Docente: ANA SILVIA MATEUS REINA	**Área**: Tecnología e informática	**Periodo:** I
Grado: NOVENO	**Sede:** LA ROSITA	**Fecha**: 01-02-2021
Estándar: Resuelvo problemas utilizando conocimientos tecnológicos y teniendo en cuenta algunas restricciones y condiciones.		

CRONOGRAMA DE ENTREGA DE ACTIVIDADES

ACTIVIDAD	FECHA MÁXIMA DE ENTREGA
1	15 al 19 de febrero de 2021
2	1 al 5 de marzo de 2021
3	15 al 19 de marzo de 2021
4	5 al 9 de abril de 2021
Finalización del I periodo 16 de abril de 2021	

TEMA 1. HACKERS

Conceptos previos

¿Qué comprendes por la palabra hacker?
Si tienes la posibilidad de ver este DOCUMENTAL sería fantástico.

https://youtu.be/AZCwMVgYGMI

HACKING

El primer eslabón de una sociedad "delictiva" según la prensa. Estos personajes son expertos en sistemas avanzados. En la actualidad se centran en los sistemas informáticos y de comunicaciones. Dominan la programación y la electrónica para lograr comprender sistemas tan complejos como la comunicación móvil. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Les encanta entrar en ordenadores remotos, con el fin de decir aquello de " he estado aquí " pero no modifican ni se llevan nada del ordenador atacado.

Normalmente son quienes alertan de un fallo en algún programa comercial, y lo comunican al fabricante. También es frecuente que un buen Hacker sea finalmente contratado por alguna importante empresa de seguridad.

El perfil del Hacker idóneo es aquel que se interesa por la tecnología, al margen de si lleva gafas, es delgado o lleva incansablemente encima un teléfono celular de grandes proporciones. Emplea muchas horas delante del ordenador, pero para nada debe ser un obsesivo de estas máquinas. No obstante, puede darse el caso. Este grupo es él más experto y menos ofensivo, ya que no pretenden serlo, a pesar de que poseen conocimientos de programación, lo que implica el conocimiento de la creación de Virus o Crack de un software o sistema informático.

CRACKERS

Es el siguiente eslabón y por tanto el primero de una familia rebelde. Cracker es aquel Hacker fascinado por su capacidad de romper sistemas y Software y que se dedica única y exclusivamente a Crackear sistemas.

Para los grandes fabricantes de sistemas y la prensa este grupo es el más rebelde de todos, ya que siempre encuentran el modo de romper una protección. Pero el problema no radica hay, si no en que esta rotura es difundida normalmente a través de la Red para conocimientos de otros, en esto comparten la idea y la filosofía de los Hackers. En la actualidad es habitual ver como se muestran los Cracks de la mayoría de Software de forma gratuita a través de Internet. El motivo de que estos Cracks formen parte de la red es por ser estos difundidos de forma impune por otro grupo que será detallado más adelante. Crack es sinónimo de rotura y por lo tanto cubre buena parte de la programación de Software y Hardware.

ACTIVIDAD 1 – HACKERS

Responder las siguientes preguntas:

1. ¿Qué es Hacker?
2. ¿Qué es Cracker?
3. Buscar la biografía de los siguientes personajes y realizar un resumen de cada uno mostrando aspectos importantes de lo que hicieron en aspectos del hacking en el cuaderno.
   a) Alan Turing
   b) Steven Wozniak
   c) Kevin Mitnick
   d) Kevin Poulson

TEMA 2. HACKING ETICO

UN POCO DE HISTORIA...

Hace algún tiempo, cuando algunas de las organizaciones apenas comenzaban a incrementar los procesos informatizados dentro de su sistema de información, sus propios administradores y analistas técnicos eran los encargados de buscar claras falencias o brechas de seguridad en el escenario para solucionarlas como podían. En ese entonces, la mayoría no tenía una noción madura acerca de la seguridad de la información o de las intrusiones de terceros no autorizados en sus sistemas. A medida que pasó el tiempo, estas organizaciones se multiplicaron de manera notable y se informatizaron aún más, incluso tomando a Internet como plataforma de sus movimientos de información. De ese modo, se hicieron fluidas las comunicaciones interpersonales, Inter sucursales, transacciones o flujo digital de todo tipo y nivel de importancia, dejando, al mismo tiempo, muchos más datos expuestos a terceros, como nunca antes había sucedido.

Hacking ético

Hacking ético es una forma de referirse al acto de una persona usar sus conocimientos de informática y seguridad para realizar pruebas en redes y encontrar vulnerabilidades, para luego reportarlas y que se tomen medidas, sin hacer daño.

La idea es tener el conocimiento de cuales elementos dentro de una red son vulnerables y corregirlo antes que ocurra hurto de información, por ejemplo.

Estas pruebas se llaman "pen tests" o "penetration tests" en inglés. En español se conocen como "pruebas de penetración", en donde se intenta de múltiples formas burlar la seguridad de la red para robar información sensitiva de una organización, para luego reportarlo a dicha organización y asi mejorar su seguridad.

Se sugiere a empresas que vayan a contratar los servicios de una empresa que ofrezca el servicio de hacking ético, que la misma sea certificada por entidades u organizaciones con un buen grado de reconocimiento a nivel mundial.

ACTIVIDAD 2 – HACKING ETICO

Responda las siguientes preguntas teniendo en cuenta los enlaces de las páginas web y el texto anterior.

1. ¿Qué es hacking ético?
2. Explique que son pruebas de penetración
3. ¿Cuáles son los tipos de hackers? Explique cada uno
4. ¿Es legal el hacking ético?
5. Realice un mapa mental o conceptual del hacking ético.

TEMA 3. VIRUS INFORMATICO

Un virus es un programa o secuencia de instrucciones que un computador es capaz de interpretar y ejecutar, todo virus ha de ser programado y realizado por expertos informáticos.

Su misión principal es introducirse, lo más discretamente posible en un sistema informático y permanecer en un estado de latencia hasta que se cumple la condición necesaria para activarse.

Las posibles vías de transmisión de los virus son: los discos, el cable de una red y el cable telefónico.

Lo primero que hace un virus típico, cuando se ejecuta el programa infectado, es situar su propio código en una parte de la memoria permaneciendo residente en ella. Todo lo que ocurra a partir de este momento depende

enteramente de la especie a la que pertenezca el virus en cuestión.

ESPECIES DE VIRUS

Caballos de Troya: Los caballos de troya no llegan a ser realmente virus porque no tienen la capacidad de autoreproducirse. Se esconden dentro del código de archivos ejecutables y no ejecutables pasando inadvertidos por los controles de muchos antivirus. Posee subrutinas que permitirán que se ejecute en el momento oportuno. Existen diferentes caballos de troya que se centrarán en distintos puntos de ataque. Su objetivo será el de robar las contraseñas que el usuario tenga en sus archivos o las contraseñas para el acceso a redes, incluyendo a Internet. Después de que el virus obtenga la contraseña que deseaba, la enviará por correo electrónico a la dirección que tenga registrada como la de la persona que lo envió a realizar esa tarea. Hoy en día se usan estos métodos para el robo de contraseñas para el acceso a Internet de usuarios hogareños. Un caballo de troya que infecta la red de una empresa representa un gran riesgo para la seguridad, ya que está facilitando enormemente el acceso de los intrusos. Muchos caballos de troya utilizados para espionaje industrial están programados para autodestruirse una vez que cumplan el objetivo para el que fueron programados, destruyendo toda la evidencia.

Camaleones: Son una variedad de similar a los Caballos de Troya, pero actúan como otros programas comerciales, en los que el usuario confía, mientras que en realidad están haciendo algún tipo de daño. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales). Un software camaleón podría, por ejemplo, emular un programa de acceso a sistemas remotos (rlogin, telnet) realizando todas las acciones que ellos realizan, pero como tarea adicional (y oculta a los usuarios) va almacenando en algún archivo los diferentes logins y passwords para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

Virus polimorfos o mutantes: Los virus polimorfos poseen la capacidad de encriptar el cuerpo del virus para que no pueda ser detectado fácilmente por un antivirus. Solo deja disponibles unas cuantas rutinas que se encargaran de desencriptar el virus para poder propagarse. Una vez desencriptado el virus intentará alojarse en algún archivo de la computadora. En este punto tenemos un virus que presenta otra forma distinta a la primera, su modo desencriptado, en el que puede infectar y hacer de las suyas libremente. Pero para que el virus presente su característica de cambio de formas debe poseer algunas rutinas especiales. Si mantuviera siempre su estructura, esté encriptado o no, cualquier antivirus podría reconocer ese patrón. Para eso incluye un generador de códigos al que se conoce como engine o motor de mutación. Este engine utiliza un generador numérico aleatorio que, combinado con un algoritmo matemático, modifica la firma del virus. Gracias a este engine de mutación el virus podrá crear una rutina de desencripción que será diferente cada vez que se ejecute.

Los métodos básicos de detección no pueden dar con este tipo de virus. Muchas veces para virus polimorfos particulares existen programas que se dedican especialmente a localizarlos y eliminarlos. Algunos softwares que se pueden baja gratuitamente de Internet se dedican solamente a erradicar los últimos virus que han aparecido y que también son los más peligrosos. No los fabrican empresas comerciales sino grupos de hackers que quieren protegerse de otros grupos opuestos. En este ambiente el presentar este tipo de soluciones es muchas veces una forma de demostrar quien es superior o quien domina mejor las técnicas de programación. Las últimas versiones de los programas antivirus ya cuentan con detectores de este tipo de virus.

FORMAS DE CONTAGIO

Existen dos grandes grupos de contaminaciones, los virus donde el usuario en un momento dado ejecuta o acepta de forma inadvertida la instalación del virus, o los gusanos donde el programa malicioso actúa replicándose a través de las redes.

Hay que tener en cuenta que Internet es una de las mayores fuentes de contagio, otra importante fuente de contagio son las BBS (Bulletin Board System, Bases de datos remotas de libre acceso).

Los virus funcionan, se reproducen y liberan sus cargas activas sólo cuando se ejecutan. Por eso, si un computador está simplemente conectado a una red informática infectada o se limita a cargar un programa infectado, no se infectará necesariamente. Normalmente, un usuario no ejecuta conscientemente un código informático potencialmente nocivo; sin embargo, los virus engañan frecuentemente al sistema operativo de

la computadora o al usuario informático para que ejecute el programa viral.

Algunos virus tienen la capacidad de adherirse a programas legítimos. Esta adhesión puede producirse cuando se crea, abre o modifica el programa legítimo. Cuando se ejecuta dicho programa, lo mismo ocurre con el virus. Los virus también pueden residir en las partes del disco duro o flexible que cargan y ejecutan el sistema operativo cuando se arranca el computador, por lo que dichos virus se ejecutan automáticamente. En las redes informáticas, algunos virus se ocultan en el software que permite al usuario conectarse al sistema.

FORMAS DE PREVENCIÓN Y ELIMINACIÓN DEL VIRUS

Copias de seguridad
Realice copias de seguridad de sus datos. Éstas pueden realizarlas en el soporte que desee, disquetes, unidades de cinta, etc. Mantenga esas copias en un lugar diferente del computador y protegido de campos magnéticos, calor, polvo y personas no autorizadas.

Copias de programas originales
No instale los programas desde los disquetes originales. Haga copia de los discos y utilícelos para realizar las instalaciones.

No acepte copias de origen dudoso
Evite utilizar copias de origen dudoso, la mayoría de las infecciones provocadas por virus se deben a discos de origen desconocido.

Utilice contraseñas
Ponga una clave de acceso a su computadora para que sólo usted pueda acceder a ella.

Anti-virus
Tenga siempre instalado un anti-virus en su computadora, como medida general analice todos los discos que desee instalar. Si detecta algún virus elimine la instalación lo antes posible.

Actualice periódicamente su anti-virus:
Un anti-virus que no está actualizado puede ser completamente inútil. Todos los anti-virus existentes en el mercado permanecen residentes en la computadora pata controlar todas las operaciones de ejecución y transferencia de archivos analizando cada archivo para determinar si tiene virus, mientras el usuario realiza otras tareas.

EFECTOS DE LOS VIRUS EN LAS COMPUTADORAS

Cualquier virus es perjudicial para un sistema. Como mínimo produce una reducción de la velocidad de proceso al ocupar parte de la memoria principal. Estos efectos se pueden diferenciar en destructivos y no destructivos.

Efectos no destructivos:

Emisión de mensajes en pantalla:

Es uno de los efectos más habituales de los virus. Simplemente causan la aparición de pequeños mensajes en la pantalla del sistema, en ocasiones se trata de mensajes humorísticos, de Copyright, etc. Ejemplo:

Soupy: “Get ready..” cause THERE´S A VIRUS IN YOUR SOUP!
Casino: “DISK DESTROYER. A SOUVENIR FROM MALTA”.

Borrado a cambio de la pantalla:

También es muy frecuente la visualización en pantalla de algún efecto generalmente para llamar la atención del usuario. Los efectos usualmente se producen en modo texto. En ocasiones la imagen se acompaña de efectos de sonido. Ejemplo:

Ambulance: Aparece una ambulancia moviéndose por la parte inferior de la pantalla al tiempo que suena una sirena.

Walker: Aparece un muñeco caminando de un lado a otro de la pantalla.

Efectos destructivos:

Desaparición de archivos:

Ciertos virus borran generalmente archivos con extensión exe y com, por ejemplo una variante del Jerusalem-B se dedica a borrar todos los archivos que se ejecutan.

Formateo de discos duros:

El efecto más destructivo de todos es el formateo del disco duro. Generalmente el formateo se realiza sobre los primeros sectores del disco duro que es donde se encuentra la información relativa a todo el resto del disco.

Los temas de protección de los sistemas operativos son preocupantes por los siguientes motivos:

El más evidente es la necesidad de prevenir la violación intencionada y maliciosa de una restricción de acceso, por parte de un usuario del sistema. Sin embargo, es de importancia más general la necesidad de asegurar que cada componente de un programa únicamente utiliza los recursos del mismo según los criterios que establezca el sistema operativo.
Para construir un sistema de protección se tiene que definir; por un lado, la estrategia de protección (de qué fallos hay que proteger al sistema) y por otro, los mecanismos de protección (cómo hacer que se consiga la protección definida por la estrategia).

¿QUÉ SON LOS ANTIVIRUS?

Los programas antivirus son una herramienta específica para combatir el problema virus, pero es muy importante saber cómo funcionan y conocer bien sus limitaciones para obtener eficiencia en el combate contra los virus.

Cuando se piensa en comprar un antivirus, no debe perderse de vista que, como todo programa, para funcionar correctamente, debe está bien configurado. Además, un antivirus es una solución para minimizar los riesgos y nunca será una solución definitiva, lo principal es mantenerlo actualizado.

La única forma de mantener su sistema seguro es mantener su antivirus actualizado y estar constantemente leyendo sobre los virus y las nuevas tecnologías. La función de un programa antivirus es detectar, de alguna manera, la presencia o el accionar de un virus informático en una computadora. Éste es el aspecto más importante de un antivirus, pero, las empresas deben buscar identificar también las características administrativas que el antivirus ofrece. La instalación y administración de un antivirus en una red es una función muy compleja si el producto no lo hace automáticamente. Es importante tener en claro la diferencia entre "detectar" e "identificar" un virus en una computadora. La detección es la determinación de la presencia de un virus, la identificación es la determinación de qué virus es. Aunque parezca contradictorio, lo mejor que debe tener un antivirus es su capacidad de detección, pues las capacidades de identificación están expuestas a muchos errores y sólo funcionan con virus conocidos.

ACTIVIDAD 3 – VIRUS INFORMATICO

Lee atentamente el texto anterior y contestar los siguientes puntos EN EL CUADERNO

1. Haga una lista de palabras desconocidas.
2. Escriba una definición de virus (REDACTE con sus propias palabras)
3. ¿Quienes crean los virus y para qué? Explique
4. ¿Cómo funcionan los virus?
5. ¿Cuáles son las especies de virus? Explique cada uno.
6. Mencione otras clases de virus conocidos.
7. Explique las formas de contagiarse con virus.
8. Escriba otras formas de contagio de virus que usted conozca.
9. Escriba las formas de prevención y eliminación de los virus. Explique cada uno.
10. ¿Qué son los antivirus? Explique.
11. En una hoja (pagina) haga una representación gráfica sobre los virus y antivirus, o cómo prevenir los virus.
12. Haga una breve conclusión sobre el tema (15 renglones).

TEMA 4. EN TIC CONFÍO

En TIC confío es la estrategia de promoción de uso seguro y responsable de las TIC del Plan El Futuro Digital es de Todos, del Ministerio de las Tecnologías de la Información y las Comunicaciones de Colombia. La estrategia busca ayudar a la sociedad a desenvolverse e interactuar responsablemente con las TIC, al tiempo que promueve la cero tolerancia con el material de explotación sexual de niñas, niños y adolescentes y la convivencia digital.

En TIC confío ofrece a la ciudadanía herramientas para enfrentar con seguridad riesgos asociados al uso de las TIC, como el grooming, el sexting, el ciberacoso, la ciberdependencia y el material de explotación sexual de niñas, niños y adolescentes. Adicionalmente, promueve buenas prácticas de uso seguro y responsable de Internet a través de contenidos relacionados con consejos de ciberseguridad e identificación de noticias falsas.

Dentro de sus iniciativas, En TIC confío realiza una Charla lúdica, gratuita, de 60 minutos de duración, con enfoque de género, la cual es realizada por los embajadores en todos los departamentos del país. La población objetivo del programa es la ciudadanía en general, especialmente los niñas, niños y adolescentes a partir de los 12 años, padres, madres y cuidadores.

En TIC confío cuenta con diversos canales digitales, que incluyen un sitio web y la presencia en las principales redes sociales, los cuales se actualizan semanalmente con contenidos dirigidos a niñas, niños, adolescentes, padres de familia, educadores y público en general. La estrategia incluye artículos, imágenes y videos que ilustran los riesgos que enfrentamos al usar las TIC, al tiempo que ofrece consejos e información sobre sus usos responsables y creativos.

ARTICULO 1. SEXTORSIÓN

te protejo

Al usar del canal de denuncia virtual te Protejo, el usuario diligencia un formulario anónimamente y activa la ruta de atención con la Policía Nacional.

Denuncie al acosador: las redes sociales ofrecen canales de denuncia que permiten dar de baja la cuenta del extorsionador y evitar que siga distribuyendo el contenido. En Colombia puede usar Te Protejo (www.teprotejo.org).

Informar y denunciar al Centro Cibernético Policial que cuenta con el CAI virtual, la primera iniciativa de atención policial en línea en Iberoamérica, que permite reportar delitos informáticos y hurtos de dispositivos móviles

No elimine ningún correo, chat o demás información en que tenga alguna evidencia de amenaza o extorsión. Es importante contar con este registro para la denuncia.

TIPS

PARA EVITAR EL ACCESO ABUSIVO A SUS PERFILES

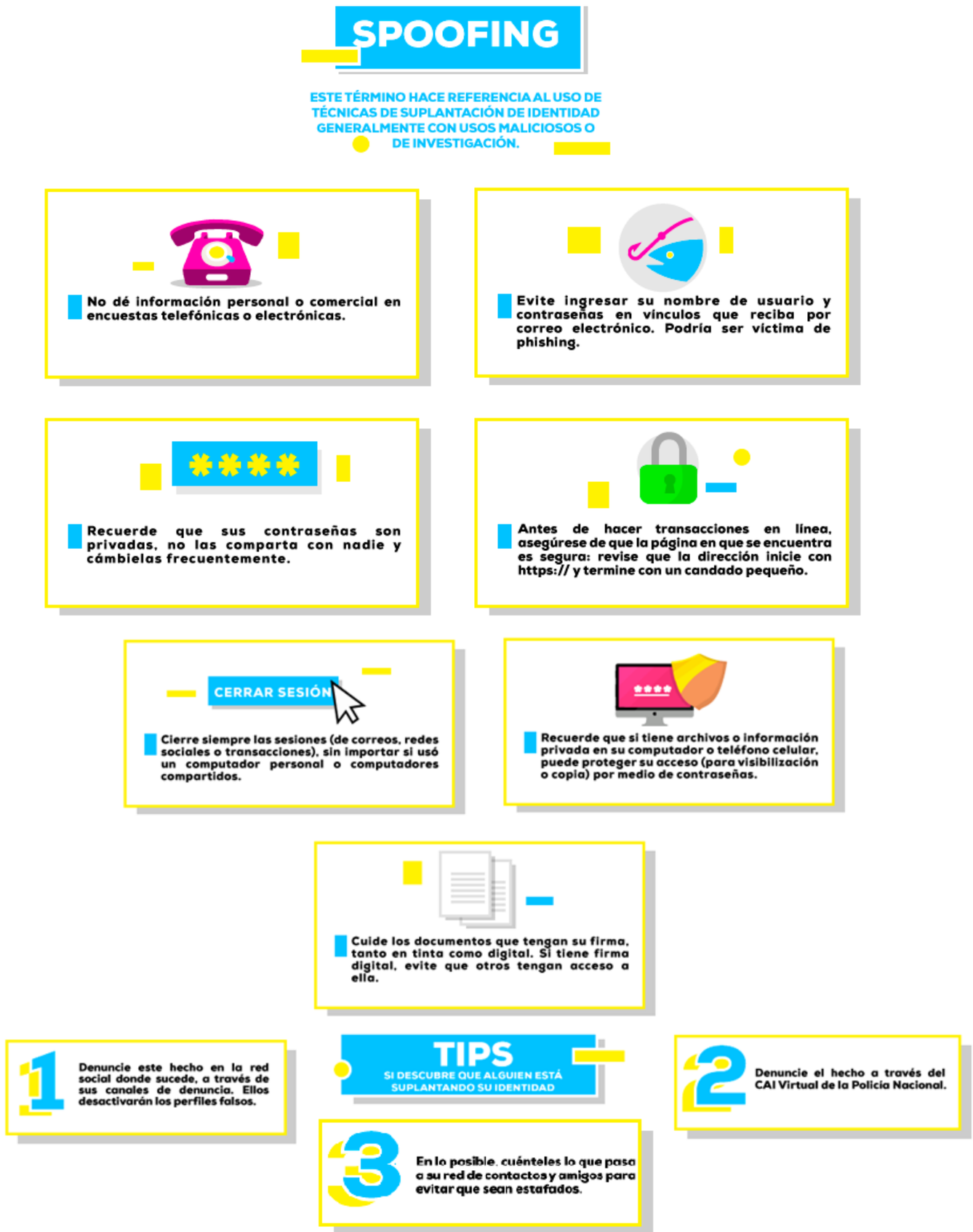
1. Nunca comparta imágenes compremetedoras con ninguna persona, no importa el nivel de confianza que tenga con ella.

2. Si alguien le pide fotografías o videos en situaciones compromtetedoras, simplemente diga no.

3. Coméntelo a personas de toda confianza y cercanía. Si se trata de un menor de edad, acuda a sus padres y autoridades escolares.

4. Sin dudarlo: denuncie al agresor ante las autoridades. Puede hacerlo de forma anónima en internet, a través de TeProtejo (www.teprotejo.org) y del CAI Virtual de la Policía Nacional

ARTICULO 2. SUPLANTACIÓN DE IDENTIDAD DIGITAL



ACTIVIDAD 4 – EN TIC CONFIO

1. Si tienes la posibilidad ingresa a la pagina https://www.enticconfio.gov.co/poder-digital
2. Selecciona un articulo de la pagina web anterior o de la expuesta en esta guía.
3. Realiza un video exponiendo el tema seleccionado.
4. Enviar el video por mensaje interno por WhatsApp.