Píldora Informativa

GPIT

Contraseñas
Y
Medidas Complementarias

No. 008

Universidad Nacional Abierta y a Distancia

Gerencia de Plataformas e Infraestructura Tecnológica - GPIT

Grupo Funcional Seguridad Informática - GFSI


https://gpit.unad.edu.co/seguridad-de-la-informacion


seguridad.informacion@unad.edu.co


601-3443700 Ext 1687


Agosto 30 de 2023

Alcance

En el estudio trabajo diario se requiere el acceso a distintos servicios, dispositivos y aplicaciones para los cuales utilizamos la dupla: usuario y contraseña. Garantizar la seguridad de estos es imperativo para la universidad y la primera medida de seguridad a tomar es utilizar contraseñas seguras

NOMBRE DE USUARIO IDENTIFICACIÓN	CONTRASEÑA AUTENTICACIÓN	INICIO DE SESIÓN

En el control de accesos, el nombre de usuario nos identifica y la contraseña nos autentica, con ella se comprueba que somos quienes decimos ser. Todo sistema de autenticación de usuarios se basa en la utilización de uno, o varios, de los siguientes factores: ► algo que sabes: contraseñas, preguntas personales, etc. ► algo que eres: huellas digitales, iris o retina, voz, etc. ► algo que tienes: tokens criptográficos, tarjeta de coordenadas, etc. El uso de la contraseña es el método más utilizado, esto significa que su gestión es uno de los aspectos más importantes para asegurarlos sistemas de la universidad. Las contraseñas deficientes o mal custodiadas pueden favorecer el acceso y el uso no autorizado de los datos y servicios. Los ciberdelincuentes saben que el uso de la contraseña es el método más extendido para acceder a muchos de los sistemas y servicios utilizados en el día a día, como redes sociales, correo electrónico o aplicaciones para acceder a servicios de la universidad. Con una simple contraseña pueden tener en su poder el futuro de la universidad, por lo que protegerlas debidamente es esencial para salvaguardar la continuidad de esta.

Objetivo

Las contraseñas seguras son útiles para **defenderte de ciberataques y reducir el riesgo de una vulneración de seguridad**. Normalmente, son largas (10 caracteres como mínimo) e incluyen letras mayúsculas, letras minúsculas, números y caracteres especiales. Las contraseñas seguras no deben incluir información personal.

Una contraseña es lo único que **evita el robo de identidad en línea por parte de ciberdelincuentes que hacen uso de su información personal**. Con acceso a sus datos, pueden usurpar sus cuentas y causarle graves daños financieros. Para evitarlo, debe contar con una contraseña sólida.

Buenas prácticas en su uso

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 [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 10 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 laMancha»;
► incluimos el servicio: «En un lugar de la Mancha Correo»;
► añadimos números: «En un lugar de la Mancha Correo de 2023»;
► añadimos caracteres especiales: «En un lugar de la Mancha Correo de 2023!»;

► podemos comprimirla para hacerla más fácil de recordar, utilizando, por ejemplo, la primera letra de cada palabra, de tal forma que quedara: «EuldlMCd2019!».

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 cuáles. 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.

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 hacerse con la contraseña en uno de estos servicios, por ejemplo, por medio de un phishing o de una fuga de información, 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.

Doble factor de autenticación El doble factor de autenticación 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
► Amazon AWS MFA

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

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 los servicios o aplicaciones tampoco lo serán.

JUEGO				
CONTRASEÑA	TECLADO	NUMÉRICAS	USUARIO	BIOMETRÍA
SEGURIDAD	PRIVACIDAD	CARACTERES	AUTENTICACIÓN	VERIFICACIÓN
ACCESO	MAYÚSCULAS	LOGIN	CRIPTOGRAFÍA	TOKEN

MFA SESIÓN AUTORIZACIÓN FIREWALL LLAVE

Z	B	L	A	G	R	L	R	B	E	N	S	S	E	M	R	N	E	G
E	I	I	A	L	L	G	C	A	O	O	E	S	M	A	E	D	A	T
C	O	M	A	Y	Ú	S	C	U	L	A	S	D	S	K	U	D	A	A
O	M	C	S	F	I	R	E	W	A	L	L	A	O	P	A	C	U	A
N	E	L	S	P	R	U	S	N	N	S	E	T	R	S	S	O	D	A
T	T	A	U	T	E	N	T	I	C	A	C	I	Ó	N	E	D	L	S
R	R	A	C	A	R	A	C	T	E	R	E	S	A	A	A	T	A	S
A	Í	O	Y	P	V	E	U	L	O	G	I	N	R	D	S	Í	L	E
S	A	O	O	R	E	P	R	T	O	D	O	A	I	A	F	C	E	I
E	E	U	H	I	R	M	O	R	O	S	S	R	Ó	A	S	P	T	L
Ñ	E	C	C	V	I	N	L	I	E	R	U	O	R	C	R	G	L	A
A	L	L	R	A	F	A	U	C	M	G	I	G	N	L	R	D	I	U
E	L	S	S	C	I	E	C	M	E	F	O	Z	A	A	I	P	L	S
A	A	B	V	I	C	A	I	S	É	T	A	S	A	D	L	C	E	U
T	V	G	Ñ	D	A	N	E	S	P	R	R	I	E	C	U	I	O	A
C	E	N	P	A	C	I	E	I	A	A	I	I	A	S	I	I	M	R
C	O	C	C	D	I	A	R	E	Ó	T	G	C	T	S	I	Ó	S	I
N	I	E	S	N	Ó	C	Q	E	Ó	S	T	F	A	M	C	Ó	N	O
G	E	N	A	I	N	T	T	E	C	L	A	D	O	S	D	A	N	L

Juegue online: https://url.unad.edu.co/1Q3iY

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-elciberdelincuente-le-pesco-su-falta-formacion
3. INCIBE – Protege tu empresa – Blog - DLP protege tus datos contra fugas de información - https://www.incibe.es/protegetu-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/dosmejor-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/