OBJETOS DE APRENDIZAJE | 2019

LÍNEA 2

MATERIALES DE FORMACIÓN PARA ESTUDIANTES DE GRADO DE LA COMPETENCIA DIGITAL

4. Seguridad: 4.1. Protección de dispositivos:

2. Contraseñas seguras

crue Universidades Españolas Red de Bibliotecas REBIUN

Colección Objetos de Aprendizaje, 2019

MATERIALES DE FORMACIÓN PARA ESTUDIANTES DE GRADO DE LA COMPETENCIA DIGITAL

4. Seguridad: 4.1. Protección de dispositivos:

2. Contraseñas seguras

REBIUN Línea 2 (3er. P.E.) Grupo de Competencia Digital

crue Universidades Españolas Red de Bibliotecas REBIUN

Seguridad.
Protección de dispositivos.

CONTRASEÑAS SEGURAS

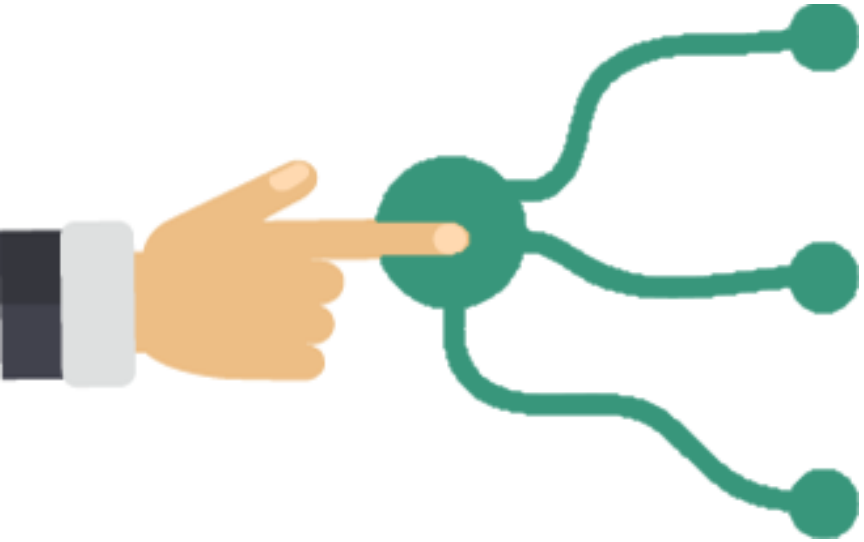
CRUE REBIUN Red de Bibliotecas Universitarias

SUMARIO

- Uso de contraseñas
- Riesgos del uso de contraseñas
- Crear contraseñas seguras
- Gestión de contraseñas
- Doble autenticación

OBJETIVOS

Al finalizar esta actividad tienes que ser capaz de:



- Conocer las ventajas del uso de contraseñas para el acceso a servicios en línea
- Entender los riesgos asociados al uso de contraseñas en el entorno digital
- Aprender a crear contraseñas seguras

USO DE CONTRASEÑAS

Las **contraseñas** son un método de protección que usamos para **limitar el acceso** a la información y los archivos contenidos en nuestros dispositivos y cuentas personales de servicios en línea como: correo electrónico, banca en línea o redes sociales.

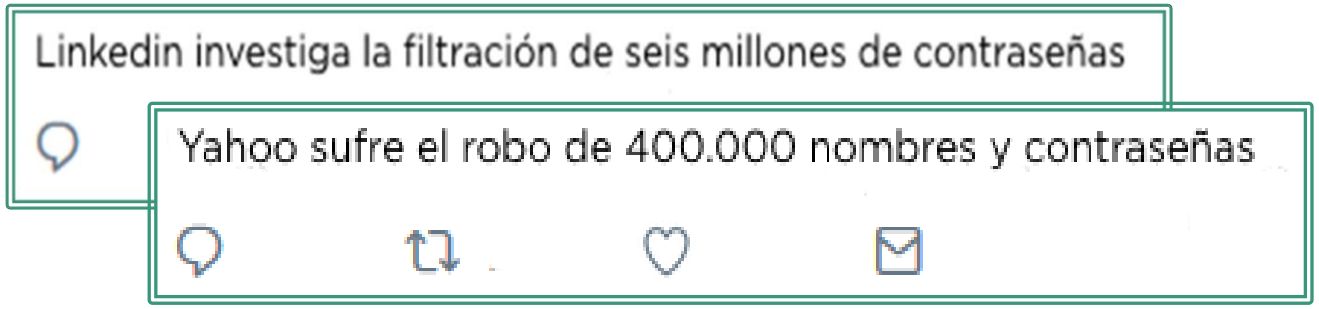
Sirven para:

- Proteger nuestra información personal
- Garantizar la privacidad de contenidos como chats, correos, fotos o archivos
- Evitar accesos no deseados a dispositivos o cuentas personales

El sistema de autentificación de acceso basado en la creación de un usuario y una contraseña es utilizado por la mayoría de servicios en línea, pero también presenta debilidades:

- Dificultad para memorizar múltiples contraseñas complejas
- Vulnerabilidad frente a las técnicas de robo de contraseñas utilizadas por ciberdelincuentes

RIESGOS DEL USO DE CONTRASEÑAS



Los **ciberdelincuentes** usan diferentes tipos de ataques para tratar de robar contraseñas y poder acceder con fines maliciosos a nuestros dispositivos y cuentas personales.

Tipo de ataque	Características
Fuerza bruta	Consiste en adivinar la contraseña a base de ensayo y error. Los ciberdelincuentes prueban distintas combinaciones hasta que dan con el patrón correcto.
Ataque de diccionario	Un software se encarga de intentar obtener la contraseña de forma automática, probando con combinaciones de letras y palabras.
Phising	Es una técnica de engaño que simula o suplanta la interfaz de un servicio en línea, como la banca electrónica, para que introduzcamos nuestras claves y obtenerlas así fácilmente.
Keylogger	Se trata de un software malicioso de tipo spyware que captura todas las pulsaciones del teclado, incluidas las contraseñas.

Adaptado de: Oficina de Seguridad del Internauta. (2019). Ataques a las contraseñas. Recuperado de https://www.osi.es/es/campanas/contrasenas-seguras/ataques-contrasenas

El uso de contraseñas robustas y seguras reduce los riesgos sobre accesos no deseados, manipulación o destrucción de datos, y difusión no autorizada de información o archivos personales.

CREAR CONTRASEÑAS SEGURAS

Cuando creamos una contraseña debemos ser cuidadosos y ponérselo difícil a los ciberdelincuentes:

- Elegir una contraseña con un mínimo de 8 caracteres de longitud.
- Utilizar datos personales como nombre, DNI, fecha de nacimiento, número de teléfono o dirección postal.
- Recurrir a una secuencia de letras del teclado (qwerty, 1234…) o repetir el mismo caracter en la contraseña (11ee44).
- Combinar letras mayúsculas y minúsculas, con números y caracteres especiales (símbolos).

Contraseña	Tiempo que tardaría en ser descubierta en un ataque
123456	Menos de 1 segundo
asdfghjk	Menos de 1 segundo
551882342	Menos de 1 segundo
alcala13	1 minuto
Tokio2020	4 días
Era$e1vez!	6 años

Según cálculos obtenidos de https://howsecureismypassword.net/

CREAR CONTRASEÑAS SEGURAS

Debemos tomar conciencia de la importancia de utilizar contraseñas robustas y seguir medidas de buenas prácticas para mejorar la seguridad en la creación y uso de contraseñas:

- Elegir una contraseña fácil de recordar
- Usar una contraseña que pueda escribirse rápidamente, sin mirar el teclado
- Crear una contraseña única para cada servicio
- Cambiar la contraseña periódicamente
- Evitar apuntar las contraseñas en papel o en un archivo
- Nunca compartir contraseñas o difundirlas por medios electrónicos

En el caso de utilizar un gran número de contraseñas diferentes, es recomendable utilizar un gestor de contraseñas

GESTIÓN DE CONTRASEÑAS

Los **gestores de contraseñas** son herramientas que nos permiten almacenar las claves de acceso a múltiples servicios, sin necesidad de tener que memorizarlas. Además, ofrecen la posibilidad de generar por nosotros contraseñas complejas.

Estas utilidades suelen estar integradas en los propios dispositivos y en los navegadores de Internet, o ser instaladas como aplicación independiente.
Su uso es recomendable para:

- Generar de forma aleatoria contraseñas robustas
- Almacenar múltiples contraseñas, asociadas a diferentes servicios
- Recordarnos la importancia de cambiar las claves de forma frecuente
- Advertirnos ante el uso repetido de una misma contraseña

El uso de un gestor de contraseñas nos protege ante posibles ataques de phising, ya que será capaz de distinguir entre la página de acceso original y una de posible suplantación pese a que su interfaz sea idéntica.

DOBLE AUTENTICACIÓN

El uso de contraseñas como método de acceso a servicios en línea tiene múltiples riesgos asociados, por lo que algunos de ellos, como correo, comercio o banca electrónica, recomiendan a sus usuarios el uso de un **sistema de verificación** de identidad en dos pasos: la **doble autenticación**.

Mediante este sistema, además del usuario y contraseña, deberemos verificar nuestra identidad aportando información adicional como puede ser:

- Introducción de código recibido por sms o llamada telefónica
- Verificación mediante sistemas de reconocimiento biométricos asociados al dispositivo como huella digital o reconocimiento facial
- Código de uso único proporcionado por un dispositivo específico para su creación como una tarjeta numérica o una criptocalculadora

Muchos servicios en línea, especialmente aquellos basados en la nube permiten activar la autenticación en dos pasos.

Como alternativa existen aplicaciones que nos permiten contar con esta segunda capa de seguridad:

Google Authenticator

Latch

PARA SABER MÁS...

[a personalizar por cada institución]

https://www.osi.es/es/campanas/contrasenas-seguras

¡Si tienes dudas pregunta a los bibliotecarios!

CRUE REBIUN
Red de Bibliotecas Universitarias