

integrales. Se evaluó la capacidad de enrollarse durante varios días de almacenamiento, con la idea de encontrar un equilibrio entre el aprovechamiento de la harina de vaina de mezquite y las cualidades que una persona consumidora espera encontrar en este alimento. Hasta el momento se cuenta con diferentes formulaciones caracterizadas por su composición química y sus propiedades tecnológicas, mientras que la evaluación de la aceptación del consumidor es el siguiente paso del proyecto.

El desarrollo de nuevos productos alimenticios no siempre requiere recurrir a importar ingredientes o crear nuevos procesos; muchas veces la innovación también puede encontrarse en recursos que ya han sido parte de la región por años. En Hermosillo, Sonora, el interés en utilizar mezquite en alimentos para integrarlo a la dieta diaria ya se refleja en emprendimientos locales que incorporan la harina de la vaina, la péchita y la chúcata del mezquite en diferentes productos, como neverías y otros igualmente con enfoque en repostería.

En el CIAD se continúa investigando el uso de esta harina en diversos

alimentos como una forma de aprovechar uno de los recursos que ofrece el desierto. Asimismo, se ofrecen talleres comunitarios para compartir el proceso de preparación y obtención de la harina, así como para enseñar la elaboración de los productos alimenticios elaborados. Este trabajo se realiza con el apoyo de Alma Rosa Islas Rubio, Nina Gisella Heredia Sandoval y María del Carmen Granados Nevárez, académicas del Laboratorio de Cereales, así como con la colaboración de Luz del Carmen Montoya Ballesteros y Yésica Yudith Martínez Núñez, del Laboratorio de Procesamiento de Frutas y Hortalizas, ambas adscritas a la Coordinación de Tecnología de Alimentos de Origen Vegetal del CIAD, sede Hermosillo. Asimismo, se trabaja en colaboración con Ana Irene Ledesma Osuna y Jesús Enrique Gerardo Rodríguez, investigadores(as) del Departamento de Investigación y Posgrado en Alimentos de la Universidad de Sonora.

*** Autora: Lorena Sosa Yáñez, investigadora del programa Estancias Posdoctorales por México (Secihti) comisionada al CIAD, sede Hermosillo.**



Cómo crear contraseñas seguras y proteger tu información en la banca digital

Por Redacción

¿Por qué es importante crear contraseñas seguras? Las contraseñas son un elemento vital para proteger nuestra vida digital. Al utilizar contraseñas seguras, se convierte en la primera línea de defensa contra el acceso no autorizado a nuestra información. Los ciberdelincuentes suelen utilizar diversas técnicas para intentar adivinar, descifrar o robar las contraseñas. Por lo que, para mantener una máxima seguridad digital en nuestras cuentas, las contraseñas deberán ser difíciles de adivinar o descifrar.

¿Cuáles son los errores más comunes al crear contraseñas? Uno de los errores más comunes al momento de crear y/o actualizar la contraseña de nuestras cuentas o plataformas digitales es crear contraseñas con combinaciones fáciles de recordar, utilizar la misma en diversas cuentas y sitios, y no actualizarlas por largos periodos de tiempo.

Errores más comunes al crear tu contraseña:

- Usar información personal. Utilizar nombres como los de tus familiares, fechas de nacimiento, el nombre de tu mascota o dirección. Esta información suele ser pública, por lo que resulta más sencillo para el atacante obtener pistas de tu contraseña.
- Combinaciones cortas y simples. Palabras con menos de 8 caracteres es un blanco fácil para los atacantes que utilizan métodos automatizados.
- Reutilizar contraseñas pasadas. Usar la misma contraseña en todas las

cuentas o utilizar contraseñas que ya habían sido utilizadas previamente. Escribirlas en un papel o un documento no seguro: por ejemplo, si escribes tus contraseñas en notas adhesivas sobre tu escritorio, cualquier persona puede robarla.

¿Cómo crear contraseñas seguras? La buena noticia es que es posible crear contraseñas seguras y robustas, las cuales sean difíciles de adivinar por medio de prácticas simples: Genera contraseñas largas para dificultar su descubrimiento: Intenta que contenga un mínimo de 12 caracteres.

Utiliza combinaciones únicas de palabras:

Las cuales tengan una mezcla de mayúsculas, minúsculas, números y símbolos especiales (¡como !, @, #, \$, %). La variedad aumenta la dificultad para que pueda ser adivinada. Evita utilizar sustitutos de caracteres (2), los cuales puedan ser obvios o fáciles de adivinar; por ejemplo, utilizar el número cero en lugar de la letra "O".

Utiliza combinaciones de palabras poco comunes: o palabras que no se asocien a ti.

No repitas contraseñas: debe ser única para cada cuenta. Evita reutilizar.

Crea contraseñas que tengan sentido para ti, pero que sean difíciles de adivinar para los atacantes utilizando sus métodos automatizados.

Activa el doble factor de autenticación (2FA) siempre que sea posible. Es una capa extra de seguridad digital.

Revisa y actualiza tus contraseñas de manera periódica.