Guardia Civil

GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR

¿Delito Informático?

Podríamos definir **delito informático o ciberdelito** a todo ilícito penal llevado a cabo a través de medios telemáticos y que está íntimamente ligado a los bienes jurídicos relacionados con las tecnologías de la información o que tiene como fin estos bienes.

Tomando como referencia el convenio de Ciberdelincuencia del Consejo de Europa: **Los actos dirigidos contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos.**

Características principales

- Son delitos difíciles de demostrar ya que, en muchos casos, es complicado encontrar las pruebas.
- Son actos que pueden llevarse a cabo de forma rápida y sencilla. En ocasiones estos delitos pueden cometerse en cuestión de segundos, utilizando sólo un equipo informático y sin estar presente físicamente en el lugar de los hechos.
- Los delitos informáticos tienden a proliferar y evolucionar, lo que complica aún más la identificación y persecución de los mismos.

Delitos informáticos:

1) Delitos en los que el objeto de la actividad delictiva son los propios sistemas informáticos o las TICs.

-Delitos de **daños, sabotaje informático y ataques de denegación de servicios** previstos y penados en el artículo 264 y concordantes del Código Penal.

-Delitos de **acceso sin autorización a datos, programas o sistemas informáticos** previstos y penados en el artículo 197.3 del Código Penal.

-Delitos de **descubrimiento y revelación de secretos** del artículo 197 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos electrónicos o telemáticos.

-Delitos de **descubrimiento y revelación de secretos de empresa** previstos y penados en el artículo 278 del Código Penal cometidos a través de las TICs o cuyo objeto sean datos que se hallen registrados en ficheros o soportes informáticos ó electrónicos.

-Delitos **contra los servicios de radiodifusión e interactivos** previstos y penados en el artículo 286 del Código Penal.

Delitos informáticos:

2) Delitos en los que la actividad criminal se sirve para su ejecución de las ventajas que ofrecen las TICs.

-Delitos de **estafa** previstos y penados en el artículo 248.2 a) b) y c) del Código Penal, siempre que, en los supuestos a) y c) **se utilicen las TICs** para llevar a efecto la transferencia u operación de cualquier tipo en perjuicio de otro.

-Delitos **contra la propiedad intelectual** de los artículos 270 y ss del Código Penal cuando se cometan utilizando las TICs.

Delitos informáticos:

3) Delitos en los que la actividad criminal, además de servirse para su ejecución de las ventajas que ofrecen las TICs, entraña <u>especial complejidad en su investigación</u> que demanda conocimientos específicos en la materia.

-Delitos de **falsificación documental** de los artículos 390 y ss del Código Penal cuando para la ejecución del delito se hubieran empleado las **TICs** siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad técnica en la investigación criminal.

-Delitos de **injurias y calumnias** contra funcionario público, autoridad o agente de la misma previstos y penados en los artículos 211 y ss del Código Penal cometidos a través de las **TICs** siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

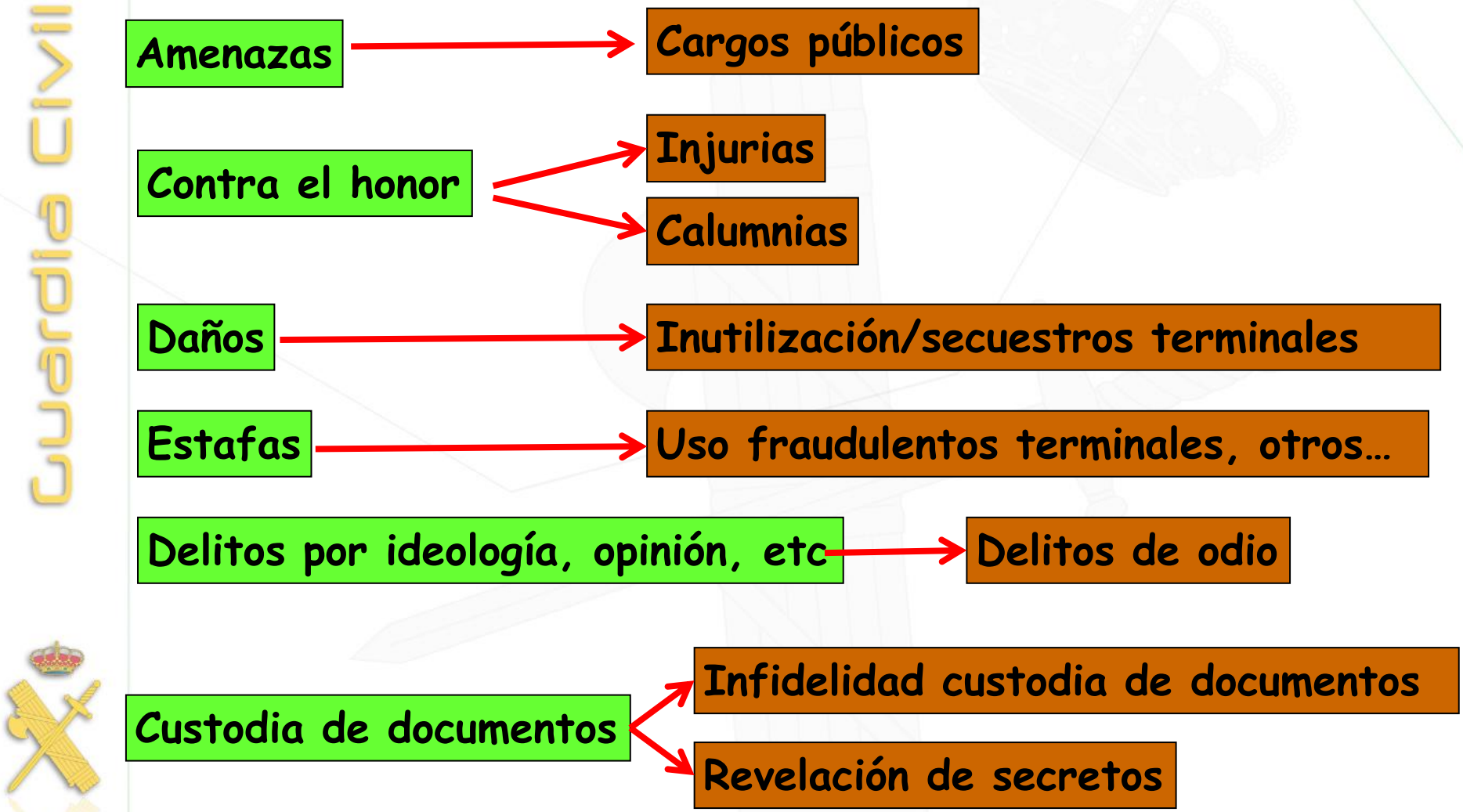
-Delitos de **amenazas y coacciones** previstos y penados en los artículos 169 y ss del Código Penal cometidos a través de las **TICs** siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos **contra la integridad moral** previstos y penados en el artículo 173.1 del Código Penal cometidos a través de las **TICs** siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-Delitos de **apología o incitación a la discriminación, el odio y la violencia o de negación o justificación de los delitos de genocidio** previstos y penados en los artículos 510 y 607.2 del Código Penal cometidos a través de las **TICs** siempre que dicha circunstancia fuera determinante en la actividad delictiva y generara especial complejidad en la investigación criminal.

-**Cualquier otro tipo delictivo en cuya ejecución haya sido determinante la utilización de las TICs** y en los que dicha circunstancia genere una especial complejidad en inves.crim.

Nos pueden afectar:



Denunciar, ¿Donde?

- Juzgado
- Cuerpo Nacional de Policía
- Guardia Civil

Denuncia

Consejos iniciales al observar el ilícito:

1- **GUARDAR** toda la información posible.
NO borrar, destruir, o modificar la información que poseemos relacionada con el delito. La integridad de la información es vital para poder seguir adelante con las causas penales que se inicien.

2- **NO** reenviar los mensajes o correos electrónicos constitutivos del delito.

3- **NO** borrar perfiles, ni cuentas hasta haber presentado la denuncia. Pero mantenerlos inactivos.

¿Qué aportar en la denuncia?

- **Toda la documentación que tenga sobre los hechos, aunque le pueda parecer irrelevante.**
- **Realizar copia en soporte digital con los datos aportados (e-mail, fotografías, capturas de pantalla, etc.). O facilitar impresiones en papel**
- **Mostar el soporte original, en los caso que sea posible.**
- **De los correos electrónicos, aportar las cabeceras del mismo. Si no se saben extraer, el especialista policial lo realizará.**

¿Qué aportar en la denuncia?

- **En caso de tratarse de mensajes en teléfonos móviles, facilitar el texto completo o capturas de pantalla. MEJOR FACILITAR EL TERMINAL.**
- **Metadatos asociados al archivo (fotografías, documentos ofimáticos,…).**
- **El agente policial sabrá qué requerir en cada caso.**

eGarante, testigo “on-line”

eG Web

eGarante te proporciona una prueba del contenido de una web o de una red social en un momento determinado.
Certificamos:

La url a la que accedemos.
El contenido realizando una captura de pantalla que incluye los enlaces existentes en la página
La fecha y hora a la cual accedimos a la página.
Informamos del hecho de que lo hacemos desde unos servidores no manipulables por el interesado

La Sala de lo penal del Tribunal Supremo ha dictado una sentencia de fecha 19 de mayo de 2015 (sentencia número 300/2015, ponente señor Marchena Gómez), por la que fija los criterios para aceptar la fuerza probatoria de las capturas de pantalla o "pantallazos", en los que se refleja el contenido de mensajes transmitidos en las redes sociales.

eGarante, testigo “on-line”

http://www.testaferro.es

Digitally signed by
EGARANTE, S.L.
Date: 2014.12.05
09:53:28 CET

Guardia Civil

¿Cómo se investiga un ciberdelito?

1.- Identificar el delito.

2.- Acotar la escena.

3.- Recopilar evidencias.

4.- Preservar las pruebas.

5.- Analizar las evidencias.

6.- Instrucción diligencias/Informes.

7.- Ratificación/Defensa informe en el Juicio.

Finalidad de la investigación

- Determinar los **datos de Tráfico** y rastros de navegación.

- Determinar el lugar de comisión de los hechos, la **máquina de origen**, los **autores** de la conducta y el tipo de conducta punible que se ha perpetrado.

- A partir de los datos obtenidos puede llegarse a:
  - **Vincular** el equipo con un usuario CONCRETO (entrada y registro).
  - **Registro** e incautación DE EVIDENCIAS
  - **Volcado** de datos de dispositivos.
  - **Análisis** del sistema y soportes intervenidos.
  - Informe policial incriminatorio. **Pericial** informática.
  - Investigación tradicional.

INVESTIGACION DE LA CRIMINALIDAD INFORMATICA

- FASE INICIAL. Denuncia
- FASE DE INVESTIGACIÓN.
  - Presencia en la red."Posteos" en webs y foros
  - Programas rastreadores
  - Copia de contenidos dinámicos
  - Intervención teléfono o correo electrónico
  - Contactos email
  - Contactos Mensajería instantánea
  - Búsquedas selectivas en programas P2P
  - Trabajo sobre los DATOS DE TRÁFICO, en especial IP,s.
  - NO HAY INVESTIGACIÓN TECNOLÓGICA POSIBLE SIN *DATOS DE TRÁFICO*

Investigación

NO HAY INVESTIGACIÓN TECNOLÓGICA POSIBLE SIN *DATOS DE TRÁFICO*

- "Datos de tráfico" son los relativos a una comunicación por medio de un sistema informático y generados como elemento de la cadena de comunicación que indican el ORIGEN, DESTINO, RUTA, HORA, FECHA TAMAÑO Y DURACIÓN DE LA COMUNICACIÓN

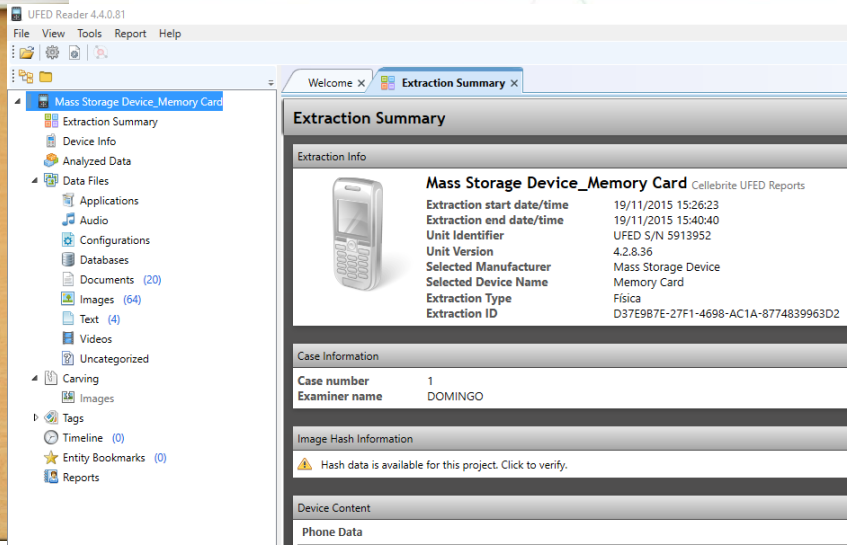
¿ DONDE ESTAN ESOS DATOS?

SERVIDORES DE LOS ISP(Logs)

CABECERAS TÉCNICAS DE CORREOS-E

- REGISTRO DE ACTIVIDAD DE LOS PROGRAMAS

Investigación



CENTRO MUNICIPAL INFORMÁTICA (C.E.M.I.) DEL EXCMO. AYTO. DE MADRID

Plaza de la Villa nº 1, (28005) MADRID

RANGO I.P.	FECHA:	HORA ESPAÑOLA (GMT + 1)
195.55.79.22	22-12-2008	18:12
195.55.79.22	23-12-2008	18:06

Entrada: **191396**
Usuario: **FRANCISCO XXXXXXX**
Departamento: **munimadrid.es\xxxxx**
Destino: **www.foroswebgratis.com**
URL:http://www.foroswebgratis.com/foro-ValidaUsuario.php?id_foro=105406&Mail= **ruperto@terra.es**&Password=

Dificultades en la investigación

- **La tecnología** facilita la perpetración de nuevas conductas dañosas y la ocultación de los rastros de las mismas.
- La **tipificación** de las conductas resulta complicada.
- **Escasa formación** en el mundo judicial sobre la mayoría de aspectos relacionados con las nuevas tecnologías de la información y las comunicaciones.
- **Falta de medios** tanto personales como materiales.
- **El enmascaramiento del autor**, difuminando su rastro electrónico.
- **La extraterritorialidad**, lo que conlleva problemas de jurisdicción, de operatividad policial y judicial, de determinación de la ley y del procedimiento aplicable.
- **Falta de colaboración** entre los Estados.

Factor humano

Cuanto más sofisticadas son las tecnologías empleadas para proteger la información, los ataques se van a centrar más en explotar las debilidades de la persona.

Muchas gracias

por su atención

Comandancia de la Guardia Civil de Burgos
Unidad Orgánica Policía Judicial
Equipo de Investigación Tecnológica (EDITE)
Avenida Cantabria nº 93, Burgos
bu-cmd-burgos-pj-edite@guardiacivil.org
Teléfono: **947.24.41.44**, ext. **481** y **447**