Passwords

Better living through better passwords

1. Usar un gestor de contraseñas
2. Usar contraseñas robustas
3. Usar contraseñas únicas
4. Mantener tus contraseñas secretas
5. Diferenciar tus contraseñas de organizaciones y personales

6. Referencias

@title = “Contraseñas” @toc = true @summary = “Vivir mejor usando contraseñas robustas”

Usar un gestor de contraseñas

Usar un gestor de contraseñas representa uno de los cambios importantes que hacer para aumentar tu seguridad personal.

Un gestor de contraseñas permite el uso de contraseñas que son a la vez fuertes y únicas. Usando un gestor de contraseñas no hay que recordar sino una sola contraseña. Es el gestor el que contiene todas las demás contraseñas.

Existen tres tipos de gestores de contraseñas.

- **Aplicación local:** Es un programa local que almacena todas las contraseñas en tu computador local, cifradas con la contraseña maestra. Es la opción más segura de las tres, pero puede ser difícil de sincronizar tus contraseñas entre los diferentes dispositivos.
- **Servicio en la nube (cloud service):** Es un servicio, por lo general pagado, que almacena tus contraseñas, sin importar el dispositivo. Este servicio te da acceso a tus contraseñas desde cualquier lugar. El costo que pagar para esta ventaja es un nivel de seguridad menor al de una aplicación local.
- **Extensión de navegador web:** Muchas veces, aplicaciones locales y servicios en la nube ofrecen extensiones para los navegadores web permitiendo el acceso a las contraseñas directamente desde el navegador. Es práctico, pero a costa de una seguridad ligeramente más baja.

Sin importar la opción escogida, la clave es usar un gestor de contraseñas. Estos son 2 consejos que tener en mente:

- **Contraseña maestra:** Cuando se usa un gestor de contraseñas, es esencial, primordial, no perder la contraseña maestra. Sin la contraseña maestra, todas las demás contraseñas están fuera de alcance. Si crees que podrías llegar a olvidar esta contraseña maestra, escríbelo en algún sitio y guarda el papelito en un lugar seguro.
- **Copia de seguridad (bakups):** Es muy importante hacer copias de seguridad de tu base de datos de las contraseñas. En el caso de los servicios en la nube, las copias de seguridad se hacen automáticamente (aunque sigue siendo buena idea hacer una copia local). En el caso de las aplicaciones locales, sólo hay que hacer una copia del archivo de base de datos.

Gestores de contraseñas populares:

- KeePass y KeePassX (aplicaciones) son 2 versiones de un mismo gestor de contraseñas. Los 2 tienen muy buenas referencias. Estas 2 herramientas usan el mismo formato de archivo. Funcionan en casi cualquier computador.
- Surveillance Self-defense / Cómo Usar KeePassXC (https://ssd.eff.org/es/module/c%C3%B3mo-usar-keepassxc)
- KeePassX para Windows / Administrador seguro de contraseñas (https://securityinabox.org/es/guide/keepassx/windows/)
- LastPass (servicio en la nube)

- 1Password (servicio en la nube y aplicación)

Usar contraseñas robustas

Las contraseñas fuertes son *generadas de forma aleatoria*. Aparte de las contraseñas para el dispositivo y para el gestor de contraseñas, todas tus contraseñas deberían ser generadas por el gestor de contraseñas y deberían tener una longitud mínima de 12 caracteres. Las contraseñas no necesitan tener más de 26 caracteres.

Lxs seres humanxs no creamos contraseñas robustas, pero los computadores sí pueden crear unas excelentes. Dejes que tu computador crea tus contraseñas.

Para las contraseñas que tienes que recordar, hay varios métodos para generar unas buenas. Primero, existe la guía Creando Contraseñas Seguras (https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras).

Diceware (https://web.archive.org/web/20041012030451/www.gjldp.org/CHARENTAISES/article.php?id_article=4) (Versión original en inglés (https://world.std.com/~reinhold/diceware.html)) es una forma eficaz y lúdica para crear contraseñas fáciles de recordar, pero aleatorias. Usa unos dados y una lista de palabras.

Otra forma de crear contraseñas fuertes es inventando una frase algo loca que nadie nunca haya dicho antes y usar la o las primeras letras de cada palabra para construir su contraseña y mezclándole puntuación y números.

Es importante usar contraseñas robustas para todas tus cuentas porque el acceso a una sola cuenta muchas veces sirve para luego acceder a otros sistemas. Es especialmente cierto para las cuentas de correo electrónico que sirven para la recuperación de contraseñas olvidadas.

Usar contraseñas únicas

El uso de contraseñas únicas es una buena forma de minimizar el riesgo ligado al uso de servicios tecnológicos de terceros. Si un servicio tecnológico está afectado y que tu contraseña para acceder a este servicio es única, lxs malhechores no podrán acceder a otras cuentas o servicios tuyos. El uso de contraseñas únicas quiere decir que no confías en los servicios que usas para tu seguridad. Es fácil si usas un gestor de contraseñas.

Mantener tus contraseñas secretas

Incluso si alguien pretende trabajar por el departamento de TIC o un soporte técnico, nunca le entregues tu contraseña. Casi todos los sistemas permiten la reinicialización de las cuentas a fines administrativas. Todo empleado legítimo puede usar este método en lugar de pedirte tu contraseña. Este método deja huella que se puede seguir y que avisa de la reinicialización. Hay que cambiar de contraseña después de tal intervención, pero así te aseguras que eres la única persona teniendo acceso a tus informaciones digitales.

Diferenciar tus contraseñas de organizaciones y personales

Una contraseña de organización otorga un acceso administrativo a sistemas de la organización o un acceso a la

identidad en línea de la organización. Son accesos muy importantes. Estas contraseñas deberían estar guardadas en un lugar muy distinto al de las contraseñas para acceder a tus cuentas personales. Una forma de realizarlo es crear una conexión o un archivo diferente en el gestor de contraseñas. Otra forma puede ser usar un gestor distinto para las contraseñas de organizaciones.

Referencias

- Security Planner / Password Managers (https://securityplanner.org/#/tool/password-manager) (en inglés)
- Security In-a-box / Crear y mantener contraseñas fuertes (https://securityinabox.org/es/guide/passwords/)
- Security Self-defense / Animated Overview: Using Password Managers to Stay Safe Online (https://ssd.eff.org/en/module/animated-overview-using-password-managers-stay-safe-online) (en inglés)
- Surveillance Self-defense / Cómo Usar KeePassXC (https://ssd.eff.org/es/module/c%C3%B3mo-usar-keepassxc)
- Surveillance Self-defense / Creando Contraseñas Seguras (https://ssd.eff.org/es/module/creando-contrase%C3%B1as-seguras)
- Security Education Companion / Passwords (https://sec.eff.org/topics/passwords) (en inglés)
- Security Education Companion / Password Managers (https://sec.eff.org/topics/password-managers) (en inglés)