MANUAL PARA LA CREACION DE CONTRASEÑAS

DESCRIPCIÓN BREVE

Esta es una guía para los estudiantes y personal del Tecnológico de Reynosa sobre el uso correcto e implementación de contraseñas afines al uso de plataformas digitales y cuentas utilizadas para el entorno educativo

Gregorio Castillo Jr. 19580589

Creación de contraseña

1. Para la creación de contraseña podemos hacer uso de software que nos permitan crear contraseñas como serían los siguientes:
   - LastPass: Es un gestor de contraseñas que también incluye un generador de contraseñas aleatorias.
   - KeePass: Es un gestor de contraseñas de código abierto que incluye un generador de contraseñas seguro.
   - 1Password: Es un gestor de contraseñas con una característica de generador de contraseñas aleatorias.
   - Dashlane: Es un gestor de contraseñas que también ofrece una función de generación de contraseñas.
   - RoboForm: Es un gestor de contraseñas que también incluye un generador de contraseñas seguras.

   Estos son solo algunos de los disponibles.

2. De no querer hacer uso de estos, entonces tendremos en cuenta lo siguiente en este documento para crear una contraseña
3. **NO** utilizar fechas importantes para nosotros como serian los siguiente: fechas de cumpleaños, graduación, boda, pareja, entre otros
4. **NO** utilizar nombres de personas importantes para nosotros como serian los siguientes: Nombre de madre, padre, amigos, pareja o hijos
5. **NO** utilizar nombres de mascotas
6. **NO** utilizar contraseñas previamente usadas o que tengamos en uso
7. **NO** utilizar contraseñas que se hayan visto vulneradas, para ello podemos hacer uso de paginas de internet que comprueben si nuestros datos se han visto vulnerados como:
   - Have I Been Pwned (https://haveibeenpwned.com/): Es una página web que te permite comprobar si tu correo electrónico o contraseña ha sido comprometida en alguna brecha de seguridad conocida.

- Pwned Passwords (https://haveibeenpwned.com/Passwords): Es una herramienta dentro de la página Have I Been Pwned que te permite comprobar si tu contraseña ha sido incluida en alguna lista de contraseñas filtradas en incidentes de seguridad.
- Firefox Monitor (https://monitor.firefox.com/): Es una herramienta de Mozilla Firefox que te permite comprobar si tu correo electrónico ha sido incluido en alguna brecha de seguridad conocida.
- Google Password Checkup (https://passwords.google.com/checkup): Es una herramienta de Google que te permite comprobar si alguna de tus contraseñas ha sido comprometida en alguna brecha de seguridad conocida.

8. **NO** utilizar lugares de nacimiento o residencia actual como lo serian el país, estado o ciudad
9. Podemos hacer uso de palabras aleatorias sin correlación como lo seria de ejemplo “Madera-Tiroides-Dálmata-Programación”
10. Tenemos que evitar que exista correlación entre estas palabras, ya que de haberla seria mucho mas sencillo ser vulnerados, un ejemplo de como **NO** debe ser nuestra contraseña sería el siguiente, “Madera-Castor-Mesa-Chocolate” si bien parece ser que no existe correlación entre ellas, tenemos como factor común el color café presente en los objetos
11. Si bien parece ser un poco difícil recordar este tipo de contraseñas podemos hacer uso de una historia que de tan ridículo que nos parezca, esta no se nos olvidara por eso mismo, haciendo uso de la contraseña de ejemplo, sería lo siguiente “Una vez vi un tronco de **madera** que tenía forma de **tiroides** el cual un perro **dálmata** estaba usando para estudiar **programación**”

Uso y cuidado de la contraseña

1. Para esto podemos hacer uso de sistemas de control de contraseñas, como lo seria Bitwarden, el cual es un sistema de bóveda que nos permite controlar todas y cada una de nuestras contraseñas de forma que incluso al entrar a una página en cuestión, este nos permite dar click en una pestaña para autocompletar tanto el usuario como la contraseña de este, para tener acceso a este, solo necesitaremos hacer uso de una contraseña maestra que nos dará acceso al resto, también tendríamos otros como:
    - LastPass: Es un gestor de contraseñas basado en la nube que te permite almacenar tus contraseñas y otra información sensible de forma segura.
    - 1Password: Es un gestor de contraseñas disponible para dispositivos móviles y de escritorio que utiliza cifrado de extremo a extremo para proteger tus datos.
    - Dashlane: Es un gestor de contraseñas que también incluye un generador de contraseñas seguras y un autofill para facilitar el inicio de sesión en sitios web.
    - KeePass: Es un gestor de contraseñas de código abierto que te permite almacenar tus contraseñas localmente en tu dispositivo.
    - RoboForm: Es un gestor de contraseñas que también incluye un generador de contraseñas seguras y un autofill para facilitar el inicio de sesión en sitios web.

2. **JAMAS** debemos dar nuestra contraseña a nadie mas
3. Tampoco haremos uso de sistemas físicos, como guardarlas en un papel o debajo del escritorio
4. Para mantener seguras nuestras cuentas, podemos realizar cambios de contraseñas cada cierto periodo de tiempo, lo recomendable en su mayoría es en un periodo de 3 a 6 meses entre contraseñas

5. En el caso de los sistemas de evaluación estudiantil, las contraseñas serán generadas por el encargado del área de sistemas, pero será responsabilidad del docente cuidar de esta
6. En caso de notar actividad sospechosa, notificar al encargado para realizar una actualización de contraseña o en casos críticos como el área de finanzas y sistemas, eliminar completamente el usuario y asignar uno nuevo
7. Los datos de las cuentas deben de estar respaldados en medios virtuales en servidores de la universidad
8. No guardar las contraseñas en medios virtuales como block de notas, sticky notes, chats privados, etc.
9. Tener monitoreada la red de conexiones, esto lo podemos hacer con los siguientes programas:
    - Wireshark: Es una herramienta de análisis de protocolos de red que te permite capturar y analizar el tráfico de red en detalle.
    - Nagios: Es una plataforma de monitoreo de red de código abierto que te permite supervisar la disponibilidad y el rendimiento de los dispositivos y servicios de red.
    - SolarWinds Network Performance Monitor: Es una solución de monitoreo de red que te permite supervisar y analizar el tráfico de red en tiempo real.
    - PRTG Network Monitor: Es una solución de monitoreo de red que te permite supervisar el rendimiento y la disponibilidad de dispositivos y servicios de red.
    - Zabbix: Es una plataforma de monitoreo de red de código abierto que te permite supervisar el rendimiento y la disponibilidad de los dispositivos y servicios de red.