

Ministerio de  
Educación Nacional  
República de Colombia



## Recomendaciones de uso de contraseñas seguras

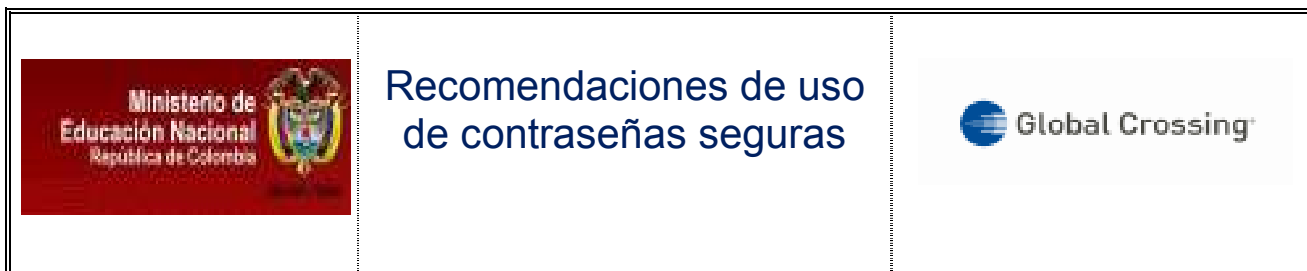


# Recomendaciones de Uso De Contraseñas Seguras

Preparado para:  
Ministerio de Educación

por:  
Johanna Quintero  
Global Crossing

9 Marzo 2010



## Tabla de contenido

1.	Introducción .....	3
2.	Como escoger una contraseña segura .....	4
3.	Para tener en cuenta .....	6
	Otros usuarios preguntando acerca de la información de conexión (login) y contraseña .	6
4.	Estrategias y Consejos para el uso de contraseñas.....	7



### 1. **Introducción**

Las contraseñas ofrecen la primera línea de defensa contra el acceso no autorizado al correo electrónico. Cuanto más segura sea la contraseña, más protegida estará la cuenta contra hackers y software malintencionado. Debe tener siempre contraseñas seguras para todas las cuentas.

A continuación se relacionan algunas de las contraseñas más usadas por los usuarios en internet:

1. password
2. 123456
3. qwerty
4. abc123
5. letmein
6. monkey
7. myspace1
8. password1
9. link182
10. (primer nombre del usuario)



## 2. Como escoger una contraseña segura

Una contraseña segura es el primer paso necesario para asegurar la seguridad de los usuarios de sus Aplicaciones (computadora, cuenta de correo, cuenta de ahorros, usuario de red, Aplicaciones web, etc, ). Su contraseña debería cumplir todos los requisitos mínimos descritos a continuación:

- Debe tener 14 caracteres o más. El requisito mínimo es de ocho caracteres.
- No contiene el nombre de usuario, el nombre real o el nombre de la empresa.
- No contiene una palabra completa.
- Es significativamente diferente de otras contraseñas anteriores.
- Está compuesta por caracteres de cada una de las siguientes cuatro categorías:

Categoría de caracteres	Ejemplos
Letras mayúsculas	A, B, C
Letras minúsculas	a, b, c
Números	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Símbolos del teclado (todos los caracteres del teclado que no se definen como letras o números) y espacios	` ~ ! @ # \$ % ^ & * ( ) _ - + = { } [ ] \   : ; " ' < > , . ? /

Una contraseña puede reunir todos los criterios anteriores y aun así ser insegura. Por ejemplo, **Hello2U!** cumple con todos los criterios mencionados para una contraseña segura, pero es insegura porque contiene una palabra completa. **H3ll0 2 U!** es una alternativa más segura porque reemplaza algunas de las letras en la palabra completa con números e incluye espacios.

Puede aplicar las siguientes recomendaciones para recordar una contraseña segura:

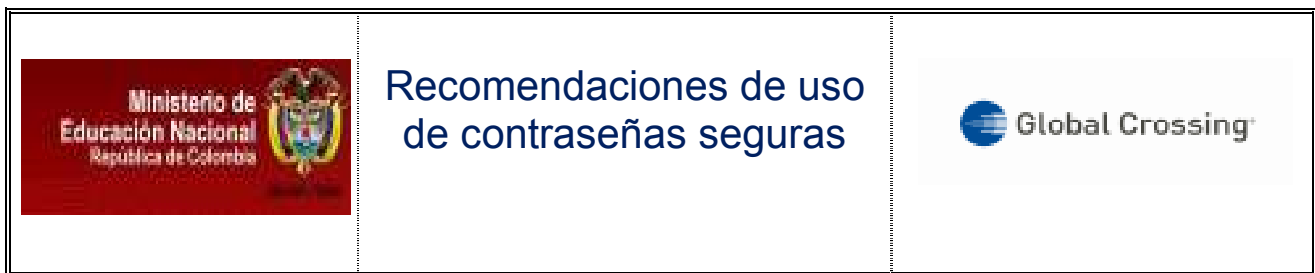
- Cree una sigla con una información que sea fácil de recordar. Por ejemplo, elija una frase que tenga significado para usted, como Mi hijo nació el 12 de diciembre de 2004. Con esa frase como guía, puede usar Mhne12/Dic,4 como contraseña.
- Use números, símbolos y errores de ortografía para reemplazar letras o palabras en una frase fácil de recordar. Por ejemplo, Mi hijo nació el 12 de diciembre de 2004



puede transformarse en M'igo n@\$io 12124 (se pueden usar espacios en la contraseña).

- Relacione la contraseña con un pasatiempo o deporte favorito. Por ejemplo, Me encanta el bádminton puede transformarse en Mn'kant6ehIB@dm1nt()n.
- Combinar palabras cortas con algún número o carácter de puntuación: soy2\_yo3
- Usar un acrónimo de alguna frase: A Rio Revuelto Ganancia De Pescadores, y puede usar como contraseña ArRGdP.
- Añadir un número al acrónimo para mayor seguridad quedando así A9r7R5G3d1P
- Elegir una palabra sin sentido, aunque pronunciable: taChunda72, AtajulH, Wen2Mar
- Puede verificar que nivel de seguridad tiene su contraseña en <http://www.microsoft.com/latam/protect/yourself/password/checker.aspx>

Si considera que debe anotar la contraseña para poder recordarla, recuerde que no debe dejar escrito que es su contraseña y debe mantenerla en un lugar seguro.



### 3. Para tener en cuenta

Los ladrones de cuentas tienen varios métodos de ataque la mayoría de los robos de cuentas ocurren cuando los usuarios comparten la información de su cuenta de correo con un ladrón. Preste atención a las actividades que se nombran a continuación para asegurar la seguridad de su cuenta:

#### **Otros usuarios preguntando acerca de la información de conexión (login) y contraseña**

Peticiones de su información de conexión (login) o contraseñas de usuarios en Correos Electrónicos Malintencionados en los que indican labores de Mantenimiento o a través de servicios de mensajería instantánea como el SPARK, Messenger, etc.



#### 4. Estrategias y Consejos para el uso de contraseñas

**No incluya secuencias ni caracteres repetidos.** Cadenas como "12345678", "222222", "abcdefg" o el uso de letras adyacentes en el teclado no ayudan a crear contraseñas seguras.

**Evite utilizar únicamente sustituciones de letras por números o símbolos similares.**

Los delincuentes y otros usuarios malintencionados que tienen experiencia en descifrar contraseñas no se dejarán engañar fácilmente por reemplazos de letras por números o símbolos parecidos; por ejemplo, 'i' por '1' o 'a' por '@', como en "M1cr0\$0ft" o en "C0ntr@señ@". Pero estas sustituciones pueden ser eficaces cuando se combinan con otras medidas, como una mayor longitud, errores ortográficos voluntarios o variaciones entre mayúsculas y minúsculas, que permiten aumentar la seguridad de las contraseñas.

**No utilice el nombre de inicio de sesión.** Cualquier parte del nombre, fecha de nacimiento, número de la seguridad social o datos similares propios o de sus familiares constituye una mala elección para definir una contraseña. Son algunas de las primeras claves que probarán los delincuentes.

**No utilice palabras de diccionario de ningún idioma.** Los delincuentes emplean herramientas complejas capaces de descifrar rápidamente contraseñas basadas en palabras de distintos diccionarios, que también abarcan palabras inversas, errores ortográficos comunes y sustituciones. Esto incluye todo tipo de blasfemias y cualquier palabra que no diría en presencia de sus hijos.

**Evite utilizar sistemas de almacenamiento en línea.** Si algún usuario malintencionado encuentra estas contraseñas almacenadas en línea o en un equipo conectado a una red, tendrá acceso a toda su información.

**No dejar las contraseñas por defecto.** Siempre que le sea asignado un usuario y contraseña, proceda a cambiar dicha contraseña de forma inmediata de acuerdo a las recomendaciones dadas y mucho más si la entrega se realizó vía correo electrónico.

**No las revele a nadie.** No deje sus contraseñas a la vista de familiares o amigos (sobre todo de los niños), ya que podrían facilitarlas de buena fe a personas menos merecedoras de



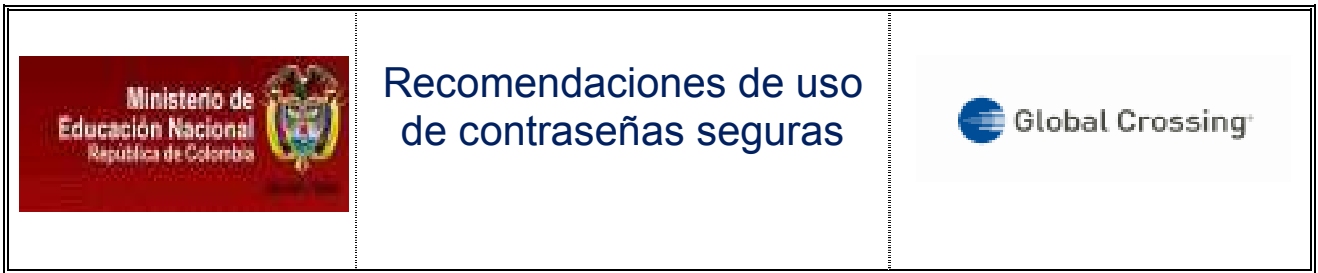
confianza. Las contraseñas que deba compartir (por ejemplo, la de una cuenta corriente en línea con otros titulares, como su cónyuge) constituyen las únicas excepciones.

**No facilite nunca su contraseña por correo electrónico ni porque se le pida por ese medio.** Desconfíe de cualquier mensaje de correo electrónico en el que se le pide la contraseña o se le indica que debe visitar un sitio web para comprobarla. Casi con total seguridad se trata de un fraude. Esto incluye las solicitudes desde empresas y personas de confianza. El correo electrónico se puede interceptar en tránsito, y un mensaje en el que se solicite información podría no proceder realmente del remitente que supuestamente lo envía. En las estafas de suplantación de identidad (phishing) a través de Internet, los timadores pueden utilizar mensajes de correo electrónico fraudulentos para convencerle de que revele nombres de usuario y contraseñas y robarle datos de identidad.

**Cambie sus contraseñas con regularidad.** Esto puede ayudar a despistar a los delincuentes y a otros usuarios malintencionados. El nivel de seguridad de su contraseña contribuirá a prolongar la vigencia de ésta. Una contraseña que tenga menos de 8 caracteres no debe mantenerse durante un período superior a una semana, mientras que una contraseña de 14 caracteres o más (y que cumpla las otras normas indicadas anteriormente) puede mantenerse sin problemas durante varios años.

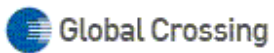
**No escriba contraseñas en equipos que no controla.** Los equipos que se encuentran en lugares como cibercafés, aulas de informática, entornos compartidos, sistemas de quiosco, salas de conferencias y terminales de aeropuertos deben considerarse no seguros para cualquier uso personal que no sea una exploración de Internet anónima. No utilice estos equipos para consultar correo electrónico en línea, comunicaciones de chat, comprobación de estados de cuentas bancarias, correo electrónico de empresa ni para utilizar ninguna cuenta que requiera un nombre de usuario y una contraseña. Los delincuentes pueden adquirir por muy poco dinero dispositivos de registro de pulsaciones que se instalan en tan sólo unos instantes. Estos dispositivos permiten a usuarios malintencionados recopilar a través de Internet toda la información que se ha tecleado en un equipo (las contraseñas y las frases codificadas son tan valiosas como los datos que protegen).

**Si considera que debe anotar la contraseña para recordarla.** Recuerde que no debe dejar escrito que es su contraseña y debe mantenerla en un lugar seguro.



Estas recomendaciones y sugerencias se emiten el 9 de Marzo de 2010.

**Johanna Quintero**  
Datacenter Specialist



tel. (57 1) 6119000 Ext.3909  
Cel: (57) 318-7346387