

SUBPROCESO DE SEGURIDAD INFORMÁTICA

MAYO - JUNIO DE 2022
BOLETÍN NO 9

En este boletín:

PÁGINA 1

Análisis de caso

PÁGINA 2

Recomendaciones para
generar una contraseña
segura.

PÁGINA 3

Generadores Online de
contraseñas seguras.

PÁGINA 4

Conclusiones

PÁGINA 5

Números de contacto

 Username or email



login

UNA CONTRASEÑA FÁCIL, PUERTA DE ACCESO A UN MUNDO DE INFORMACIÓN

Análisis de caso

Hugo tiene por costumbre llegar a casa después de una larga jornada laboral, encender su computadora personal, abrir su cuenta de correo y eliminar los mensajes innecesarios como también desocupar el buzón de Spam. Usualmente no tiene cuenta de estos mensajes, pero, en esta oportunidad un correo le llamo la atención

El asunto del correo era directo y convincente: "Por procedimientos de seguridad, suspendimos de manera temporal el acceso a los canales virtuales". Al revisar el cuerpo del mensaje Hugo encontró un enlace en el que le facilitan el cambio de contraseña.

El mensaje manifestaba una urgencia, sin embargo, había algo en el mensaje que le generaba sospecha, por lo que le solicito ayuda a unos de sus hijos. En la revisión con detenimiento del correo, se confirmaron las sospechas: el mensaje era un intento de phishing.

Los ciberdelincuentes tenían como objetivo capturar el usuario y contraseña. Lo anterior no era lo más grave, pues Hugo utilizaba solo una contraseña para todas sus cuentas (correos, entidades bancarias, redes sociales, archivos en drive, entre otros). Una contraseña única para todas las plataformas para evitar olvidos.

Ante este inconveniente Hugo decide no arriesgarse más y opto por mejorar la seguridad de todas sus cuentas, lo primero es generar una contraseña segura: dejaría atrás su antigua contraseña H654321 y tendría presente las siguientes recomendaciones.

Notificación de Seguridad



Apreciado Cliente,

Por procedimientos de seguridad, suspendimos de manera temporal el uso de sus productos y el acceso a los canales virtuales.

Lo invitamos a restablecer el acceso a todos nuestros canales, para ello debemos verificar la titularidad de usted como cliente.

Haga click en el link y comience el proceso de manera rápida, ágil y segura. Así de fácil, sin necesidad de desplazarse a una oficina.

[Restablecer mi Cuenta](#)

[<http://sneaker****.gr/https/>](http://sneaker****.gr/https/)

Diligencie la información solicitada, nuestro sistema verificará de manera inmediata y usted ingresará de manera normal a su cuenta, y de esta manera continúa disfrutando de todos nuestros servicios nuevamente.

En Bancolombia a un Clic estamos innovando para que pueda disfrutar de más tiempo libre, tener la oportunidad de contar con servicios ágiles y simples, y estar para usted cuando, como y donde nos necesite.

Juan Diego Agudelo Ordóñez
Gerencia Canales Digitales

RECOMENDACIONES PARA GENERAR UNA CONTRASEÑA SEGURA

1. Números y letras: Una contraseña con solo números o solo letras no es recomendable. Se sugiere en términos de seguridad que sea una combinación de ambas.

PASSWORD **mAr25Z70** ✓

2. Mayúsculas y minúsculas: Alternar entre números y letras es lo más adecuado, se recomienda el uso de Mayúsculas y minúsculas procure no repetir un carácter por más de 3 veces.

PASSWORD **mAr25Z70** ✓

3. Longitud de 8 a 16 caracteres: Se sugiere que la contraseña debe tener como mínimo 8 caracteres de longitud hasta 16 caracteres como máximo (VAF-PI-001- UDES). Recuerda a más caracteres es una contraseña más segura.

PASSWORD **mAr25Z0070** ✓

4. Caracteres especiales: Los caracteres especiales son se tratan de símbolos, por lo general algunos sistemas sugieren el uso de los más convencionales.

PASSWORD **m@r25Z0#70** ✓

5. Nunca utilice la misma contraseña para diferentes plataformas: Como es difícil muchas veces recordar una contraseña diferente en todas las plataformas, se recomienda utilizar alguna frase o palabra que sea cómoda para usted y de fácil recordación, puede anteponer la primera letra de la plataforma que tiene previsto abrir.

Password: C0ntR4s3ñA*

Facebook: **F**C0ntR4s3ñA*

Correo institucional: **U**C0ntR4s3ñA*

GENERADORES ONLINE DE CONTRASEÑAS SEGURAS

En Internet podemos encontrar diferentes programas en línea que te pueden ayudar a generar contraseñas seguras, en este boletín recomendaremos tres (3) de los mejores:



Es un sitio web que te permite generar contraseñas de manera fácil y seguras, el sistema permite escoger el tipo u la longitud. Como detalle tiene la posibilidad de escoger una contraseña segura de fácil recordación. Esta página cuenta con un algoritmo que escoge fragmentos de palabras al azar.

Para ingresar a clave segura, puedes dar clic en el siguiente enlace:

[CLICK AQUI](#)



Algunas empresas que suministran servicios de antivirus promueven campañas para que los usuarios generen contraseñas seguras, Avast es una de ellas. Desde su entorno web ofrece esta posibilidad de manera rápida, además la página cuenta con una tabla de medición que nos permite saber el nivel de seguridad de nuestra contraseña.

Para ingresar a este servicio puedes ingresar desde el siguiente enlace

[CLICK AQUI](#)

En esta página puede generar una contraseña de manera dinámica. Permite seleccionar entre la longitud mediante una barra de desplazamiento o la manera en cómo quiere recordarla (fácil de recordar, fácil de leer o con todos los caracteres).

Para ingresar a Lastpass puedes ingresar desde el siguiente enlace

[CLICK AQUI](#)

CONCLUSIONES



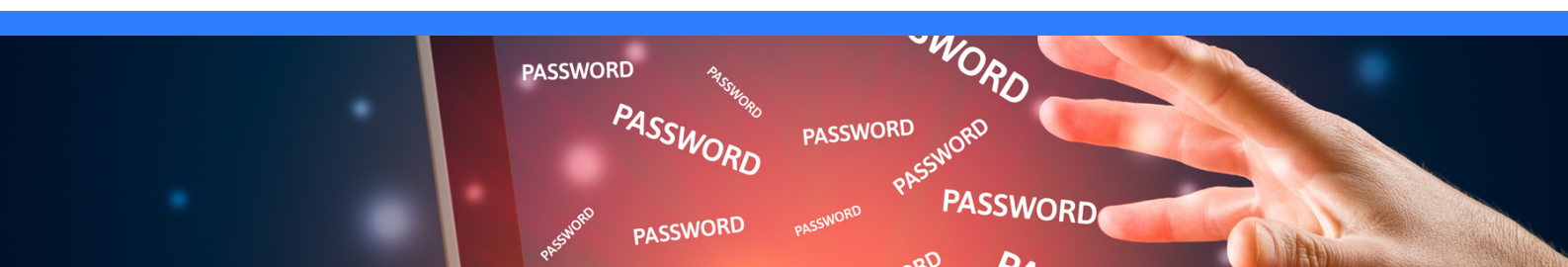
Si hacemos nuestras contraseñas seguras evitaremos que terceros ingresen a nuestra información. Recuerde que Internet puede ser una enorme grieta para acceder a los datos del usuario.

Recuerde cambiar la contraseña de manera frecuente y no utilice la misma para cuentas diferente. El cambio de algún carácter puede ayudar a proteger sus datos.



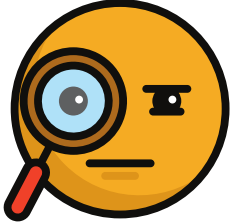
Aunque parezca difícil cambiar las “A” por “4” o las “E” por “3” es una gran forma de despistar y tener una contraseña segura.

Si tienes presente la información que brinda este boletín, tu navegación por Internet permanecerá segura en consecuencia podrás proteger todos tus datos personales de forma efectiva.



Dato Curioso

Según un artículo publicado en el boletín de www.techrepublic.com, la siguiente tabla nos muestra el tiempo que tarda un hacker en descifrar tu contraseña.



Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	1 sec	5 secs
7	Instantly	Instantly	25 secs	1 min	6 mins
8	Instantly	5 secs	22 mins	1 hour	8 hours
9	Instantly	2 mins	19 hours	3 days	3 weeks
10	Instantly	58 mins	1 month	7 months	5 years
11	2 secs	1 day	5 years	41 years	400 years
12	25 secs	3 weeks	300 years	2k years	34k years
13	4 mins	1 year	16k years	100k years	2m years
14	41 mins	51 years	800k years	9m years	200m years
15	6 hours	1k years	43m years	600m years	15 bn years
16	2 days	34k years	2bn years	37bn years	1tn years
17	4 weeks	800k years	100bn years	2tn years	93tn years
18	9 months	23m years	6tn years	100 tn years	7qd years

Fuente: <https://www.techrepublic.com/article/how-an-8-character-password-could-be-cracked-in-less-than-an-hour/#>

!RECUERDA!

**!SI PRESENTAS DUDAS O
ALGUNA SITUACIÓN
SOSPECHOSA CONTÁCTANOS!**



Subproceso de Seguridad informática
UDES

- En Bucaramanga:
Correo: seguridadinformatica@udes.edu.co
Teléfono: (607) 6516500 Ext 1005 - 1001
- En Valledupar
Correo: lortiz@valledupar.udes.edu.co
Teléfono: (605) 5730073 Ext 129
- En Cúcuta:
Correo: wpena@udes.edu.co
Teléfono: (607) 5748717 Ext 4196

