CONTRASEÑAS

Y medidascomplementarias

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

metared

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
www.incibe.es

BUENAS PRÁCTICAS EN SU USO

Seguir una serie de recomendaciones de seguridad en el uso de contraseñas reducirá, en gran medida, el riesgo de que los ciberdelincuentes consigan acceso a los sistemas de la universidad.

1.1 Robustez

La robustez o lo compleja que sea la contraseña es una de las principales medidas de seguridad.

En muchas ocasiones, se eligen contraseñas débiles fáciles de recordar para acceder a los servicios que provee la universidad. Esto supone un riesgo, ya que los ciberdelincuentes pueden adivinarlas **[Ref. - 1]** muy rápido, por ejemplo, una contraseña basada en un nombre de persona o el comúnmente usado 123456 es descubierta en segundos.

Para conseguir una contraseña robusta se han de seguir las siguientes recomendaciones:

- **longitud mínima de 8 caracteres,** ya que cuanto más larga sea esta, más tiempo se tardará en descubrirla;
- utilizar combinaciones de letras **mayúsculas, minúsculas, números y símbolos.**

Una forma de conseguir contraseñas robustas es utilizar reglas nemotécnicas aplicadas a una frase:

- seleccionamos una frase: «en un lugar de la mancha»;
- hacemos uso de mayúsculas: «En un lugar de la Mancha»;
- incluimos el servicio: «En un lugar de la Mancha Correo»;
- añadimos números: «En un lugar de la Mancha Correo de 2019»;
- añadimos caracteres especiales: «En un lugar de la Mancha Correo de 2019!»;
- podemos comprimirla para hacerla más fácil de recordar, utilizando, por ejemplo, la primera letra de cada palabra, de tal forma que quedara: «EuldlMCd2019!».

NOTA: La forma más segura de obtener una contraseña robusta es utilizar un generador de contraseñas que nos permita elegir, longitud, tipo de caracteres, etc. No obstante, cuanto más complejas sean, mayor será la dificultad para recordarlas. Por ello, lo más recomendable es utilizar un gestor de contraseñas y así solo tener que recordar y conservar la clave maestra, la que abre el gestor.

1.2 No compartida

Tal y como indica la RAE, las contraseñas deben ser una seña secreta, es decir, **no se debe compartir con nadie.** Este es un principio básico, pero que muchas veces se omite como cuando necesitamos un documento que se encuentra en nuestro ordenador o en el correo electrónico.

La contraseña debe ser intransferible y nadie bajo ningún concepto debe saber cuál es. Si otra persona conocedora de tu contraseña hiciera algo con tus credenciales de acceso, podrías ser responsable pues aparecerá registrado como si lo hubieras hecho tú.

1.3 No usar la misma

Utilizar la misma clave para acceder al correo electrónico, redes sociales, aplicaciones y servicios ofrecidos por la universidad, etc., no es una práctica segura. **La reutilización de las contraseñas es uno de los errores más comunes** que se cometen.

Si un ciberdelincuente consigue la contraseña en uno de estos servicios, por ejemplo, por medio de un phishing **[Ref. - 2]** o de una fuga de información **[Ref. – 3]**, todos los servicios que utilizan la misma contraseña se verían comprometidos. **Cada servicio debe tener su propia contraseña de acceso**.

En el ejemplo anterior se creó una contraseña segura utilizando como parte de esta el servicio al que está destinada, esa es una forma de diferenciar contraseñas para distintos servicios y que sean fáciles de recordar.

1.4 Doble factor de autenticación

El doble factor de autenticación **[Ref. - 4] es un mecanismo que añade una capa extra de seguridad** a los servicios que requieren de usuario y contraseña para su uso. Esto se consigue por medio una nueva clave que, generalmente, es de un solo uso. Normalmente, este segundo factor de autenticación está vinculado a un teléfono móvil, por medio de una aplicación específica, aunque también existen dispositivos hardware conocidos como tokens.

Son varias las compañías que han desarrollado sistemas de doble autenticación basados en software y que suelen utilizar una aplicación específica para su uso como:

- Google Authenticator **[Ref. - 5]**
- Amazon AWS MFA **[Ref. - 6]**

Siempre que sea posible se ha de habilitar el doble factor de autenticación para todos los servicios que se utilizan en Internet.

1.5 Gestores de contraseñas

En muchas ocasiones, debido a la gran cantidad de servicios y aplicaciones que se utilizan en el estudio o trabajo diario en la universidad, puede resultar complicado acordarse de todas las contraseñas, por esa razón, muchas veces, se recurre a utilizar la misma para multitud de servicios, algo desaconsejable.

Para evitar tener que recordar todas esas contraseñas existen herramientas específicas que simplifican el trabajo, conocidas como gestores de contraseñas. Utilizando este tipo de herramientas, únicamente será necesario, acordarse de una contraseña, la que permite el acceso al gestor. Estos gestores también pueden ser multiplataforma, por lo que desde cualquier lugar y desde cualquier dispositivo puedes tener acceso a todas tus credenciales de acceso.

Los gestores de contraseñas suelen contar con una característica que permite crear contraseñas aleatorias robustas lo que aumenta considerablemente la seguridad de los servicios o aplicaciones para los que se utilice.

Como único requisito a tener en cuenta es utilizar una contraseña maestra lo más robusta posible, ya que si esta no es lo suficientemente segura el resto de servicios o aplicaciones tampoco lo serán.

REFERENCIAS

1. INCIBE – Protege tu empresa – Blog - Día Mundial de las Contraseñas, ¿aún utilizas 123456? - https://www.incibe.es/ protege-tu-empresa/blog/dia-mundial-las-contrasenas-aun- utilizas-123456

2. INCIBE – Protege tu empresa – Blog - Historias reales: el ciberdelincuente le «pescó» por su falta de formación - https:// www.incibe.es/protege-tu-empresa/blog/historias-reales-el- ciberdelincuente-le-pesco-su-falta-formacion

3. INCIBE – Protege tu empresa – Blog - DLP protege tus datos contra fugas de información - https://www.incibe.es/protege- tu-empresa/blog/dlp-protege-tus-datos-fugas-informacion

4. Dos mejor que uno: doble factor para acceder a servicios críticos - https://www.incibe.es/protege-tu-empresa/blog/dos- mejor-uno-doble-factor-acceder-servicios-criticos

5. Google - Instalar Google Authenticator - https://support.google.com/accounts/answer/1066447?hl=es

6. Amazon - Autenticación multifactor - https://aws.amazon.com/es/iam/details/mfa/