



Delitos informáticos en ECUADOR

Departamento de Seguridad de las TIC -
DNTIC

AGENDA



01 Intro.

Como se ha venido generando el delito en el Ecuador.

02 Tipos de delito

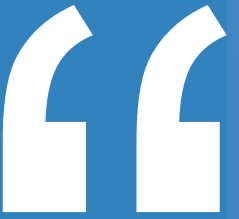
03 Como opera la delincuencia

Modus operandi..

04 Conclusiones y recomendaciones

A man with a beard and glasses, wearing a dark suit and tie, is seated at a table. He is looking down at a smartphone in his hands. A clear glass mug is on the table in front of him. The background is a solid blue color.

INTRODUCCIÓN



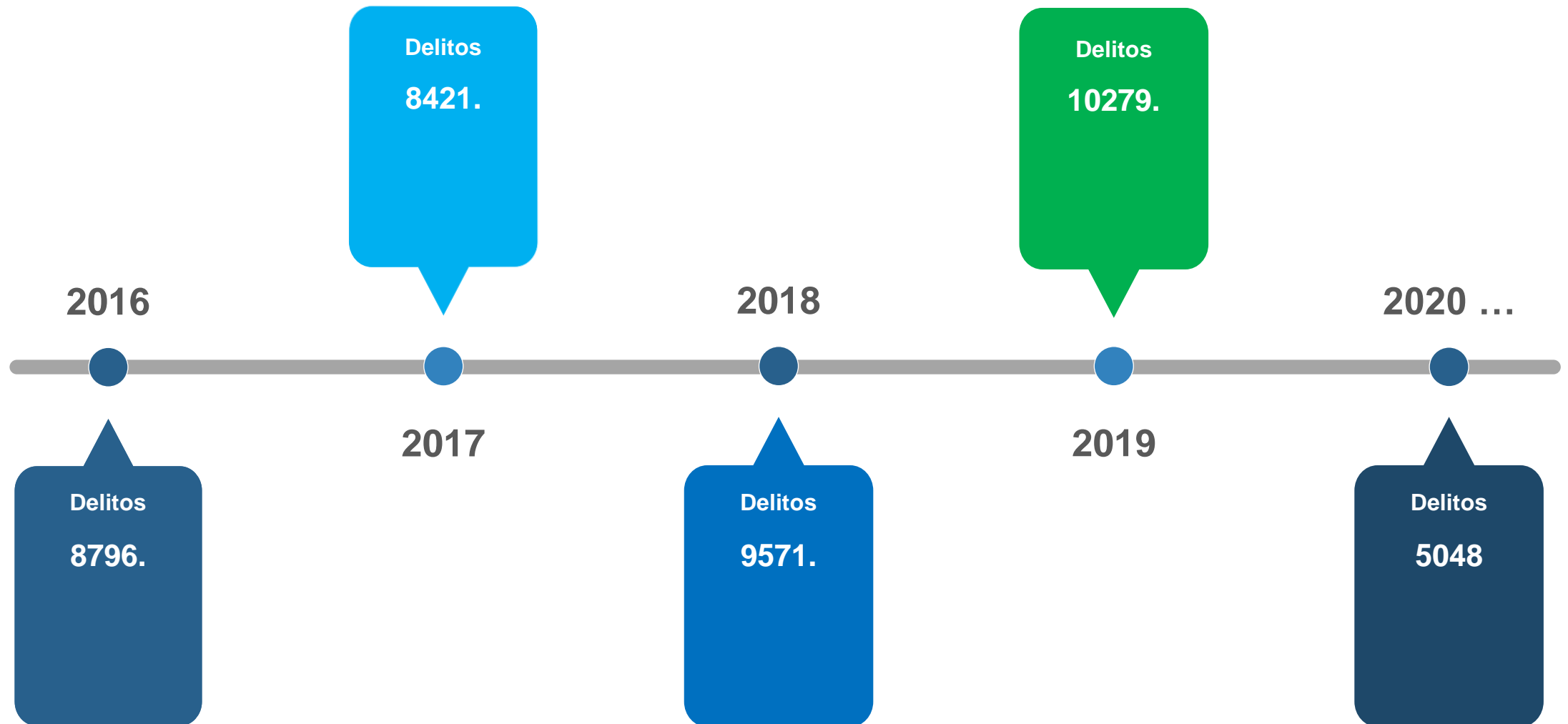
Los delitos informáticos van en aumento en Ecuador.

Según las denuncias presentadas en la Fiscalía, desde antes de la pandemia del COVID-19. En el 2017 se registraron 8421 casos; subieron a 9571 y 10 279 en 2018 y 2019. La tendencia se mantiene. Los más frecuentes son las estafas digitales con modalidades como la **suplantación de la identidad** y la **apropiación fraudulenta** a través de medios electrónicos. La primera implica la creación de **perfiles falsos de las personas** que están en las redes sociales con el fin de pedir dinero a sus contactos. La segunda **es comprar o hacer transferencias económicas sin la autorización del titular** de la tarjeta o de la cuenta. Y la tercera son **llamadas para vender bienes o servicios** ganan espacio en medio de la crisis y causan malestar entre consumidores

Los ciberdelincuentes están al acecho de los rastros que se dejan al usar aplicaciones móviles, correos, perfiles y chats de redes sociales, al hacer los pagos virtuales o transferencias electrónicas. Todo es sujeto a ser hackeado para dar mal uso a los datos.

DELITOS INFORMÁTICOS

Delitos Informáticos en el Ecuador

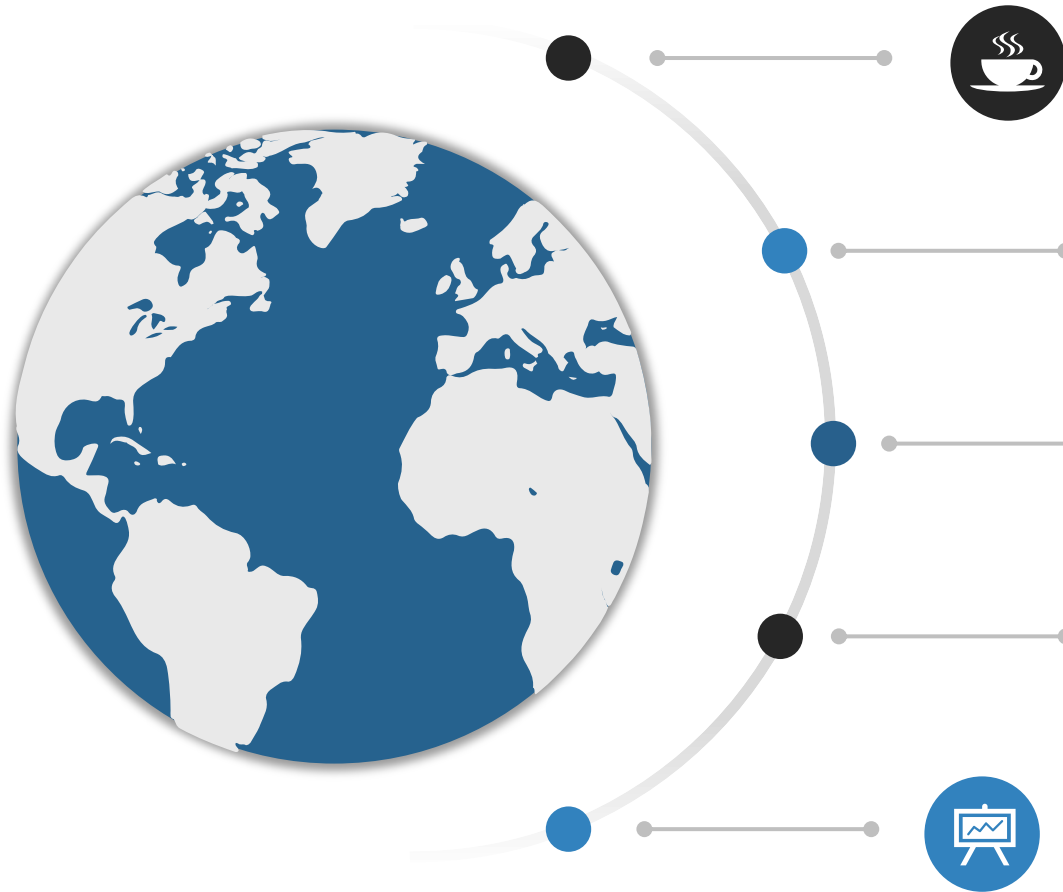


Tipos de delitos



Fuente: Fiscalía General del Estado.

Como opera la ciberdelincuencia?



Referencias básicas:

- El bajo costo para poder cometer el acto lesivo es lo que le da la popularidad a esta clase de delincuencia.
- Lo único que se necesita es tener el conocimiento, un computador con especificaciones técnicas claras y tener acceso a la web.
- Absolutamente todo dispositivo conectado a internet es **hackeable**.

Hackers:

Hackers que solo atrapan y descargan la información que captan en internet para vendérsela al mejor postor.

Otros ciberdelincuentes:

Apropiación fraudulenta a través de medios electrónicos o las estafas.

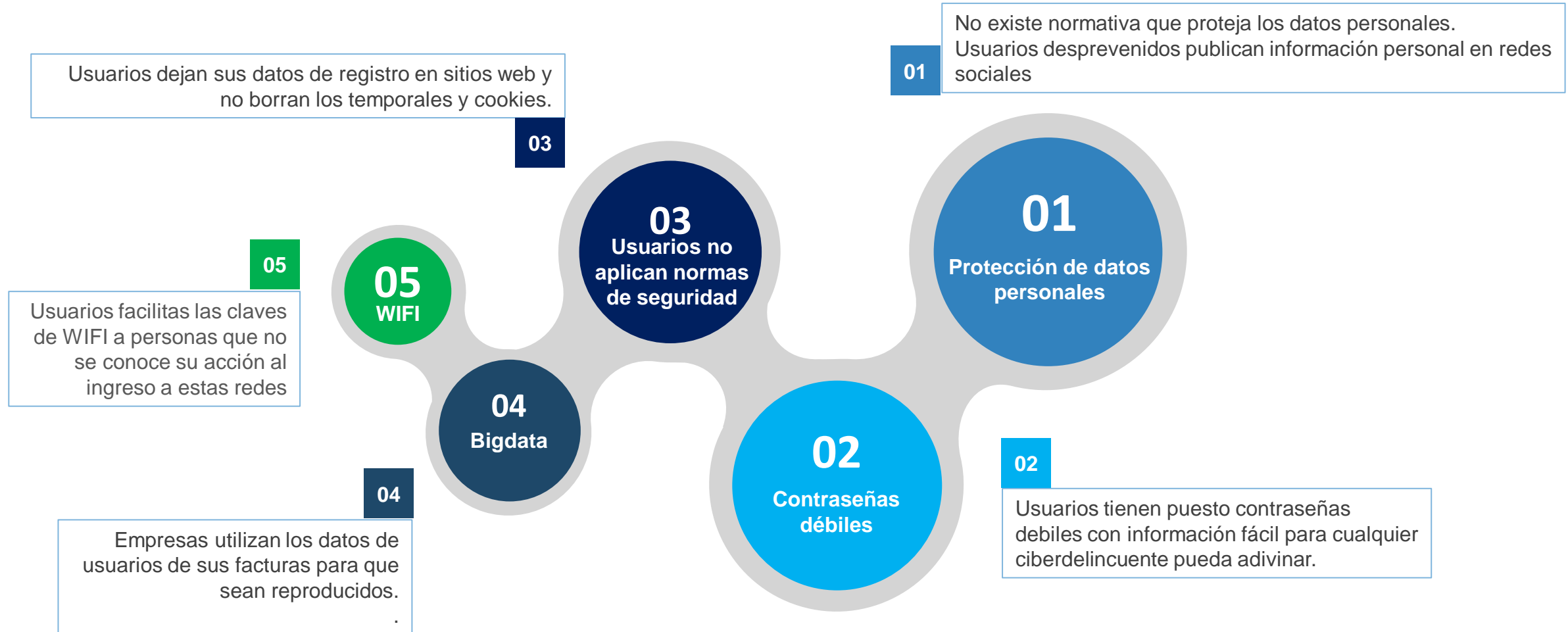
A través de dispositivos electrónicos:

Ingreso a un dispositivo móvil, laptop o computador sin el consentimiento del dueño de esa información. Lo que se facilita, por ejemplo, al entregar la clave del WIFI de una red doméstica a visitantes o conocidos de quienes se desconoce sus intenciones

Servicios:

Llamadas para vender servicios o bienes.
Ofertas en redes sociales y correos electrónicos de servicios a domicilio
Educación Online

Conclusiones:



Recomendaciones de Seguridad:

-  **Llamadas y mensajes:**
No se debe contestar ningún número o mail cuyo remitente es desconocido, ni ningún mensaje en el que no se identifique el número.
-  **Usar correos institucionales y no los gratuitos**
Los padres pueden exigir que los mails tengan la terminación del nombre del colegio y que no se usen las versiones gratuitas. Los hackers cuando ven que el correo pertenece a una organización, pues asumen que hay más monitoreo
-  **Leer las políticas de seguridad.**
Leer las políticas de seguridad y privacidad de las aplicaciones y de los sitios web
No dejar abiertas las sesiones de internet en los cibercafé
Borrar los temporales cada que usen el internet.
-  **Contraseñas mas fuertes**
Crear contraseñas mas seguras es decir que tengan números letras y simbolos. Y que la contraseña tenga como mínimo 8 caracteres.
Cambian cada cierto tiempo.
-  **Antivirus y antimalware**
Instalar y mantener actualizado el antivirus y antimalware en sus computadores personales.



MUCHAS GRACIAS