **No compartas tu clave**, sin excepción

Mantenla en secreto. Tampoco las escribas ni las guardes en un archivo en tu ordenador. Podrían hacerse con ella y comprometer el funcionamiento de los sistemas de información y de nuestra organización.

Conjugando **todas estas acciones** conseguirás una dupla (usuario-contraseña) **difícilmente descifrable** para un ciberdelincuente y serás el **primer escudo de ciberseguridad** para nuestra organización.