DGTIC UNAM
DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

Contraseñas

Cursos en Línea

Contraseñas

Las contraseñas son un elemento de seguridad fundamental que debemos proteger encarecidamente ya que representan la llave de acceso a nuestra información y recursos. Día a día utilizamos diversos servicios que requieren la autenticación por medio del uso de una contraseña. Como seres humanos que somos, es común que sigamos patrones que nos permitan recordar nuestras contraseñas de manera fácil. Sin embargo, son justamente estos patrones los que pudieran llegar a ser explotados por atacantes que, a su vez, utilizan herramientas especializadas para descifrarlos. Por esta razón, se vuelve necesario conocer cómo es que podemos definir contraseñas seguras y cuáles son las mejores prácticas a seguir para su gestión. Por otro lado, revisaremos también los tipos de cuentas de usuario y sus correspondientes privilegios para conocer cuáles son aquellas en las que debemos prestar más atención y establecer medidas de seguridad más estrictas.

Función de una contraseña

Una contraseña es una cadena de caracteres utilizada para verificar la identidad de un usuario durante el proceso de autenticación (confirma que somos quienes decimos ser). Su función principal es proteger el acceso a sistemas, cuentas, datos y recursos sensibles. Al actuar como una barrera de seguridad, las contraseñas aseguran que solo las personas autorizadas puedan acceder a la información o realizar acciones específicas, previniendo accesos no deseados y protegiendo la privacidad y la integridad de los datos. Por lo tanto, la gestión de contraseñas es una tarea muy importante para la seguridad de la información y, en algunos casos, para la seguridad de nuestra integridad personal.

Figura 1. La correcta gestión de contraseñas permite asegurar nuestra información y proteger nuestra integridad.

Seguridad en contraseñas

La seguridad en contraseñas es fundamental para proteger las cuentas y sistemas contra accesos no autorizados. Se debe tener en cuenta que existen personas maliciosas con los conocimientos técnicos necesarios para implementar herramientas que pueden descifrar en segundos contraseñas sencillas en un sistema. Por esta razón, las contraseñas deben cumplir con algunos parámetros de seguridad que dificulten en la medida de lo posible esta actividad.

Figura 2. Usted debe pensar que sus contraseñas se enfrentarán a programas especializados en la detección de palabras y patrones comunes, por lo que es necesario que tome las medidas de precaución necesarias en su definición.

Las contraseñas en los sistemas informáticos se almacenan comúnmente como un hash. Es decir, no se encuentran en texto en claro, justamente, para agregar una capa adicional de protección. Recuerde que un hash es un grupo fijo de caracteres que se obtiene como resultado de una función matemática a la que se le proporcionan datos de entrada (como puede ser un archivo, un conjunto de caracteres, o, en este caso, una contraseña). Recuerde además que, a diferencia de algunos algoritmos de cifrado, las funciones hash no están pensadas para obtener de regreso el valor de entrada. Es decir, resulta imposible, o muy difícil, saber qué contraseña produjo un hash determinado. Por ejemplo, en la tabla siguiente se muestra el hash producido por las contraseñas correspondientes cuando se utiliza el algoritmo hash conocido como SHA-1:

Tabla 1. **TABLA COMPARATIVA ENTRE CONTRASEÑAS Y HASHES PRODUCIDOS.**

Contraseña	HASH
123456	7c4a8d09ca3762af61e59520943dc26494f8941b
qwerty	b1b3773a05c0ed0176787a4f1574ff0075f7521e
admin	d033e22ae348aeb5660fc2140aec35850c4da997

De tal manera que, si alguien obtiene el hash, NO podrá saber cuál es la contraseña que lo produjo. Y usted puede estarse preguntando, entonces ¿por qué necesitamos que las contraseñas

sean seguras? Y esta es justamente la pregunta clave. Pero para responderla debemos observar primero cómo es que los hashes y las contraseñas funcionan.

En este nivel no es necesario que comprenda con detalles el funcionamiento de las funciones hash, simplemente debe saber que son funciones que producen un conjunto de caracteres fijos a partir de una entrada determinada y que suelen utilizarse para comprobar la integridad de archivos o, en este caso, para autenticar a un usuario por medio de contraseñas.

Como se ha mencionado, los hashes funcionan para agregar una capa de seguridad en nuestras contraseñas porque permiten que estas últimas no se almacenen en texto en claro. De tal manera que, cuando un usuario ingresa su contraseña en un sistema, el sistema convierte esa entrada por medio de una función hash, si el hash resultante es igual al que tiene almacenado el sistema en su base de datos, entonces se concede el acceso. Este procedimiento se ejemplifica en la imagen siguiente:

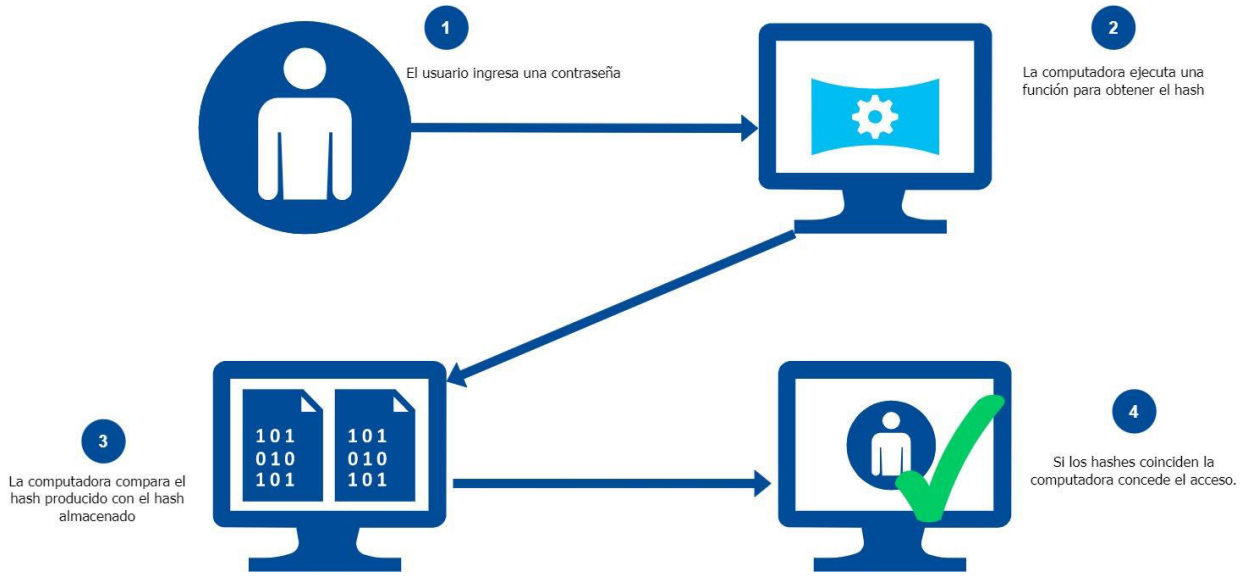

Figura 3. Representación del proceso de autenticación por contraseña en un sistema informático.

Sin embargo, existen personas malintencionadas que utilizan técnicas y programas especializados para vencer la seguridad de los sistemas de información abusando de este proceso. Entre los principales ataques a contraseñas se pueden encontrar:

- Ataque de diccionario. El atacante ingresa, por medio de software especializado, un conjunto de palabras de un diccionario de contraseñas intentando que alguna de ellas sea la indicada y produzca el mismo hash. Por esta razón, se sugiere que las contraseñas no sean palabras ni contraseñas comunes. Con la ayuda de estos programas y diccionarios es relativamente sencillo obtener la contraseña utilizada en un sistema. De hecho, existen diferentes diccionarios de contraseñas que se pueden descargar de internet para usarse con estos programas.
- Ataque de fuerza bruta. En este tipo de ataque, el atacante prueba cualquier posible combinación (por ejemplo: a, aa, aaa, aaa…). Pero esto se realiza por medio de sistemas especializados que agilizan enormemente el proceso. Por esta razón, se sugiere que las

contraseñas sean robustas, pues esto dificulta este proceso. Además, se sugiere que se configuren los sistemas de manera tal que después de un número razonable de intentos se prohíba el acceso.

Existen muchas técnicas más que los atacantes utilizan para poder obtener una contraseña como lo es la ingeniería social y diversos ataques técnicos cuya explicación supera los alcances del curso. Pero usted debe asumir su responsabilidad en la creación de contraseñas seguras y a preservarlas de manera confidencial.

Recomendaciones generales para la gestión de contraseñas

A continuación, se listan algunas de las principales recomendaciones para la gestión de contraseñas:

- Nunca compartir sus contraseñas. Se sugiere que solo usted conozca sus contraseñas, en especial si se trata de aquellas que conceden acceso a sistemas críticos.
- Seguir mejores prácticas y utilizar contraseñas robustas de al menos 12 caracteres que combinen letras mayúsculas con minúsculas, caracteres especiales y números.
- Evite utilizar en una contraseña:
  - Palabras sencillas, así como su nombre, fecha de nacimiento u otros datos fáciles de adivinar.
  - Utilizar contraseñas con base en la disposición del teclado. Por ejemplo: "QWERTY", "asdfgh", "zxcvb", etc., ya que son fáciles de adivinar y están registradas en la base de datos de programas especializados para el descifrado de contraseñas.
  - Palabras cortas o comunes.
- Utilice frases de contraseñas. Las frases de contraseñas son una alternativa efectiva a las contraseñas tradicionales. En lugar de usar una palabra o una combinación corta de caracteres, se utilizan frases completas que son más largas y complejas, lo que las hace más difíciles de descifrar. Una frase de contraseña podría ser una oración o una combinación de palabras al azar, por ejemplo:

"Camarón que se duerme, se lo lleva la corriente". Esta frase se puede utilizar para tomar las primeras letras de cada palabra y combinarla con números, mayúsculas y caracteres especiales. De tal manera que se puede obtener la siguiente contraseña:

CqsdslllC18%!

- No utilizar la misma contraseña para diferentes servicios (por ejemplo: inicio de sesión en equipos, aplicaciones, redes sociales, correo electrónico, etc.) ya que, si uno de estos servicios llega a estar comprometido, es posible que todos los demás también. Por otro lado, tampoco es recomendable utilizar las mismas contraseñas de nuestro ambiente de trabajo a aquellas que utilizamos en nuestros sistemas personales por las mismas razones.

- Cambiar de manera periódica las contraseñas que se utilizan en los diferentes servicios, en especial si estos son críticos para nuestras actividades.
- No utilizar los servicios de recordatorio de contraseñas de los navegadores, sistemas y aplicaciones. Muchos usuarios, por facilidad de uso, seleccionan las opciones que permiten que los sistemas los mantengan autenticados, sin embargo, esto es una mala práctica, pues si el equipo cae en las manos de alguien más se puede comprometer la información de estos servicios.
- De ser necesario utilizar un gestor de contraseñas que utilice una contraseña principal muy robusta.
- No utilizar las contraseñas por defecto pues estas pueden verse comprometidas fácilmente.
- Utilizar servicios de doble factor de autenticación en sistemas críticos. Por ejemplo, en correos electrónicos u otras aplicaciones.

Existen varios servicios que prueban la fortaleza de una contraseña en los que puede conocer qué tan eficiente podría ser. Por ejemplo:

https://password.kaspersky.com/es/

https://nordpass.com/es/secure-password/

Aunque, como medida adicional, introduzca solo contraseñas similares a las que usa o piensa utilizar, NUNCA ingrese su contraseña real en un sitio web ajeno.

Cuentas de usuario

Las cuentas de usuario son perfiles que permiten a los individuos acceder a sistemas y servicios con un conjunto específico de permisos y privilegios. Cada cuenta de usuario suele estar protegida por una contraseña, y la gestión adecuada de estas cuentas es crucial para mantener la seguridad de la información y los sistemas. La asignación correcta de permisos y la monitorización de las cuentas ayudan a minimizar el riesgo de accesos no autorizados y el uso indebido de los recursos.

Tipos de cuentas

En un sistema, las cuentas de usuario se dividen en varios tipos según sus permisos y privilegios. Comprender los diferentes tipos de cuentas y su propósito es esencial para la gestión efectiva y segura de los sistemas informáticos. Básicamente, se pueden dividir en cuentas administrativas y cuentas limitadas.

En algunos documentos se puede llegar a encontrar que los tipos de cuenta se dividen en cuentas administrativas y cuentas de usuario. Lo importante a comprender es que las cuentas administrativas son las que tienen mayores privilegios y las limitadas (o de usuario) se encuentran restringidas a los parámetros determinados por las cuentas de administración.

Cuentas administrativas

Las cuentas administrativas tienen altos niveles de acceso y privilegios dentro de un sistema. Los usuarios con estas cuentas pueden realizar una amplia gama de tareas, como instalar y desinstalar software, modificar configuraciones del sistema, y acceder a todas las áreas y datos del sistema. Debido a su amplio acceso, las cuentas administrativas son objetivos frecuentes de los atacantes, por lo que deben estar protegidas con contraseñas extremadamente seguras y medidas adicionales de seguridad, como la autenticación de doble factor.

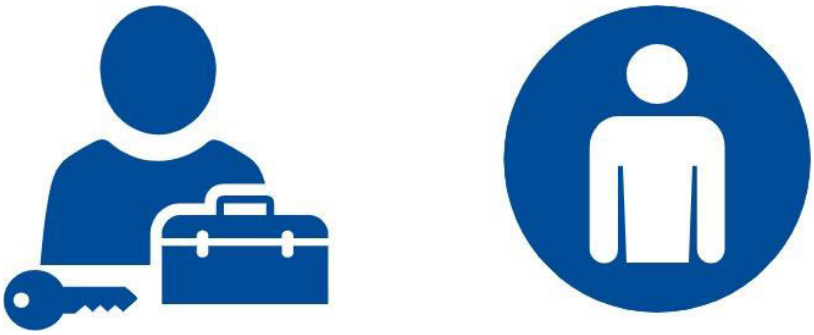

Figura 4. Las cuentas de administración tienen el poder de configuración y acceso a todas las funcionalidades del sistema a diferencia de las cuentas de usuario estándar.

Cuentas limitadas

Las cuentas limitadas, también conocidas como cuentas estándar, tienen permisos restringidos en comparación con las cuentas administrativas. Los usuarios de estas cuentas pueden realizar tareas cotidianas, como ejecutar aplicaciones y trabajar con documentos, pero no pueden realizar cambios significativos en el sistema o instalar software nuevo. Utilizar cuentas limitadas para las actividades diarias reduce el riesgo de que malware o usuarios no autorizados comprometan el sistema, ya que cualquier daño potencial está limitado por los permisos restringidos de estas cuentas.

Figura 5. Las cuentas administrativas tienen mayor jerarquía que las limitadas-usuarios y, por esta razón, son las que se otorgan a los miembros más experimentados en TIC en una organización.

Conocer la diferencia entre cuentas administrativas y cuentas limitadas es crucial en el contexto de la seguridad informática, ya que cada tipo de cuenta tiene diferentes niveles de acceso y permisos. Las cuentas administrativas poseen privilegios elevados, permitiendo al usuario instalar software, modificar configuraciones del sistema y acceder a todos los archivos en el dispositivo incluso a aquellos de otros usuarios. Esto las convierte en un objetivo atractivo para los atacantes, ya que el control total del sistema puede facilitar la implementación de malware y otras actividades maliciosas. Por otro lado, las cuentas limitadas restringen estos permisos, lo que reduce significativamente los riesgos asociados a la instalación de software no autorizado y cambios no intencionados en la configuración del sistema.

Conclusiones:

Para mejorar nuestra postura de seguridad, las contraseñas deben ser complejas, robustas, únicas y, además, necesitan ser cambiadas regularmente. Una contraseña segura suele incluir una combinación de letras mayúsculas y minúsculas, números y caracteres especiales, y debe evitar el uso de información personal fácil de adivinar como nombres o fechas de nacimiento.

Por otro lado, existen diferentes tipos de cuentas en los sistemas de información que otorgan al usuario diferentes tipos de privilegios. Típicamente las cuentas de administración son aquellas que tienen una mayor jerarquía y a las que se les conceden mayores privilegios de configuración. Son en estas cuentas donde se debe tener especial atención y debe asegurarse que se utilicen cuentas robustas para su protección, además de utilizarlas lo mínimo posible para no comprometer el sistema en caso de que se presente un ataque.

AUTOR

ELIER EMANUEL LÓPEZ BASILIO