TALENTO TECH

TIC

REGIÓN 3

CAUCA – NARIÑO

LECCIÓN 1 - UNIDAD 1

Universidad Tecnológica de Pereira

faceIT

Ciberseguridad

TIC

La ciberseguridad son las tecnologías, procesos y aprendizaje que permiten proteger sistemas, redes y programas de ataques cibernéticos.
El principal objetivo de la ciberseguridad es lograr constantemente tres objetivos que son:

Confidencialidad: *La información solo debe ser visible para personas autorizadas.*

Integridad: *Los datos deben permanecer completos y solamente pueden ser modificados por personas autorizadas a través de procesos adecuados.*

Disponibilidad: *La información debe permanecer accesible y visible cuando un usuario autorizado la requiera.*

TALENTO TECH

Universidad Tecnológica de Pereira | faceIT

A este modelo se le conoce como CIA en el contexto de la ciberseguridad y son los pilares sobre los que se crean estrategias para compartir información en internet mientras se mantiene a salvo de atacantes.

Para determinar qué tipos de ataques se pueden sufrir al exponer información en internet es necesario definir un panorama de amenazas. Este panorama permite conocer los potenciales puntos de entrada de un ciber ataque y mitigarlos.

Algunos puntos de entrada comunes son:

- Cuentas de correo electrónico
- Cuentas de redes sociales
- Dispositivos móviles
- Infraestructura tecnológica
- Servicios en la nube
- Personas

Ciberseguridad

El panorama de amenazas no solo abarca computadores, puede incluir cualquier elemento tanto interno como externo a una organización ya que un atacante puede valerse de infraestructura interna o externa a una organización para robar información. También puede valerse de engaños para que personas pertenecientes a una organización abran brechas de seguridad.

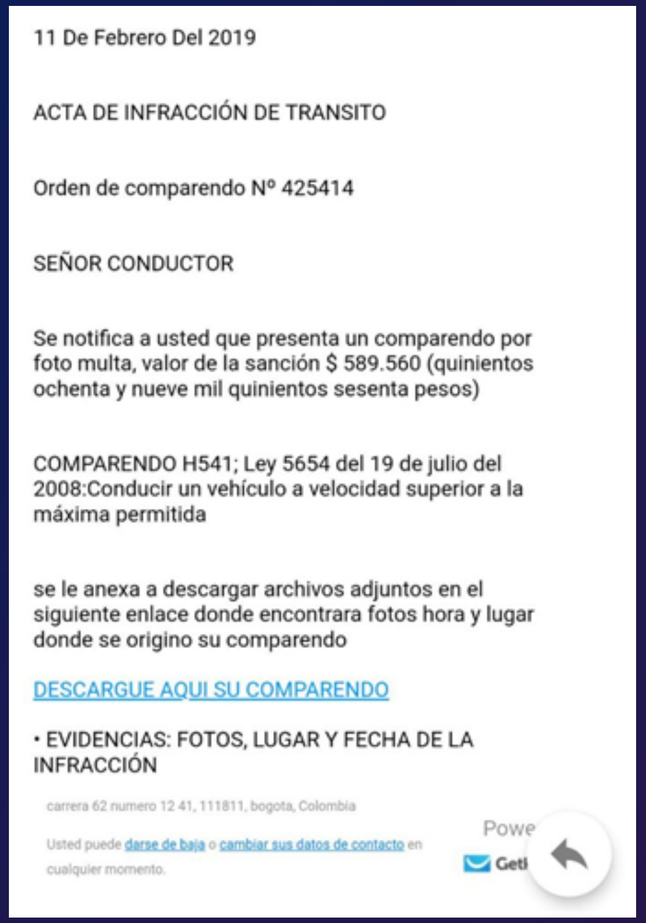
Vectores de ataque

Son todos los elementos que pueden convertirse en un punto de entrada para que una persona malintencionada obtenga acceso a un sistema. Entre los diferentes vectores se tiene:

TIC

El correo electrónico, a través del cual ciberdelincuentes envían mensajes que parecen legítimos y que pueden lograr que un usuario realice una acción. Por ejemplo, descargar un archivo, exponer un vínculo falso par robar contraseñas o incluso vínculos que descargan e instalan programas con los que atacantes se valen para el robo de información.

En Colombia desde el año 2021 han crecido considerablemente este tipo de amenazas con correos suplantando identidad, como, por ejemplo, haciéndose pasar por la fiscalía de la nación, por una autoridad de tránsito o por una entidad bancaria para que un usuario descargue archivos e infecte sus equipos y las redes empresariales.



11 De Febrero Del 2019

ACTA DE INFRACCIÓN DE TRANSITO

Orden de comparendo Nº 425414

SEÑOR CONDUCTOR

Se notifica a usted que presenta un comparendo por foto multa, valor de la sanción $ 589.560 (quinientos ochenta y nueve mil quinientos sesenta pesos)

COMPARENDO H541; Ley 5654 del 19 de julio del 2008:Conducir un vehículo a velocidad superior a la máxima permitida

se le anexa a descargar archivos adjuntos en el siguiente enlace donde encontrara fotos hora y lugar donde se origino su comparendo

DESCARGUE AQUI SU COMPARENDO

• EVIDENCIAS: FOTOS, LUGAR Y FECHA DE LA INFRACCIÓN

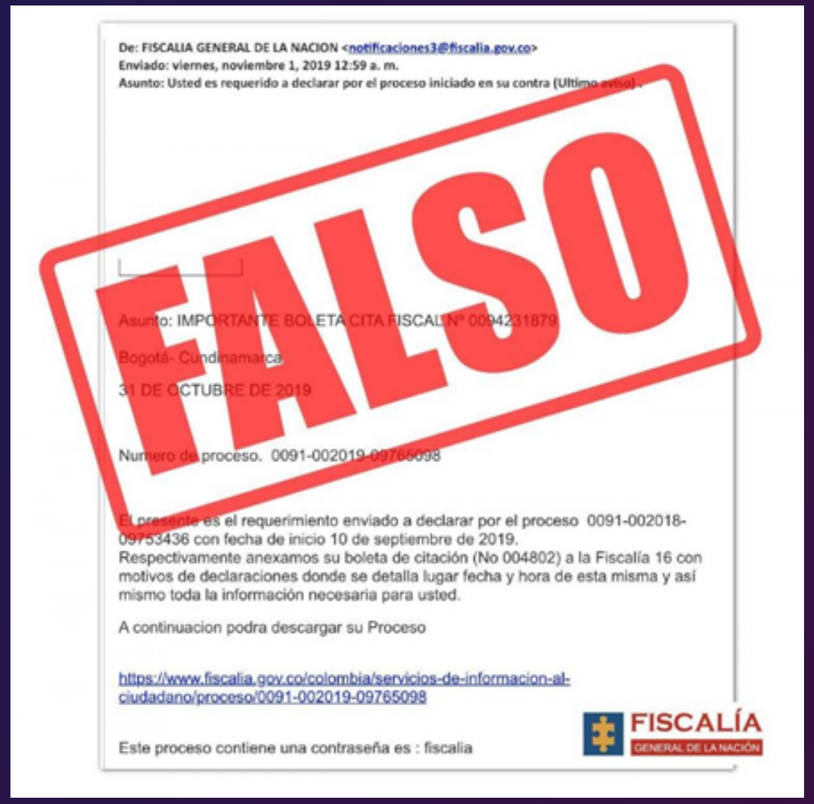
carrera 62 numero 12 41, 111811, bogota, Colombia

Usted puede darse de baja o cambiar sus datos de contacto en cualquier momento.

Powe

Geti

En el ejemplo de la imagen se aprecia un correo con archivos maliciosos que, al ser descargados, simulando ser un comparendo, roban información.



De: FISCALIA GENERAL DE LA NACION <notificaciones3@fiscalia.gov.co>
Enviado: viernes, noviembre 1, 2019 12:59 a. m.
Asunto: Usted es requerido a declarar por el proceso iniciado en su contra (Ultimo aviso) .

FALSO

Asunto: IMPORTANTE BOLETA CITA FISCALN° 0094231879

Bogotá- Cundinamarca

31 DE OCTUBRE DE 2019

Numero de proceso. 0091-002019-09765098

El presente es el requerimiento enviado a declarar por el proceso 0091-002018-09753436 con fecha de inicio 10 de septiembre de 2019.
Respectivamente anexamos su boleta de citación (No 004802) a la Fiscalía 16 con motivos de declaraciones donde se detalla lugar fecha y hora de esta misma y así mismo toda la información necesaria para usted.

A continuacion podra descargar su Proceso

https://www.fiscalia.gov.co/colombia/servicios-de-informacion-al-ciudadano/proceso/0091-002019-09765098

Este proceso contiene una contraseña es : fiscalia

FISCALÍA GENERAL DE LA NACIÓN

De la misma manera, la fiscalía general de la nación advierte que han detectado atacantes que simulan correos con citaciones para que los usuarios descarguen malware.

TIC

TALENTO TECH

Universidad Tecnológica de Pereira

faceIT

- **Redes inalámbricas gratuitas o abiertas:**

Este vector de ataque consiste en agentes malintencionados que crean o aprovechan redes abiertas que no piden contraseñas para conectarse. Generalmente aprovechan espacios como aeropuertos, cafeterías, centros comerciales y otros lugares concurridos. Lo que buscan es que usuarios se conecten a las redes abiertas y buscan vulnerabilidades en los equipos conectados. Por ejemplo, si un computador que permite a usuarios anónimos ver los archivos, se conecta a una red abierta, todos los archivos podrán ser leídos por cualquier persona en la misma red. Un atacante fácilmente puede robar información e incluso instalar programas a través de puertos y protocolos no seguros que permitan el acceso desde redes inalámbricas. En esencia, explotar vulnerabilidades por malas configuraciones de un dispositivo.

- **Medios extraíbles:**

Un vector de ataque son los medios portátiles que se pueden conectar a uno o a muchos computadores. Por ejemplo, CDs, memorias USB, celulares con cables USB, Tarjetas de memoria, entre otros. Un atacante que emplee estos medios suele cargar programas que se ejecutan en cuanto un computador detecte que hay un medio extraíble conectado. Al ejecutar tales programas se crean brechas de seguridad y los atacantes pueden robar información e instalar todo tipo de malware.Se han hallado casos en donde atacantes utilizan memorias con código malintencionado que se dejan en sitios públicos para que alguien las encuentre y las conecte. También a través de regalos gratuitos o incluso atacantes que logran entrar físicamente a donde hay computadores y conectan estas memorias con el fin de robar información.

- **Exploradores web:**

Un atacante puede emplear técnicas para confundir a los usuarios y que estos entren a sitios malintencionados. Desde allí se cambian las configuraciones de los exploradores para crear puntos de entrada de los atacantes. También hay sitios que regalan plugins o programas que aumentan las funciones de un explorador, comprometiendo la seguridad en la información. En la imagen se ve un sitio web malintencionado que simula haber hecho un análisis de virus en el computador e intenta engañar al usuario para que entre en un enlace que descarga malware. El engaño consiste en hacer creer que el malware es un programa que eliminará los supuestos virus detectados.

- **Servicios en la nube:**

Los servicios en la nube cuentan con muchas estrategias para interconectar los equipos en la nube, los datos y las soluciones que ofrecen. Generalmente las malas prácticas en la seguridad de las redes y los accesos en servicios de la nube ponen en alto riesgo los datos y comprometen tanto la información como la infraestructura. Por ejemplo, un atacante que logre entrar a un sistema de control de máquinas virtualizadas puede crear decenas o cientos de máquinas y conectarlas a una botnet para atacar. Los servicios en la nube cobran por la capacidad de cómputo instalada por el atacante generando grandes pérdidas económicas.

- Agentes internos:

Los empleados de las organizaciones pueden actuar como vectores de ciberataques, en ocasiones de forma intencional o en ocasiones con desconocimiento de que son un vector de riego en la seguridad de la información. Un empleado puede ser suplantado y robar información, también puede robar datos intencionalmente y causar daños.