Universidad Nacional Abierta y a Distancia
ACREDITADA EN ALTA CALIDAD

Centro de Respuestas a Incidentes Informáticos
CIP - CSIRT Académico UNAD

Boletín Informativo
Número **Seis**

Seguridad Digital: Responsabilidad de Todos

ECBπ
Escuela de Ciencias Básicas, Tecnología e Ingeniería

VIEM
Vicerrectoría de Innovación y Emprendimiento

Semillero de Investigación
Ceros y Unos

Medio de Divulgación del Centro de Respuestas a Incidentes Informáticos: CIP – CSIRT Académico UNAD

E-boletín Informativo CIP- CSIRT Académico UNAD

Edición electrónica, financiada por la Universidad Nacional Abierta y a Distancia (UNAD)

Medio de divulgación: Correo Electrónico, Sitio Web

Incluye: Noticias, alertas o informes relacionados con la disciplina de la ciberseguridad

Número Seis
Junio de 2022

Universidad Nacional Abierta y a Distancia (UNAD)
Vicerrectoría de Innovación y Emprendimiento (VIEM)
Escuela de Ciencias Básicas Tecnología Ingeniería (ECBTI)
CIP – CSIRT Académico UNAD

Vicerrectoría de Innovación y Emprendimiento (VIEM)
Ing. Andrés Ernesto Salinas - Vicerrector

Escuela de Ciencias Básicas Tecnología e Ingeniería (ECBTI)
Ing. Claudio Camilo González Clavijo – Decano

Especialización en Seguridad Informática (ECBTI)
Ing. Sonia Ximena Moreno Molano – Líder Programa de Especialización en Seguridad Informática

Semillero de Investigación Ceros y Unos, adscrito al Grupo de Byte InDesign

Centro de Respuestas a Incidentes Informáticos
CIP – CSIRT Académico UNAD
Ing. Luis Fernando Zambrano Hernández – Director CIP CSIRT Académico UNAD

Responsable de la Edición
Ing. Luis Fernando Zambrano Hernández

Estado legal:
Periodicidad: Quincenal
ISSN: **2806-0164**

Universidad Nacional Abierta y a Distancia
Calle 14 sur No. 14-23 |Bogotá D.C
Correo electrónico: csirt@unad.edu.co
Página web: https://csirt.unad.edu.co

Tabla de Contenido

Boletín informativo Número 5

Junio 10 de 2022

Seguridad Digital: Responsabilidad de Todos

Autores:

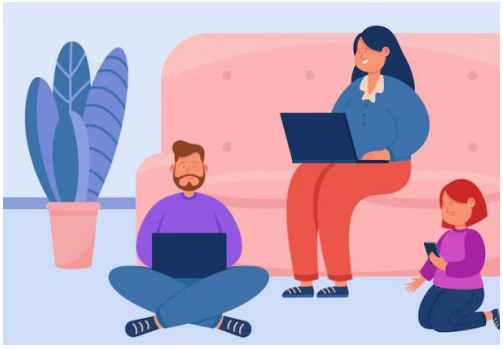
Luis Fernando Zambrano Hernández
ORCID: https://orcid.org/0000-0002-4690-3526

John Freddy Quintero Tamayo
ORCID: https://orcid.org/0000-0003-0128-1214

Néstor Raúl Cárdenas Corral
ORCID: https://orcid.org/0000-0003-3691-0148

Introducción

La seguridad digital es el factor base de buenas prácticas[1], políticas y procesos en el uso de tecnología software o hardware para salvaguardar la información. Los delincuentes informáticos estarán a la espera para poder vulnerar cualquier descuido por parte de los usuarios y de esta manera lograr obtener información como por ejemplo credenciales de redes sociales, correos electrónicos, banca móvil entre otros.



Recuperado de: https://www.freepik.es/

[1] Seguridad Digital | Colombia Aprende

Desarrollo

Banca móvil [2]:

Uno de los procesos más comunes en la actualidad en cuanto a aplicaciones es la banca móvil, muchos usuarios suelen hacer transferencias vía pasarelas de pago lo que se ha vuelto un objetivo por parte de la delincuencia en general, sin importar que tengan experiencia en el campo de la informática. La banca móvil viene implementando una serie de sistemas de control de acceso que tienen como objetivo mejorar la seguridad y experiencia de usuarios.

Basado en lo que el usuario sabe[3]:

Dentro de los sistemas de control de acceso el más popular se encuentra orientado a la memorización de contraseñas siendo una práctica de hace años y conformando uno de los sistemas de autenticación más básicos que existen conllevando a grandes fallos de seguridad como, por ejemplo: ataques de fuerza bruta haciendo uso de contraseñas donde intentan una y otra vez mediante múltiples combinaciones encontrar la contraseña correcta para un determinado usuario, pero quizás uno de los ataques más populares que no requieren software es el shoulder surfing o sorfear sobre el hombro de la víctima para obtener su contraseña.

Recuperado de: https://www.freepik.es/

Basado en lo que el usuario tiene:

Hace unos años atrás se viene implementando hardware el cual se conoce como sistemas tokens que no son más que un pequeño dispositivo el cual genera de manera aleatoria una cadena de seis dígitos, esta cadena numérica no se repite y es generada cada minuto. Con el pasar del tiempo y por temas de costos las grandes empresas empezaron a hacer uso del token digital que cuenta con el mismo principio del token físico, pero, con la diferencia que los números generados llegan al correo electrónico o vía mensaje de texto.

[2] Banca móvil: ¿Qué es banca móvil y cómo funciona? (bancodebogota.com)
[3] Mecanismos de autenticación para verificar la identidad - Redtrust

Basado en lo que el usuario es[4]:

Este sistema de control de acceso hace parte de los dispositivos biométricos los cuales por medio de la lectura de algunos parámetros del ser humano como: huellas dactilares, voz, iris, palma de la mano, venas o facial que logran identificar a un usuario determinado. Es importante resaltar que este sistema es uno de los más utilizados en la actualidad por la agilidad y seguridad que maneja, pero no todo sistema es perfecto y este no es la excepción dado que algunos cambios físicos del usuario pueden llevar a una no identificación, por ejemplo, si un usuario sufre de dermatitis será bastante difícil que sea identificado por un sistema de huellas, por otro lado, si un usuario tiene gripe sus pupilas se verán afectadas en el cambio de su radio lo que llevará a una no identificación o lectura correcta.

Recuperado: https://www.freepick.com

Estos tres sistemas de control de acceso apoyan al fortalecimiento de múltiples plataformas dentro de las que se encuentran la banca móvil. Dentro de los procesos de seguridad digital los cuales el CSIRT académico UNAD recomienda a la hora de una transacción segura se encuentran los siguientes factores:

- Hacer uso de una red móvil y no wifi, debido a que las redes wifi suelen ser más fácil de irrumpir por parte de un atacante lo que llevaría a que este pueda obtener información e interceptar datos.
- Utilizar VPN para que sus datos como usuarios viajen de manera cifrada entre punto y punto del servicio; cabe resaltar que este servicio no debe ser adquirido de manera gratuita ya que no se sabrá quien pueda visualizar los datos en claro, pagar el servicio es una opción, no es costoso.
- Haga uso siempre de un mismo dispositivo para dichas transacciones, sea desconfiado y piense que realizar una transacción desde un computador o móvil ajeno a los de su propiedad es una práctica que puede poner en peligro sus cuentas bancarias por intercepción o captura de información.
- Digite siempre en el navegador la url de su banco, si cuenta con una aplicación web descárguela directamente de la página del banco.

Cuentas de correo electrónico:

Las cuentas de correo electrónica se han convertido en la base de acceso a cualquier servicio como lo son redes sociales y banca móvil, indicando que si un atacante obtiene el correo es posible que pueda acceder a sus redes sociales y banca móvil. Por este motivo el CSIRT académico UNAD dispone las siguientes medidas las cuales contribuirán a fortalecer la seguridad digital no solo de su cuenta de correo sino de sus redes sociales:

Al momento de crear una contraseña tenga en cuenta los siguientes parámetros:

a. No use contraseñas que tengan un sentido gramatical para que no sea fácil de detectar por parte de un delincuente informático.
b. Utilice caracteres especiales como: *** / , . +** y uno de los más importantes la letra ñ[5]
c. Haga uso de contraseñas mínimo de 5 caracteres

d. No escriba o almacenes sus contraseñas en lugares visibles

Tenga en cuenta que entre mejor sea la combinación entre caracteres especiales más tiempo le tomará al delincuente informático en obtener la contraseña:

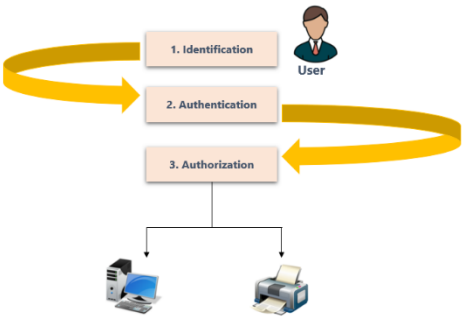
Tabla 1. *Tiempo de vulneración que lleva un atacante en descubrir contraseñas, según su complejidad*

Longitud	Minúscula	Agrega Mayúscula	Números y Símbolos
6 caracteres	10 minutos	10 horas	18 días
7 caracteres	4 horas	23 días	4 años
8 caracteres	4 días	3 años	463 años
9 caracteres	4 meses	178 años	44.530 años

Elaboración propia

La tabla anterior evidencia que la combinación entre longitud, minúscula, números y símbolos aumentan el tiempo en el que un atacante puede descifrar una contraseña. El proceso para combinar las contraseñas se basa en el procesamiento o equipo de cómputo de los atacantes, no es lo mismo atacar contraseñas con un computador con procesador corei3 a un servidor, entre más capacidad hardware se tenga mayores resultados obtendrán.

El factor de doble autenticación es un sistema implementado en la mayor parte de aplicaciones en el mundo. Muchos se preguntarán, ¿cómo funciona un factor de doble autenticación? Su funcionamiento es sencillo, un usuario determinado iniciará sesión con su login y password, pero anexo a esto deberá ingresar una segunda contraseña (2FA autenticación de dos factores) indicando que si está es incorrecta no se podrá iniciar sesión, además esa segunda contraseña en la mayoría de los casos se encuentra articulada con los sistemas de control de acceso basado en lo que el usuario tiene (token físico o digital).



Los 2FA hacen parte de la identificación, autenticación y autorización. En la siguiente imagen se podrá visualizar este proceso cómo funciona fusionando los parámetros anteriores:

Como primera medida el usuario debe ser identificado por el sistema esto se puede llevar a cabo por algún sistema biométrico, posteriormente se autentica indicando que el usuario es quien dice ser, si no fuera identificado de manera

[4] 52752700.pdf (unad.edu.co)
[5] Cómo crear una contraseña fuerte en un minuto y proteger tu identidad digital | WeLiveSecurity

correcta no podría ser autenticado, y como último paso el sistema autoriza el ingreso del usuario. El 2FA hace parte del proceso inicial de la identificación.

En los correos electrónicos al igual que en redes sociales se puede agregar la opción de 2FA como un método de prevención y buenas prácticas, además es un proceso gratuito que no requerirá de pagos o recargos extras a su facturación.

Canales de comunicación

El CIP CSIRT Académico UNAD, actualmente cuenta con los siguientes canales de comunicación:

- Correo: csirt@unad.edu.co
- Twitter: @csirtunad
- Página web: https://csirt.unad.edu.co

Recursos Bibliográficos Consultados

[1] Generación Digital Segura [en línea]. Colombia Aprende [fecha de consulta: 08/06/2022] Disponible en: https://www.colombiaaprende.edu.co/recurso-coleccion/seguridad-digital

[2] ¿Qué es la Banca Móvil? [en línea]. Banco de Bogotá [fecha de consulta: 08/06/2022] Disponible en: https://www.bancodebogota.com/wps/portal/banco-de-bogota/bogota/educacion-financiera/articulos-educacion-financiera/seguridad-financiera/que-es-banca-movil

[3] Mecanismos de autenticación para verificar la identidad [en línea]. Redtrust fecha de consulta: 08/06/2022] Disponible en: https://redtrust.com/mecanismos-autenticacion/

[4] Cómo crear una contraseña fuerte en un minuto y proteger tu identidad digital [en línea]. ESET [fecha de consulta: 07/06/2022] Disponible en: https://www.welivesecurity.com/la-es/2016/05/06/crear-contrasena-fuerte-un-minuto/#:~:text=Normalmente%2C%20se%20dice%20que%20una%20contrase%C3%B1a%20es%20fuerte,de%20peores%20contrase%C3%B1as%20habituales%20como%20%E2%80%9C123456%E2%80%9D%20o%20%E2%80%9Cpassword%E2%80%9D.

[5] ESTADO DEL ARTE DE LA SEGURIDAD EN SISTEMAS BIOMETRICOS [en línea]. UNAD [fecha de consulta: 06/06/2022] Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/14348/52752700.pdf?sequence=1&isAllowed=y