

Principio 3: “Usa contraseñas fuertes”

En la actualidad, toda información sensible a ser accedida por medios digitales (cuentas de home banking, e-mail, acceso a sistemas, etc.) debe ser protegida debidamente con una contraseña. Por lo general, el usuario adquiere acceso a un recurso, ingresando un identificador (nombre de usuario, e-mail, DNI, etc.), más la contraseña en cuestión.

Las contraseñas son las llaves de acceso a información de índole personal y/o financiera. Por lo tanto, es valiosa para un intruso o un atacante.

Existen diferentes medios por los que estos pueden obtener las contraseñas de los usuarios. Algunos de ellos son técnicos, a través de aplicaciones que permiten encontrar las contraseñas a través del método de prueba/error y la realización de cientos de pruebas por minuto de manera automática. Otras técnicas son manuales, como la Ingeniería Social (ver *Principio 2: “No brindes información indebida”*) y el uso del ingenio humano para obtener las contraseñas de acceso a un recurso determinado.

Es por ello que se debe tener en cuenta la gravedad de un acceso indebido a la información. La elección de la contraseña es una tarea que debe realizarse tomando ciertos recaudos para construir lo que se denomina una **contraseña fuerte**.

Entre los consejos más importantes se incluye que la contraseña debe ser, a la vez fácil de recordar, pero sin la necesidad de ser anotada. De ser necesario su anotación, es conveniente hacerlo en forma encriptada ó codificada. Para este fin, existe software de gestión de datos personales para el que solo debemos conocer una contraseña maestra, y todas las demás serán almacenadas en forma segura.

Precauciones

Para construir contraseñas fuertes, tener en cuenta las siguientes precauciones:

- **No utilizar contraseñas simples.**
 - No utilizar nombres propios.
 - No utilizar nombres de mascotas, parientes o aspectos cotidianos.
 - No utilizar fechas de cumpleaños o aniversarios
 - No utilizar números de identificación personal (DNI, Legajo laboral, Número de teléfono).
 - No utilizar series de números consecutivas ni todos sus caracteres iguales (12345678, aaaaaaaa, 22222222).

Estos datos se pueden obtener fácilmente utilizando *Ingeniería Social*. En el caso de palabras de uso cotidiano, su decodificación es más simple para los programas de vulneración de sistemas dado que utilizan diccionarios para la búsqueda de combinaciones de palabras a razón de cientos por minuto.

- **Utilizar contraseñas largas.** Se recomienda al menos 8 caracteres de longitud.
- **Combinar diferentes tipos de caracteres.** Utilizar en las contraseñas al menos dos tipos de los siguientes dígitos:

- Números.
 - Letras mayúsculas.
 - Letras minúsculas.
 - Signos de puntuación.
 - Caracteres del código ASCII.
- **Utilizar contraseñas recordables.** Sin hacer uso de lo expuesto en el primer ítem, se pueden utilizar otro tipo de combinaciones o aspectos recordables. Por ejemplo, combinaciones de iniciales de familiares, películas favoritas o aspectos más complejos de adivinar para un intruso, pero de simple recuerdo para el usuario.
 - **Rotar las contraseñas periódicamente.** Para lograr que una posible contraseña robada, carezca de utilidad; es recomendable modificar periódicamente las contraseñas. El tiempo recomendado para modificar una contraseña dependerá de la criticidad del servicio al que brinda acceso.
 - **No utilizar contraseñas por defecto.** El usuario *nunca* debe dejar la contraseña por defecto del fabricante o proveedor. Mucho menos utilizar "Administrador" o sus derivaciones (admin1234, admin, adminstrator). Estas contraseñas son de dominio público y fáciles de vulnerar.

En conclusión, cuanto más heterogénea sea la composición de una contraseña, mayor seguridad brindará al usuario.

Autor: Damián Altamirano - Openware

El presente artículo es uno de los principios publicados por **Openware**, en el marco de la **Semana Internacional de la Seguridad Informática**. Para visualizar el resto de los textos de concientización, consulte el siguiente sitio Web:
http://www.openware.biz/es/noticias/semana_internacional_de_la_seguridad_informatica_principios_de_seguridad_%E2%80%9Cdale_valor_tu_inf

Licencia

El presente artículo es liberado bajo [licencia Creative Commons](#).

Usted es libre de:

- copiar, distribuir, exhibir, y ejecutar la obra.
- hacer obras derivadas de ella.

Bajo las siguientes condiciones:

- Usted debe atribuir la obra en la forma especificada por el autor o el licenciente.
- Usted no puede usar esta obra con fines comerciales.
- Si usted altera, transforma, o crea sobre esta obra, sólo podrá distribuir la obra derivada resultante bajo una licencia idéntica a ésta.

<http://creativecommons.org/licenses/by-nc-sa/2.5/ar/>