Guía práctica
Sobre el uso de contraseñas

Recomendaciones para la elección de contraseñas fuertes

ArCERT - Coordinación de Emergencias en Redes Teleinformáticas de Argentina.
ONTI - Oficina Nacional de Tecnologías de Información.
versión 1.0 - Abril de 2009

SsTG Subsecretaría de Tecnologías de Gestión
SECRETARÍA DE LA GESTIÓN PÚBLICA

SGP Secretaría de la Gestión Pública
JEFATURA DE GABINETE DE MINISTROS

Jefatura de Gabinete de Ministros
Presidencia de la Nación

Consideraciones sobre el uso de contraseñas.

Descuidar una contraseña, o elegirla sin un buen criterio, posibilita que pueda ser obtenida muy fácilmente y utilizada para perjudicarlo de diversas maneras, tanto a usted como a la organización a la que pertenece.

Dado que el uso de la combinación de nombre de usuario y clave es el método mayormente utilizado para acceder a una multiplicidad de servicios y aplicaciones, le hacemos llegar esta guía de buenas prácticas para el uso y elección de contraseñas.

El nombre de usuario y la contraseña constituyen las credenciales que sirven de única identificación para acceder a la mayoría de los servicios que se brindan por Internet, ya sea correo electrónico, redes sociales, banca electrónica o “home banking”, sitios de compra en línea, servicios de chat, portales de juegos, etc.

No menos importantes son los accesos a redes internas corporativas o gubernamentales, conocidas como “intranets”, a las estaciones de trabajo o equipos hogareños, y a dispositivos de conexión, como “routers” o “switches”. Los escenarios donde se utilizan son muy variados y los límites entre el uso laboral y hogareño no son exclusivos.

Especialmente interesa a los fines de este documento, recomendar que se tengan presentes algunos riesgos que pueden afectar su información y que ésto lo motive a tomar recaudos, ya que las credenciales cumplen la función de identificarlo para darle acceso y proteger sus datos, sus fotos, documentos de terceros o de las organizaciones a las que pertenece, etc.

Es por ello, que se deben establecer normas para el uso adecuado de las contraseñas para prevenir que éstas sean vulneradas y utilizadas por terceros para acceder a su información y a los sistemas de forma ilegítima.

Este documento está dirigido a usuarios de servicios informáticos en general, asumiendo que las particularidades que puedan presentarse en el ámbito de cada organización deberán ser consultadas con las áreas de sistemas o seguridad de la información, según corresponda, sin perjuicio de que, como toda buena práctica, deben también ser utilizadas por técnicos, desarrolladores, administradores, gerentes medios, autoridades, etc.

Recomendaciones generales para el uso de contraseñas:

✔ Cuide que no lo vean cuando escribe su clave y no observe a otros mientras lo hacen.
✔ No comparta su clave con otros, ni pida la clave de otros.
✔ No escriba la clave en un papel ni la guarde en un archivo sin cifrar.
✔ Si por algún motivo tuvo que escribir la clave, no la deje al alcance de terceros (debajo del teclado, en un cajón del escritorio, etc.) y NUNCA pegada al monitor.
✔ No habilite la opción de “recordar claves/contraseñas” en los programas que utiliza.
✔ NUNCA envíe su clave por correo electrónico o chat ni la mencione en una conversación presencial o telefónica, ni se la entregue a nadie, aunque sea o diga ser el administrador del sistema.
✔ No mantenga una misma contraseña indefinidamente. Cámbiela regularmente, aunque las políticas de Administración de Claves no lo obliguen expresamente.
✔ No dude en cambiar sus contraseñas si sospecha que alguien puede conocerlas. Adicionalmente, en el ámbito laboral, hágale saber al administrador de la red cualquier incidente que tenga con su cuenta.
✔ No utilice ni permita que le asignen una cuenta sin contraseña.
✔ Si se le ha otorgado una contraseña para el primer acceso a un sistema o si la ha olvidado, proceda a cambiarla en forma inmediata, aún cuando el mismo sistema no se lo requiera.
✔ Si debe acceder a algún servicio o a su correo electrónico en un lugar público, por ejemplo un cibercafé, considere que su clave puede haber sido espiada o comprometida, por lo que se recomienda que proceda a cambiarla ni bien le sea posible.

Características que debe reunir una contraseña para que sea segura:

A continuación encontrará las principales características que debe tener una contraseña para ser considerada segura:

(a) Personal: cada persona que acceda a un servicio, aplicación o sistema debe tener su propia contraseña.
(b) Secreta: sólo el usuario de la contraseña debe conocerla.
(c) Intransferible: la contraseña no debe ser revelada a ningún tercero para su uso.
(d) Modificable sólo por el titular: el cambio de contraseña, sea cual fuere el motivo, debe ser realizado por el usuario titular de la misma. Sólo en situaciones excepcionales, podría ser cambiada por el administrador, por ejemplo, cuando el usuario la hubiera olvidado o si estuviera en riesgo la seguridad de la organización, como sería en el caso de que fuera divulgada o detectada como débil luego de una auditoría.

(e) Difícil de averiguar: Al momento de elegir su nueva contraseña, el usuario debe seguir ciertos lineamientos que impidan que pueda ser obtenida fácilmente. Más adelante se verán algunas sugerencias.

Recomendaciones para la elección de contraseñas fuertes:

Una contraseña débil, como el nombre de su hijo o de su perro es fácilmente predecible. Un caso especial son los dispositivos de conexión como routers hogareños, donde la mayoría de las veces se suelen mantener la misma contraseña que trae de fábrica, convirtiéndose en blanco trivial para ataques.

En el ámbito de las organizaciones, este tema debe estar contemplado en la política de seguridad de la información, generalmente formando parte de un apartado especial sobre control de accesos lógicos, formalizando el procedimiento adoptado para la creación de contraseñas, así como las condiciones de uso dependiendo el recurso y el tipo de información al que se brinda acceso.

Dicho procedimiento debe especificar:

(1) Un plazo de caducidad.
(2) Una longitud mínima.
(3) El conjunto de caracteres utilizables (en ciertas aplicaciones no se permiten, por ejemplo, caracteres especiales como “*”, “$”, “#”, etc.).
(4) Un diccionario de términos no permitidos, como nombres propios, días de la semana, meses, estaciones del año, etc., si fuera aplicable.

Algunas de las técnicas que pueden utilizarse para formar una clave robusta o fuerte, que conlleve cierta dificultad para averiguarla, pero que al mismo tiempo, permita ser recordada sin dificultad, son las que se listan a continuación. Tenga en cuenta que pueden existir sistemas particulares que por sus características, podrían no estar preparados para aceptar algunas de las técnicas enumeradas.

(1) No utilice palabras comunes o que se encuentren en un diccionario, ni nombres propios o de fácil deducción por terceros (nombre de mascota, nombre de equipo de fútbol favorito, etc.), ya que estas claves podrían ser conseguidas fácilmente mediante el uso de técnicas que realizan pruebas de forma automática utilizando palabras extraídas de diccionarios. Mucho menos su nombre de usuario o nombre de pila.
(2) No las vincule a una característica personal, (número de teléfono o D.N.I., patente del automóvil, etc.).
(3) No utilice terminología técnica conocida. Por ejemplo: “admin”.

(4) Combine caracteres alfabéticos en mayúscula y minúscula, números y caracteres especiales, como espacio, guión, símbolo “$”, etc.

(5) Constrúyalas utilizando 8 caracteres o más.
(6) Use claves distintas para máquinas y/o sistemas diferentes.
(7) Use un acrónimo de algo fácil de recordar. Por ejemplo: "NorCarTren" (Norma , Carlos, Tren).
(8) Añada números al acrónimo para mayor seguridad: "NorCarTren1810" (Norma, Carlos, Tren, Año de la independencia Argentina).

(9) Utilice frases conocidas o nombres de películas o libros en forma concatenada. Por ejemplo: "veranodel42".
(10) Elija una palabra sin sentido, aunque pronunciable. Por ejemplo: "galpo-glio".
(11) Realice reemplazos de letras por signos o números. Por ejemplo: "3duard0palmit0".
(12) Elija una clave que no pueda olvidar, para evitar escribirla en alguna parte. Por ejemplo: "arGentina6-0aza".
(13) Utilice las primeras letras de un dicho o frase célebre. Por ejemplo: "NpmmsamT" (No por mucho madrugar se amanece más temprano).
Preferentemente incluya además signos de puntuación: "Npmm,samT."
(14) Defina su propia regla de construcción sobre la base de una canción, frase, poema o texto que pueda recordar u obtener fácilmente. Por ejemplo, una regla podría ser:

> (a) seleccionar la frase,
> (b) elegir la primera letra de cada palabra
> (c) poner las primeras dos letras en "minúscula", las segundas dos en mayúsculas" y así sucesivamente, hasta tener una longitud de 8 caracteres ("mmMMmmMM"),
> (d) elegir un número de 2 cifras (que recordemos): si el número es impar entonces colocarlo al inicio de la clave; si por el contrario es par colocarlo al final.
> (e) agregar al número un carácter especial, "-" entre los dígitos. Por ejemplo: si el número es "01", quedaría "0-1".
>
> Si tomamos por ejemplo, la letra de la canción de María Elena Walsh:
> "M*anuelita* v*ivía* e*n* P*ehuajó,* p*ero* u*n* d*ía* s*e* m*archó.*
> *Nadie supo bien por qué, a París ella se fue*
> *un poquito caminando y otro poquitito a pie. ..... "*
> y elegimos el número "04" (que corresponde al número del mes en el que debo cambiar la clave), entonces la nueva contraseña, según la regla de construcción sería: "mvEPpuDS0-4"
>
> Otra sugerencia para lograr una mayor longitud, es directamente utilizar frases separando las palabras por algún carácter. Por ejemplo: "manuelitA-viviA_En-Pehuajo".

(15) Si el sistema lo permite, puede también utilizar frases de longitud considerable como contraseña. Este método es mencionado en algunas ocasiones como "passphrase".

Siguiendo el ejemplo anterior, podría utilizar “Manuelita vivía en Pehuajó, un poquito caminando, y otro poquitito a pie”.

Por último, recomendamos especialmente NO utilizar ninguna de las claves que han sido enumeradas como ejemplo en este documento, ya que pueden ser utilizadas por un tercero para probar si puede acceder a sus cuentas.
Los lineamientos descriptos no pretenden reemplazar las políticas y procedimientos internos establecidos en cada organización, constituyendo sólo recomendaciones y buenas prácticas.

En caso de dudas, correcciones o sugerencias para mejorar este documento, le agradeceremos nos envíe un correo electrónico a: info@arcert.gob.ar.