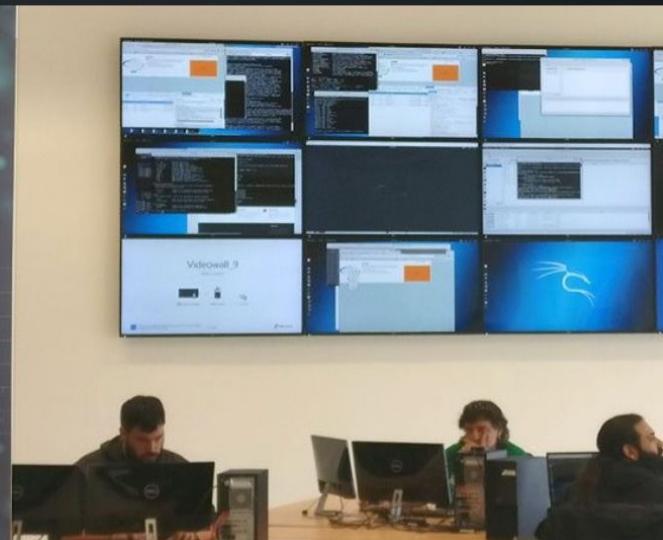


[Home](#) | [White Paper on Cybersecurity](#) | [Basque Digital Innovation Hub](#) | [About BCSC](#)



Basque Cybersecurity Centre

Nombre del Equipo/Capacidad

Basque Cybersecurity Centre

Siglas

BCSC

Logotipo



Organización a la que pertenece

Agencia de Desarrollo Empresarial del Gobierno Vasco (SPRI)

Año de creación:

2017

Ámbito de Actuación:

Euskadi

Dirección web:

www.basquecybersecurity.eus

Email de contacto para propósitos generales de la organización. No utilizar para reportar incidentes.

Email de contacto para otros equipos de respuesta a incidentes. No utilizar para reportar incidentes.

Correo electrónico:

y Emails para reportar incidentes de ciberseguridad.

Email de contacto para solicita de información general.

Twitter

Redes sociales:

LinkedIn



Estás en: Comisarías

- >> Consejera
- >> Ertzaintza. La policía de Euskadi
- >> Comisarías
- >> Servicios en la web
- >> Programas de calidad
- >> Ekinbide - iniciativas de mejora
- >> Derechos sobre Protección de Datos
- >> Delincuencia Terrorista
- >> Estadísticas delictivas
- >> Servicio de prensa
- >> Consejos de seguridad
- >> Empresas
- >> Proyectos normativos
- >> Entidades de participación
- >> PGSPE 2020

Línea directa confidencial
Antiterrorismo
900 840 843

Denuncias por Internet

SOS DEIAK

TRAFIKOA **011**

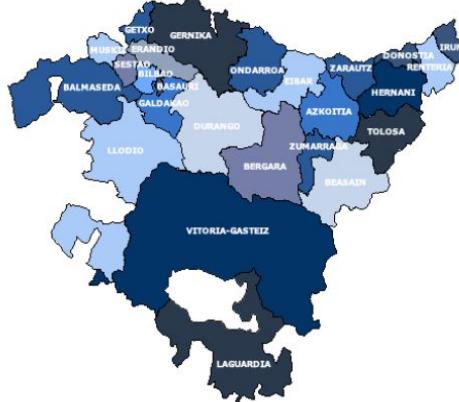
Udalzaingoa

WAI-A
WCAG 1.0

Comisarías

Las comisarías de la Ertzaintza abarcan la totalidad del territorio de la Comunidad Autónoma Vasca.

Seleccione una comisaría para obtener información más detallada.



>> Información legal

© 2019 - Eusko Jaurlaritza - Gobierno Vasco

Euskadi, auzolana, bien común



Estás en: Servicios en la web / Prevención frente a la delincuencia informática / ¿Qué es el delito informático?

- » Consejera
- » Ertzaintza. La policía de Euskadi
- » Comisarías
- » Servicios en la web
- » Programas de calidad
- » Ekintza - iniciativas de mejora
- » Derechos sobre Protección de Datos
- » Delincuencia Terrorista
- » Estadísticas delictivas
- » Servicio de prensa
- » Consejos de seguridad
- » Empresas
- » Proyectos normativos
- » Entidades de participación
- » PGSPE 2020

Línea directa confidencial
Antiterrorismo
900.840.843

Denuncias
por Internet

SOS DEIAK

TRAFIKOA 011

Udalzaingoa

WAI-A
WCAG 1.0

¿Qué es el delito informático?

El "delito informático", "ciberdelito", "delitos telemáticos"... bajo varias denominaciones se pueden encuadrar los hechos que de alguna forma tienen dos componentes básicos: existencia de delito y uso de la informática.

Vamos a definir por lo tanto el delito informático como el acto delictivo en el que se hace uso de la informática para su comisión, bien sea como medio o como fin del mismo.

En todo caso, los actos delictivos que comúnmente vamos a calificar como "delitos informáticos" deben estar tipificados en el código penal, donde veremos que no existe ningún título o capítulo dedicado específicamente a ellos, sino que cada acto estará encuadrado en el título dedicado al bien jurídico que se pretende proteger.

Así, vemos que existen delitos que pueden cometerse mediante el uso de la informática en los siguientes apartados del código penal:

- Amenazas
- Acoso sexual
- Exhibicionismo y provocación sexual
- Prostitución y corrupción de menores
- Descubrimiento y revelación de secretos
- Calumnias
- Injurias
- Robos
- Extorsión
- Estafas
- Defraudaciones de fluido eléctrico y análogas
- Daños
- Propiedad intelectual
- Mercado y consumidores
- Falsedades
- Falsificación de moneda y efectos timbrados
- Derechos fundamentales y libertades públicas garantizadas por la Constitución
- Faltas contra el patrimonio





Estás en: Servicios en la web / Prevención frente a la delincuencia informática / Consejos

- >> Consejera
- >> Ertzaintza. La policía de Euskadi
- >> Comisarías
- >> Servicios en la web
- >> Programas de calidad
- >> Ekinbide - iniciativas de mejora
- >> Derechos sobre Protección de Datos
- >> Delincuencia Terrorista
- >> Estadísticas delictivas
- >> Servicio de prensa
- >> Consejos de seguridad
- >> Empresas
- >> Proyectos normativos
- >> Entidades de participación
- >> PGSPE 2020

Línea directa confidencial
Antiterrorismo
900 840 843

Denuncias por Internet

Atención de emergencias

TRAFIKOA 011

Udalzaingoa

WAI-A
WCAG 1.0

Consejos

• NIÑOS

Como bien sabes chatear consiste en comunicarse con otras personas a través del ordenador (generalmente). Como la mayoría de las veces no ves a la persona con la que te estás comunicando, no puedes saber de una forma segura quién es el que está al otro lado de la linea. Es decir, que es posible que creas que estas chateando con un niñ@ de 12 años y en realidad sea un hombre de 45 años.

Debido a esta falta de identificación has de tener en cuenta una serie de consejos prácticos para evitar que puedas ser víctima de algún delito.

- No digas tu nombre verdadero
 - No digas tu número de teléfono
 - No digas tu dirección
 - No des datos de tus padres o hermanos
 - No quedes nunca solo con alguien que has conocido a través de internet. Si conciertas alguna cita, vete en compañía de tus padres.
 - Si observas algún contenido no apropiado para tu edad ponlo en conocimiento de tus padres.
 - No instales programas "piratas", podrían contener virus dañinos para tu ordenador.
 - No instales ningún programa que ofrezca la posibilidad de ver fotos o videos GRATIS.
- Generalmente detrás de esos programas existe una conexión telefónica a un número 906, con un coste elevado.

• PADRES

- Es conveniente que la navegación de los niños sea guiada, o supervisada por los progenitores, dependiendo de su edad.
- Existe la posibilidad de instalar programas que actúan de filtro de contenidos entre internet y el usuario, bloqueando aquellos contenidos que se determinen, pero ninguno de ellos pueden ser sustituidos por una adecuada educación a los menores.
- Solicitar a su compañía telefónica la restricción de acceso a líneas 903, 906, o instalación de algún programa que impida esas conexiones, para evitar el funcionamiento de los "dialers 906".

• COMPRAS

- Existe un principio básico: NADIE DA EUROS A 90 CÉNTIMOS (actualización de nadie da duros a cuatro pesetas).
- Si un objeto es demasiado barato, es conveniente sospechar de su autenticidad. Comprar por internet puede ser más barato, ya que se reducen gastos de distribución, almacenaje, intermediarios, etc. Pero hay que desconfiar de precios ridículos.
- Confirmar la identidad del vendedor antes de hacer la compra..

• SEGURIDAD INFORMÁTICA

- Instalación de un cortafuegos. Un cortafuegos es un dispositivo físico o un programa, que actúa de barrera entre un ordenador y una red, en este caso Internet. Existen diversos productos comerciales, así como también gratuitos para uso personal con una aceptable seguridad.
 - Instalación de un antivirus. Los virus son una de las mayores amenazas para los ordenadores que existe en Internet, por el número de daños causados. La actualización constante del mismo es importantísimo, cada mes se descubren más de 500 nuevos virus, lo cual indica que si únicamente instalamos el programa y no lo actualizamos seremos vulnerables a los nuevos virus.
 - Realizar una constante actualización del sistema operativo. Frecuentemente se descubren agujeros de seguridad en los mismos y los fabricantes ofrecen actualizaciones para subsanarlos.
 - Realizar copias periódicas de los datos contenidos en el ordenador, a ser posible a un sistema no borrable como pudiera ser un CDR.
 - No previsualizar los mensajes de correo electrónico, de esta forma se evitaría la acción de determinados virus, quienes actúan con la mera previsualización de los mismos.
 - No leer mensajes de correo de desconocidos, sobre todo si vienen en un idioma que no es el nativo. ¿Tiene algún amigo o conocido que le pudiera escribir en inglés?
 - No instalar programas de fuentes desconocidas o poco fiables, ya que nadie garantiza que los mismos no estén modificados y realicen algunas acciones no deseadas. Usar software original.
- Existen alternativas de bajo coste o incluso gratuitas a casi todos los programas comerciales.



Estás en: Servicios en la web / Prevención frente a la delincuencia informática / Denuncia.

- » Consejera
- » Ertzaintza. La policía de Euskadi
- » Comisarías
- » Servicios en la web
- » Programas de calidad
- » Ekinbide - iniciativas de mejora
- » Derechos sobre Protección de Datos
- » Delincuencia Terrorista
- » Estadísticas delictivas
- » Servicio de prensa
- » Consejos de seguridad
- » Empresas
- » Proyectos normativos
- » Entidades de participación
- » PGSPE 2020

Línea directa confidencial
Antiterrorismo
900.840.843

Denuncias por Internet 

Atención de emergencias

TRAFIKOA **011** 

 **Udalzaingoa**

Denuncia

Si usted desea interponer una denuncia formal por considerar que ha sido víctima de un "delito informático", no dude en acudir a la Comisaría de la Ertzaintza más cercana, donde será atendido de inmediato.

A la hora de interponer la denuncia, tenga presente:

- No olvide aportar toda la documentación que tenga sobre los hechos ilícitos, aunque le pueda parecer irrelevante
- Si es posible, realice copia en soporte digital (disquete o cdr) con los datos aportados, como correos electrónicos, fotografías, etc.
- De los correos electrónicos, es especialmente importante la información contenida en las cabeceras del mismo, por lo que, si no puede aportar una copia del mismo, es conveniente que adjunte una impresión de los datos contenidos en su cabecera.
- En caso de tratarse de mensajes a teléfonos móviles, aporte el texto completo.
- Su denuncia siempre será atendida por personal experto en esta tipología delictiva. En este sentido, la Ertzaintza, dentro de la Unidad de Investigación Criminal y Policía Judicial, dispone de un grupo especializado en esta materia, integrado por agentes con formación específica en aspectos jurídicos y técnicos, y con experiencia en investigación criminal, denominado Sección Central de Delitos en Tecnologías de la Información (SCDTI).

Los agentes de la SCDTI, dentro de su actividad de descubrimiento e investigación de los delitos relacionados con las nuevas tecnologías e internet, dan cobertura a todas las actuaciones de la Ertzaintza en estas cuestiones.

◀ Consejos

Información y colaboración ▶



Estás en: Servicios en la web / Prevención frente a la delincuencia informática / Información y colaboración

- » Consejera
- » Ertzaintza. La policía de Euskadi
- » Comisarías
- » Servicios en la web
- » Programas de calidad
- » Ekinbide - iniciativas de mejora
- » Derechos sobre Protección de Datos
- » Delincuencia Terrorista
- » Estadísticas delictivas
- » Servicio de prensa
- » Consejos de seguridad
- » Empresas
- » Proyectos normativos
- » Entidades de participación
- » PGSPE 2020

Línea directa confidencial
Antiterrorismo
900.840.843

Denuncias
por Internet

SOS DEIAK

TRAFIKOA 011

Udalzaingoa

Información y colaboración

Si usted no pretende interponer una denuncia formal, pero desea aportar información a la Ertzaintza sobre un hecho relacionado con la informática, con internet..., que considera delictivo, puede igualmente acudir a la Comisaría de la Ertzaintza más cercana.

No obstante, puede también dirigirse directamente al grupo de la Ertzaintza especializado en "delincuencia informática", Sección Central de Delitos en Tecnologías de la Información, (SCDTI), contactando mediante la siguiente dirección de correo electrónico: di@ertzaintza.eus

La información que usted facilite por esta vía será en todo caso atendida y estudiada, iniciando la Ertzaintza las gestiones necesarias para confirmar la existencia de delito y, en caso de resultar procedente, iniciar las investigaciones precisas tendentes al esclarecimiento del mismo.



◀ Denuncia



Estás en: Entidades de participación / De relación directa con Ertzaintza

- » Consejera
- » Ertzaintza. La policía de Euskadi ▼
- » Comisarías
- » Servicios en la web ▼
- » Programas de calidad ▼
- » Ekinbide - iniciativas de mejora
- » Derechos sobre Protección de Datos
- » Delincuencia Terrorista
- » Estadísticas delictivas
- » Servicio de prensa
- » Consejos de seguridad
- » Empresas ▼
- » Proyectos normativos
- » Entidades de participación ▼
- » PGSPE 2020

De relación directa con Ertzaintza

<< < 1 > >>

Oficina de iniciativas ciudadanas para la mejora del sistema de seguridad pública-Ekinbide

Comisiones de Coordinación de ámbito local de Ertzaintza y Policías Locales

Consejo de Seguridad Pública de Euskadi

Comisión de Seguridad Vial de Euskadi

Comisión Mixta de Coordinación de la Seguridad Privada de Euskadi

Ertzaintza SCDTI

Nombre del Equipo/Capacidad
Sección Central de Delitos en Tecnologías de la Información
Secciones Centrales de Investigación Criminal y Policía Judicial
División de Investigación Criminal
Ertzaintza

Siglas
SCDTI

Logotipo



Organización a la que pertenece
ERTZAINZTA

Año de creación:
1998

Ámbito de Actuación:
Comunidad Autónoma del País Vasco

Dirección web:
www.ertzaintza.eus

Correo electrónico:

Redes sociales:

FIRST:

TRUST INTRODUCER:

OTROS:



COMUNICACIÓN

COMISARÍA VIRTUAL

CONÓCENOS

PARTICIPACIÓN
CIUDADANA

Estás en [PORTADA](#) > [ORG. CENTRAL](#) > [P. JUDICIAL](#) >[UDEF / Brig. C. Inv. Tecnológica / Quiénes somos?](#)

Domingo 19 de Mayo de 2019

Comisaría General de Policía Judicial

Policía Judicial

Estructura

Funciones

Unidad de Inv. Tecn.

Brig. Central Invest. Tecnológica

➤ Quiénes Somos

➤ Funciones

➤ Actuaciones

➤ Consejos de Seguridad

➤ Enlaces

Unidad Atención a la Familia y Mujer

B.C.I.T. - ¿Quiénes somos?

La Brigada Central de Investigación Tecnológica es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería...

La Brigada Central de Investigación Tecnológica está encuadrada en la Unidad de Delincuencia Económica y Fiscal (UDEF) que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución de las actividades delictivas, de ámbito nacional e internacional, en materia de delincuencia económica y fiscal, así como la coordinación operativa y apoyo técnico a las respectivas Unidades Territoriales.

Nuestra misión consiste en obtener las pruebas, perseguir a los delincuentes y poner a unas y otros a disposición judicial. Nuestras herramientas son la formación continua de los investigadores, la colaboración de las más punteras instituciones públicas y privadas, la participación activa en los foros internacionales de cooperación policial y la colaboración ciudadana.





COMUNICACIÓN

COMISARÍA VIRTUAL

CONÓCENOS

PARTICIPACIÓN
CIUDADANA

Estás en [PORTADA](#) > [ORG. CENTRAL](#) > [P. JUDICIAL](#) > [UDEF / Brig. C. Inv. Tecnológica / Funciones](#)

Domingo 19 de Mayo de 2019

Comisaría General de Policía Judicial

Policía Judicial

Estructura

Funciones

Unidad de Inv. Tecn.

Brig. Central Invest. Tecnológica

➤ Quiénes Somos

➤ Funciones

➤ Actuaciones

➤ Consejos de Seguridad

➤ Enlaces

Unidad Atención a la Familia y Mujer

B.C.I.T.- Funciones

- La realización directa de las investigaciones especialmente complejas.
- La coordinación de las operaciones que involucren a diversas Jefaturas Superiores.
- La formación del personal del Cuerpo Nacional de Policía y otros cuerpos de Policía extranjeros.
- La representación internacional y la ejecución y/o coordinación de las investigaciones que tengan su origen en otros países.



COMUNICACIÓN

COMISARÍA VIRTUAL

CONÓCENOS

PARTICIPACIÓN
CIUDADANA

Estás en [PORTADA](#) > [ORG. CENTRAL](#) > [P. JUDICIAL](#) > [UDEF / Brig. C. Inv. Tecnológica](#) / Actuaciones

Domingo 19 de Mayo de 2019

Comisaría General de Policía Judicial

Policía Judicial

Estructura

Funciones

Unidad de Inv. Tecn.

Brig. Central Invest. Tecnológica

➤ Quiénes Somos

➤ Funciones

➤ Actuaciones

➤ Consejos de Seguridad

➤ Enlaces

Unidad Atención a la Familia y Mujer

B.C.I.T. - Actuaciones

- Amenazas, injurias, calumnias. Por correo electrónico, sms, tablones de anuncios, foros, newsgroups, web...
- Pornografía infantil. Protección al menor en el uso de las nuevas tecnologías.
- Fraudes en el uso de las comunicaciones. Piratería de señales de televisión privada.
- Fraudes en Internet. Estafas. Uso fraudulento de tarjetas de crédito. Fraudes en subastas. Comercio electrónico.
- Seguridad lógica. Virus. Ataques de denegación de servicio. Sustracción de datos. Hacking. Descubrimiento y revelación de secreto. Suplantación de personalidad. Sustracción de cuentas de correo electrónico.
- Piratería de programas de ordenador, de música y de productos cinematográficos.

Comisaría General de Policía Judicial

Policía Judicial

- Estructura
- Funciones
- Unidad de Inv. Tecn.
 - Brig. Central Invest. Tecnológica
 - Quiénes Somos
 - Funciones
 - Actuaciones
 - Consejos de Seguridad
 - Enlaces
- Unidad Atención a la Familia y Mujer

B.C.I.T. - Consejos de seguridad

- En las redes sociales: mantén tu perfil privado, evite las contraseñas fáciles de adivinar.
- Utilice contraseñas "de calidad" (con letras, números y otros caracteres). Cámbielas periódicamente.
- No desestime las medidas de seguridad al elegir "la pregunta secreta", puede que esté dejando una puerta abierta a sus cuentas de correo electrónico y perfiles sociales. Actualice su sistema operativo según las recomendaciones del fabricante o distribución.
- Adquiera un buen producto antivirus y actualícelo con regularidad. Realice periódicamente copias de seguridad de su sistema.
- Nunca ofrezca datos personales por Internet, a menos que sea en sitios de total confianza. COMPRUEBE LOS CERTIFICADOS.
- No introducir el número de tarjeta en páginas de contenido sexual o pornográfico, en los que se solicita como pretexto, para comprobar la mayoría de edad. Extreme la precaución en los archivos que recibe en sesiones chat.
- Para evitar los fraudes telefónicos, controle sus facturas, compruebe los números a los que ha llamado, y que el gasto facturado se corresponde con las comunicaciones realizadas. Adopte las medidas necesarias, cuando le ofrecen "regalos" sustanciosos y, para recibirlos tiene que llamar por teléfono a prefijos de tarificación adicional.
- No facilite sus números de teléfono, tanto fijo como móvil, a personas desconocidas o en webs que no le ofrezcan confianza suficiente.
- Asista a su hijo/a menor en su navegación por Internet. Tútelos como lo hace en cualquier otra actividad cotidiana.
- Hábleles de los peligros del chat, donde se pueden confundir, al chatear con supuestos amigos que no resultan tales, prestando especial atención a los contenidos sexuales. No les permita que envíen sus fotos o de su familia ni cualquier información sobre ellos y ellas, sin la autorización de sus padres.
- No les permita que envíen sus fotos o de su familia ni cualquier información sobre ellos y ellas, sin la autorización de sus padres.
- Consensúe con su hija o hijo ciertas normas a seguir en Internet, compruebe que contenidos consideran ellos y ellas que son los adecuados para exponer y compartir en la red.

Comisaría General de Policía Judicial

Policía Judicial

Estructura
Funciones
Unidad de Inv. Tecn.
Brig. Central Invest. Tecnológica

- Quiénes Somos
- Funciones
- Actuaciones
- Consejos de Seguridad
- Enlaces

Unidad Atención a la Familia y Mujer

BIT - Enlaces

Contacto

➤ **Brigada de Investigación tecnológica**

Centro Policial de Canillas
C/ Julián González Segador, s/n
28043 - Madrid

➤ **Formulario de Contacto**

Enlaces de interés

» Oficina de Seguridad del Internauta
www.osi.es

» Agencia Española de Protección de Datos
www.agpd.es

» www.seguridadweb20.es

» www.chaval.es

» www.pantallasamigas.net

» www.alia2.org

» conexioninversa.blogspot.com



[Inicio](#) » [Miembros](#) » **Policía Nacional (Seguridad Lógica)**

Policía Nacional (Seguridad Lógica)

Nombre del Equipo/Capacidad	Seguridad Lógica
-----------------------------	------------------

Siglas	U.I.T. P.N.
--------	-------------

Logotipo



Organización a la que pertenece	Policía Nacional
---------------------------------	------------------

Año de creación:	-
------------------	---

Ámbito de Actuación:	Todo el territorio nacional
----------------------	-----------------------------

Dirección web:	www.policia.es
----------------	--

Correo electrónico:	-
---------------------	---

Redes sociales:	Twitter
-----------------	-------------------------

FIRST:

TRUST INTRODUCER:



S E R V I C E S

› SERVICES

Citizen's advice bureau

null

Reporting

Administrative procedures

Weapons & explosives

Private security

Safety advice

Gender violence and child abuse

Efectos recuperados

Links of interest

Notice board

La Ciberseguridad es una responsabilidad compartida

Inglés > Services > Delitos Telemáticos



› Delitos Telemáticos

Si está **interesado en denunciar delitos relacionados con las nuevas tecnologías** (internet, correo electrónico, SMS, WhatsApp, etc.) debe acceder al portal del Grupo de Delitos Telemáticos de la Guardia Civil.

El Grupo de Delitos Telemáticos (GDT) **fue creado para investigar**, dentro de la Unidad Central Operativa de la Guardia Civil, **todos aquellos delitos que se cometen a través de Internet**.

› ¿Conoces el portal web del Grupo de Delitos Telemáticos de la Guardia Civil?

En sus páginas encontrarás contenidos de interés:

- Alertas de seguridad tecnológicas
- Consejos de seguridad
- Enlaces de seguridad
- Preguntas más frecuentes
- Recursos: aplicaciones para móviles, navegadores, multimedia y el libro "X1Red+Segura".



También puedes colaborar con el Grupo de Delitos Telemáticos **informando de la comisión delitos informáticos**.

INFORMACIÓN INSTITUCIONAL

› INFORMACIÓN INSTITUCIONAL

› Conoce a la Guardia Civil

- Cuándo dirigirse a la Guardia Civil
- Estructura y organización
- Misiones
- Funciones
 - Seguridad Ciudadana
 - Seguridad Vial
 - Control de las armas
 - Lucha antiterrorista
 - Violencia de género
 - Resguardo Fiscal, Costas y Fronteras
 - El mar
 - El aire
 - La montaña
 - Medio ambiente
 - Orden Público
 - Protección de altas personalidades
 - Seguridad del Estado
 - Delincuencia informática
 - Galería de imágenes
 - Desactivación de Explosivos y Defensa NRBQ
 - Protección de Edificios Públicos
 - Criminalística
 - Patrimonio Histórico
 - Cooperación Internacional
 - Gestión estratégica
 - Identidad corporativa
 - Historia
 - Museo
 - Terrorismo

Web Oficial de la Guardia Civil > Información Institucional > Conoce a la Guardia Civil > Funciones > Delincuencia informática



› Delincuencia informática

En esta sección podrá obtener información sobre los guardias civiles dedicados a la **lucha contra la delincuencia organizada y los delitos por Internet y otros medios telemáticos**. En concreto sobre la creación y antecedentes, la misión general y los cometidos fundamentales, la organización y estructura, así como el despliegue territorial de la **Unidad Central Operativa (UCO)** y de los **Grupos de Delitos Telemáticos (GDT)**.

Grupo de delitos telemáticos (GDT), lucha contra el Ciberdelito

Historia

El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos actos delictivos que se cometen a través de sistemas de telecomunicaciones y mediante las tecnologías de la información. En 1996, cuando las investigaciones sobre delitos informáticos empezaron a adquirir especial relevancia, se vio la necesidad de crear un Grupo específicamente destinado a perseguir esta clase de delincuencia, constituido por agentes que unieran a su preparación en investigación criminal una buena formación informática.

A mediados de 1999, dado que el campo de actuación se había ampliado a los fraudes en el sector de las telecomunicaciones, se adoptó una terminología más en consonancia con la realidad, pasando a llamarse **Departamento de Delitos de Alta Tecnología (DDAT)**.

En 2000, se produce una mayor especialización de sus miembros, estructurándose en las áreas delictivas de pornografía infantil, fraudes y estafas, propiedad intelectual y delitos de hacking, en consonancia con el Convenio de Ciberdelincuencia del Consejo de Europa, en el que participa personal de la Guardia Civil como expertos policiales.

Es en 2003 cuando la Unidad adquiere su actual nombre: **GRUPO DE DELITOS TELEMÁTICOS (GDT)** se crean a nivel provincial los **Equipos de Investigación Tecnológica (EDITE)**.

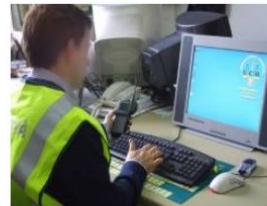
Desde el año 2002, la Guardia Civil organiza anualmente un Foro Iberoamericano de Encuentro de Ciberpolicías (FIEC), que se ha constituido en un referente de colaboración internacional entre unidades de lucha contra la delincuencia informática a nivel latinoamericano y nexo de unión con otros foros a nivel europeo.

Misión

- Llevar a cabo **investigaciones relacionadas con la delincuencia informática y los fraudes en el sector de las telecomunicaciones** bien por propia iniciativa, a requerimiento de las Autoridades Judiciales o por denuncia de los ciudadanos.
- **Detección de delitos informáticos en la Red** (patrullas ciberméticas).
- **Apoyar** las investigaciones del resto de las Unidades de la Guardia Civil.

Organización y estructura

El Grupo de Delitos Telemáticos (GDT) se integra en la Unidad Central Operativa de la Guardia Civil. Los **Equipos de Investigación Tecnológica (EDITE)** se encuadran en las Unidades Orgánicas de Policía Judicial de la Guardia Civil, desplegadas a nivel provincial.





GDT Grupo de Delitos Telemáticos
Unidad Central Operativa

Inicio
La unidad
Consejos de seguridad
Enlaces de seguridad
Preguntas más frecuentes
Denunciar el delito
Quiero denunciar
Quiero informar
Colaborar con el GDT
Recursos
Multimedia
Libro X1Red+Segura

Ayúdanos a perseguir los delitos en la red.

[DENUNCIAR EL DELITO](#)

[Alertas de seguridad tecnológicas](#) [+ Alertas](#) [Noticias del GDT](#)

30-06-2017 Sobre el proceder afectados Estafas investigadas en Operación Rikati

iGDT Informa!

OPERACIÓN RIKATI

DDT
DEPARTAMENTO DE DELITOS TELEMÁTICOS

... Alerta completa.





- GRUPO DE DELITOS TELEMÁTICOS - GUARDIA CIVIL

GDT

Grupo de Delitos Telemáticos
Unidad Central Operativa

[Inicio](#)

La Unidad

[Consejos de seguridad](#)

[Enlaces de seguridad](#)

[Preguntas más
frecuentes](#)

[Denunciar el delito](#)

[Quiero denunciar](#)
[Quiero informar](#)

[Colaborar con el GDT](#)

[Recursos](#)

[Multimedia](#)

[Libro X1Red+Segura](#)

[< Atrás](#)

La unidad

El Grupo de Delitos Telemáticos fue creado para investigar, dentro de la Unidad Central Operativa de la Guardia Civil, todos aquellos delitos que se cometen a través de Internet.

Su origen se remonta al año 1.996, cuando se constituyó el Grupo de Delitos Informáticos (GDI) para atender a las pocas denuncias que había entonces por los llamados delitos informáticos.

Su buen hacer y el crecimiento exponencial de usuarios de la red, propiciaron el **crecimiento del grupo**, que pasó a llamarse Departamento de Delitos de Alta Tecnología (DDAT), asumiendo como nueva competencia **el fraude en el sector de las telecomunicaciones**.

Con la socialización de Internet y el crecimiento de los hechos delictivos, se amplía el abanico de competencias de investigación, que alcanza a todas aquellas conductas delictivas realizadas a través de los sistemas de información o contra éstos, lo que se conoce popularmente como el cibercrimen. El departamento cambia de nombre por el actual, Grupo de Delitos Telemáticos (GDT). Estos cambios se acompañaron de la creación de los Equipos de Investigación Tecnológica (EDITE,s) en cada uno de las provincias de España.

El esfuerzo principal del GDT y de los EDITE,s ha sido, desde su creación, la investigación de la delincuencia que se vale de las redes y sistemas de información para su comisión. También cabe destacar los esfuerzos que realizan para fomentar un uso seguro de las nuevas tecnologías, consciente de que a la larga este esfuerzo ayudará a minimizar el impacto de la delincuencia.

Cabe destacar en el trabajo del GDT, su presencia continuada en seminarios y conferencias internacionales, lo que le ha permitido crear con una red de contactos policiales a nivel internacional, esencial en la resolución de determinadas investigaciones.

Actualmente es miembro y participa activamente en los Grupos de Trabajo de Interpol de Europa y Latinoamérica, en el Foro internacional del G-8 para el cibercrimen, y en Grupo de Europol.



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR



- GRUPO DE DELITOS TELEMÁTICOS - GUARDIA CIVIL

- DELITOS TELEMÁTICOS - GUARDIA CIVIL



GDT

Grupo de Delitos Telemáticos
Unidad Central Operativa

[Inicio](#)

[La Unidad](#)

[Consejos de seguridad](#)

[Enlaces de seguridad](#)

[Preguntas más frecuentes](#)

[Denunciar el delito](#)

[Quiero denunciar](#)

[Quiero informar](#)

[Colaborar con el GDT](#)

[Recursos](#)

[Multimedia](#)

[Libro X1Red+Segura](#)

[< Atrás](#)

DECÁLOGO DE NAVEGACIÓN SEGURA

Actualice de forma regular el sistema operativo.
[\(pulse para ampliar\)](#)

Utilice un navegador actualizado.
[\(pulse para ampliar\)](#)

Elija contraseñas seguras y diferentes para cada servicio de Internet.
[\(pulse para ampliar\)](#)

Verifique regularmente los movimientos de su cuenta bancaria.
[\(pulse para ampliar\)](#)

Utilice un antivirus con licencia y actualizado, e instale un firewall.
[\(pulse para ampliar\)](#)

Considere la posibilidad de utilizar un único dispositivo para las transacciones de banca y comercio electrónicos (PC, Smartphone, ...etc.).
[\(pulse para ampliar\)](#)

Desconfíe de los mensajes cortos y extraños que pueda recibir por redes sociales, sobre todo si incluyen un enlace para acceder a otro contenido.
[\(pulse para ampliar\)](#)

No piense que es inmune al software malicioso porque utilice un determinado sistema operativo o un dispositivo portátil
[\(pulse para ampliar\)](#)

No confíe ciegamente en las aplicaciones de seguridad instaladas, éstas no remplazan a la navegación responsable ni a la prudencia del usuario.

Si dispone de un router inalámbrico para conectarse a internet, cambie las contraseñas por defecto y establezca una más segura.
[\(pulse para ampliar\)](#)

**EN DEFINITIVA, UTILICE EL SENTIDO COMÚN
COMO MEJOR ANTIVIRUS Y NO CONFÍE
CIEGAMENTE EN LOS SISTEMAS Y SUS
APLICACIONES**



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR





- GRUPO DE DELITOS TELEMÁTICOS - GUARDIA CIVIL

- [Inicio](#)
- [La Unidad](#)
- [Consejos de seguridad](#)
- Enlaces de seguridad**
- [Preguntas más frecuentes](#)
- [Denunciar el delito](#)
 - [Quiero denunciar](#)
 - [Quiero informar](#)
- [Colaborar con el GDT](#)
- [Recursos](#)
 - [Multimedia](#)
 - [Libro X1Red+Segura](#)

< Atrás

Enlaces de seguridad

Yo denuncio.

La campaña YO DENUNCIO bajo el lema "entre todos haremos una red mas segura" invita a cualquier usuario a poner de manifiesto las irregularidades que haya presenciado en la Red. Para ello solicitamos tu ayuda. Si lo deseas, copia el código HTML y colócalo en tu web. De esta manera, los usuarios podrán denunciar contenidos ilícitos y fraudes de una manera rápida y sencilla



Páginas Web de seguridad:

1. Oficina de seguridad del internauta

<http://www.osi.es>



2. Instituto Nacional de la Ciberseguridad

<http://www.incibe.es/>



3. Agencia de Protección de Datos

<https://www.agpd.es>



4. Asociación Española de Usuarios de Internet

<http://www.aui.es>



5. Asociación de Internautas

<http://www.internautas.org>



6. Hispacsec

- GRUPO DE DELITOS TELEMÁTICOS - GUARDIA CIVIL

- GRUPOS TELEMÁTICOS - GUARDIA CIVIL



GRUPO DE DELITOS TELEMÁTICOS - GUARDIA CIVIL

GDT

Grupo de Delitos Telemáticos
Unidad Central Operativa



GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR



[Inicio](#)

[La Unidad](#)

[Consejos de seguridad](#)

[Enlaces de seguridad](#)

Preguntas más frecuentes

[Denunciar el delito](#)

[Quiero denunciar](#)

[Quiero informar](#)

[Colaborar con el GDT](#)

[Recursos](#)

[Multimedia](#)

[Libro X1Red+Segura](#)

[< Atrás](#)

Preguntas más frecuentes

¿Quién investiga los Delitos Informáticos en la Guardia Civil?

¿Cómo se puede formar parte de GDT?

¿Qué tengo que hacer para ser Guardia Civil del GDT?

¿Cómo puedo colaborar con la lucha contra el cibercrimen?

¿Puedo remitir cualquier tipo de información?

¿Puedo informar de un problema de configuración o seguridad en mi ordenador? ¿A quién debo dirigirme?

¿Qué diferencia hay entre informar o denunciar?

¿Qué debo poner en la denuncia?

¿Qué sucede con mi denuncia?

¿Qué pasa si denuncio y luego no llevo el papel a un centro policial o judicial?

¿Qué pasa con las informaciones que facilito?

¿Cómo puedo acreditar o demostrar que he informado al GDT de un hecho delictivo?

GRUPO DE DELITOS TELEMÁTICOS - GUARDIA CIVIL



- GRUPO DE DULITOS TELÉMÁTICOS -
- SUDARÍA EIVIL -

GDT Grupo de Delitos Telemáticos
Unidad Central Operativa

GOBIERNO
DE ESPAÑA

MINISTERIO
DEL INTERIOR

GUARDIA CIVIL

[Inicio](#)

[La Unidad](#)

[Consejos de seguridad](#)

[Enlaces de seguridad](#)

[Preguntas más frecuentes](#)

[Denunciar el delito](#)

[Quiero denunciar](#)

[Quiero informar](#)

[Colaborar con el GDT](#)

[Recursos](#)

[Multimedia](#)

[Libro X1Red+Segura](#)

[< Atrás](#)

Denunciar el delito

Respetado internauta:

Si Vd. cree que ha sido testigo o víctima de un **delito informático**, puede denunciar los hechos para que sean investigados. No todos los hechos investigados llegan a ser esclarecidos, pero su conocimiento ayuda a disminuir la cifra negra de delitos ocultos y a dimensionar adecuadamente el problema de la delincuencia informática.

La *denuncia*, conforme a nuestra Ley de Enjuiciamiento Criminal, artículos **265** y **266**, exige la personación del denunciante o su representante legal, en un juzgado o centro policial, donde debe acreditar su identidad.

Toda denuncia da lugar a un procedimiento judicial en el que Vd. podrá ser citado a declarar y efectuar las reclamaciones que la ley prevé.

Si decide denunciar, le ofrecemos un **formulario de denuncia** con todos los datos necesarios para la denuncia, que una vez rellenado, generará un documento denuncia, en formato **pdf**, que podrá imprimir y presentar en el centro policial o judicial que decida, acreditándose con su DNI, NIE o pasaporte. Este formulario con su documento denuncia, le permitirá reducir los trámites y tiempos de espera.

*Si su intención es únicamente facilitar información a este Grupo de Delitos Telemáticos de la Guardia Civil, de los hechos que considera no ajustados a la legalidad, puede realizarlo de forma totalmente anónima a través del **formulario de información ciudadana**.*

Si la información refiere hechos no relacionados con delitos informáticos, o desea realizar alguna consulta o solicitud de información, debe visitar la web de **Oficina de Atención al Ciudadano** o enviar un mensaje al correo electrónico electrónico sugerencias@guardiacivil.org.

[QUIERO DENUNCIAR](#)

[QUIERO INFORMAR](#)



G.D.T.

- GRUPO DE DELITOS TELÉMATICOS - GUARDIA CIVIL

- GRUPOS TELÉMATICOS - GUARDIA CIVIL

< Atrás

FORMULARIO PARA COLABORAR CON EL GDT

Los datos solicitados son necesarios para contactar con Ud.

Localidad:

Provincia:

Teléfono:

Correo electrónico:

Exponga sus conocimientos informáticos y en qué estaría dispuesto a colaborar:



Texto imagen

Enviar

Guardia Civil - Departamento de Delitos Telemáticos

Nombre del Equipo/Capacidad	Departamento de Delitos Telemáticos
-----------------------------	-------------------------------------

Siglas	DDT
--------	-----

Logotipo



Organización a la que pertenece	Guardia Civil
---------------------------------	---------------

Año de creación:	1996
------------------	------

Ámbito de Actuación:	Investigación criminal del cibercrimen
----------------------	--

Dirección web:	www.gdt.guardiacivil.es
----------------	--

Correo electrónico:	gdt@guardiacivil.es
---------------------	--

Facebook

Redes sociales:

Twitter

Youtube

FIRST:

TRUST INTRODUCER:

OTROS:

[Inicio](#) » [Miembros](#) » **Guardia Civil - Ciberinteligencia y Ciberterrorismo**

Guardia Civil - Ciberinteligencia y Ciberterrorismo

Nombre del Equipo/Capacidad

Guardia Civil - Ciberinteligencia y Ciberterrorismo

Siglas

GC

Logotipo



Organización a la que pertenece

Dirección General de la Guardia Civil

Año de creación:

Ámbito de Actuación:

Seguridad Pública, Fuerzas de Seguridad del Estado

Dirección web:

www.guardiacivil.es

Correo electrónico:



Redes sociales:

FIRST:

TRUST INTRODUCER:

[ABOUT EUROPOL](#)[ACTIVITIES & SERVICES](#)[CRIME AREAS & TRENDS](#)[PARTNERS & AGREEMENTS](#)[CAREERS & PROCUREMENT](#)[NEWSROOM](#)[PUBLICATIONS & DOCUMENTS](#)

2/4



INTERNET ORGANISED CRIME THREAT ASSESSMENT 2018

Europol's latest cybercrime report provides insights into emerging threats and key developments.

[READ MORE](#)

Latest

UPDATES



GOZNYM MALWARE: CYBERCRIMINAL NETWORK DISMANTLED IN INTERNATIONAL OPERATION

PRESS RELEASE



3, 2, 1... Capture!

PRESS RELEASE



Caliphate Soldiers and Lone
Actors: What to Make of IS
Claims for Attacks in the West
2016-2018

Are you looking for a new
career challenge?

Apply now at Europol

[ABOUT EUROPOL](#)[ACTIVITIES & SERVICES](#)[CRIME AREAS & TRENDS](#)[PARTNERS & AGREEMENTS](#)[CAREERS & PROCUREMENT](#)[NEWSROOM](#)[PUBLICATIONS & DOCUMENTS](#)[HOME](#) ➤ [ACERCA DE EUROPOL](#)

ACERCA DE EUROPOL



Cómo contribuye Europol a hacer de Europa un lugar más seguro

Desde nuestra sede principal en La Haya (Países Bajos), asistimos a los 28 Estados miembros de la Unión en su lucha contra la gran delincuencia internacional y el terrorismo. Colaboramos asimismo con numerosos estados asociados no pertenecientes a la UE y organizaciones internacionales.

Las redes de delincuencia y terroristas a gran escala constituyen una amenaza significativa para la seguridad interna de la UE y para la seguridad y los medios de vida de sus ciudadanos. Las amenazas más graves para la seguridad se derivan de:

- el terrorismo;
- el tráfico de drogas y el blanqueo de dinero a escala internacional;
- el fraude organizado;
- la falsificación de euros;
- y el contrabando de personas.

Crecen además nuevos peligros, como la ciberdelincuencia y la trata de seres humanos. Las redes que subyacen a tales formas de delincuencia en cada una de estas áreas aprovechan con rapidez las nuevas oportunidades que se les plantean, y resisten con tenacidad las medidas encaminadas a velar por el cumplimiento de la ley.

Europol es la agencia de la Unión Europea en materia policial. Nuestro principal objetivo es contribuir a la consecución de una Europa más segura para beneficio de todos los ciudadanos de la UE.

SERVICIOS SINGULARES

Nuestra posición central en la arquitectura europea en materia de seguridad nos permite ofrecer una singular gama de servicios y ejercer como:

- › centro de apoyo a las operaciones policiales;
- › eje para la información sobre actividades delictivas;
- › centro de conocimientos policiales especializados.

El análisis constituye la piedra angular de nuestras actividades. Empleamos a unos 100 analistas de actividades delictivas, que figuran entre los mejor cualificados en esta materia en Europa. Estos utilizan herramientas de vanguardia para contribuir a las investigaciones emprendidas por los cuerpos policiales en los Estados miembros a diario.

Con el fin de ofrecer a nuestros socios una visión más detallada de los delitos a los que se enfrentan, Europol lleva a cabo evaluaciones periódicas que proporcionan análisis prospectivos de gran exhaustividad de las actividades delictivas y el terrorismo en la UE, entre los que figuran:

- › la Evaluación de la amenaza de la delincuencia grave y organizada en la UE (SOCTA), en la que:
 - › se identifican y valoran las amenazas emergentes;
 - › o se describe la estructura de los grupos de delincuencia organizada (GDO) y el modo en que operan estos, así como los principales tipos de delito que afectan a la UE;
- › El Informe sobre la situación y las tendencias del terrorismo en la UE (TE-SAT), en el que se refiere con detalle el estado del terrorismo en la Unión.
- › La publicación anual Panorama de Europol, en la que se esbozan resultados y se facilita información específica sobre los tipos de funciones y sistemas de los que dispone Europol, y sobre su prestación, en forma de un apoyo coordinado a las operaciones policiales en toda Europa y, en ocasiones, en otros ámbitos geográficos.

EUROPOL EN CIFRAS

- › Una plantilla compuesta por más de 1 000 miembros
- › 220 funcionarios de enlace de Europol
- › En torno a 100 analistas de actividades delictivas
- › Se presta apoyo a más de 40 000 investigaciones internacionales cada año



READ MORE

MANDATO

Europol asiste a las autoridades policiales de toda la UE en las actividades de lucha contra la delincuencia y el terrorismo en todos los ámbitos que forman parte de su mandato.

Actividades operativas

Estas actividades se centran en:

- las drogas ilegales,
- la trata de seres humanos,
- la facilitación de la inmigración ilegal,
- la ciberdelincuencia,
- los delitos contra la propiedad intelectual,
- el contrabando de tabaco,
- la falsificación del euro,
- el fraude en el IVA,
- el blanqueo de dinero y el seguimiento de activos,
- los grupos de delincuencia organizada itinerantes,
- las bandas de motociclistas al margen de la ley,
- y el terrorismo.

GESTIÓN Y CONTROL

Europol responde a escala de la UE ante el Consejo de Ministros de Justicia y Asuntos de Interior.

Corresponde a este Consejo el desempeño de las funciones principales de orientación y control de Europol. Designa asimismo al Director y a los Directores Adjuntos, y aprueba el presupuesto de la Oficina (que forma parte del presupuesto general de la UE), junto con el Parlamento Europeo. Puede adoptar además, de manera conjunta con el Parlamento Europeo, las normativas que atañen a la labor de Europol. Cada año, el Consejo remite al Parlamento Europeo un informe especial sobre las actividades de Europol.

[New Europol regulation](#)

[Visit our statistics page](#)

Estructura organizativa

A la cabeza de Europol se encuentra su Director Ejecutivo, que ejerce como representante legal de la Oficina y es designado por el Consejo de la Unión Europea.

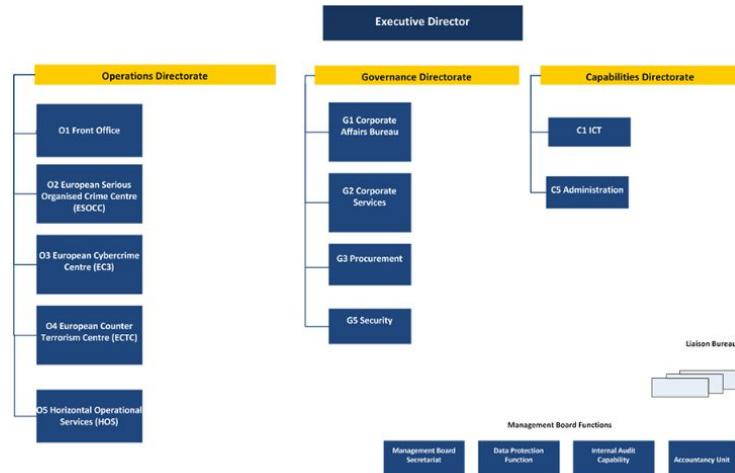
La actual Directora Ejecutiva de Europol es [Catherine De Bolle](#), que asumió el cargo en mayo 2018.

Cuenta con el apoyo de tres Directores Ejecutivos Adjuntos:

- [Wil van Gemert](#), del Departamento de Operaciones;
- [Oldrich Martinu](#), del Departamento de Gobernanza;
- [y Luis de Eusebio Ramos](#), del Departamento de Capacidades.

La plantilla de Europol está compuesta por miembros de muy diversos bagajes, procedentes de distintos países. Para más información, véase nuestra página de estadísticas.

El 1 de enero de 2010 Europol se convirtió en una agencia de la UE de pleno derecho. A continuación figura su estructura organizativa actual:



[GET IN TOUCH](#)

[SEE ALSO](#)

Subscribe to
[OUR NEWSLETTER](#)

Ciberdelincuencia

[MÁS INFORMACIÓN](#)

Destacados



MOST WANTED

Ten Most Wanted | Fugitives | Terrorism | Kidnapping/Missing Persons | Seeking Info | Parental Kidnapping | Bank Robbers | ECAP | ViCAP
Crimes Against Children | Murder | Additional Violent Crimes | Cyber | White Collar Crimes | Counterintelligence | CEI | Human Trafficking

Cyber's Most Wanted

Select the images of suspects to display more information.

Sort by:

Results: 69 Items



GOZNYM SUBJECTS



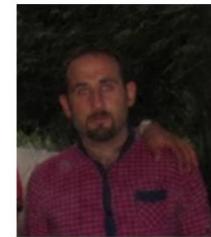
FUJIE WANG



IRGC-AFFILIATED CYBER ACTORS



MOJTABA MASOUMPOUR



BEHZAD MESRI



HOSSEIN PARVAR



MOHAMAD PARYAR



APT 10 GROUP



ZHANG SHILONG



ZHU HUA