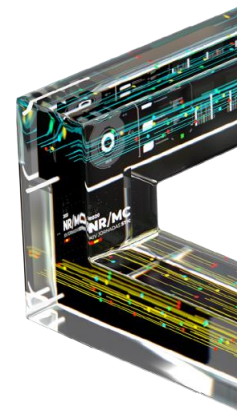
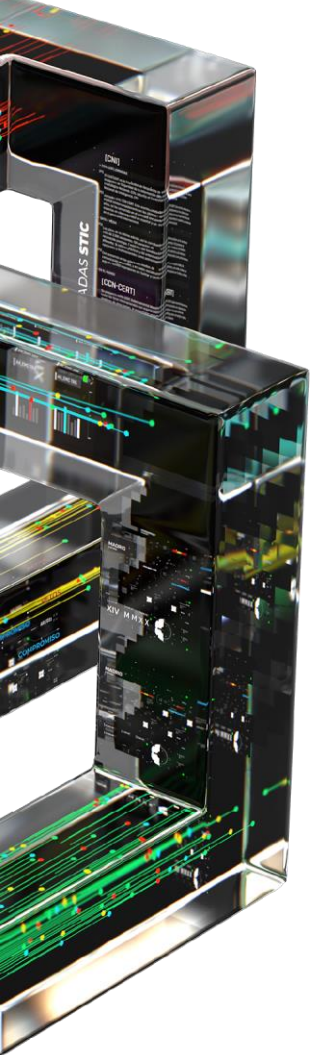


#XIVJORNADASCCNCERT

**“Ordenamiento jurídico y
Cibercriminalidad”**





Rosa María Serrano Oliver

DLTCode

rosa@dltcode.es

www.linkedin.com/in/rm-serrano

REALIDAD SOCIAL

Para adjuntar documentación, pulse "Examinar" para localizar el fichero que quiere adjuntar y pulse "Adjuntar". Realice esta acción tantas veces como desee sin exceder el espacio disponible para adjuntar archivos: 10240 kbytes restantes

Documento: No se eligió archivo

[Todos](#) [En tramitación](#) [Buscar expediente](#) [Ayuda](#)

[Desplegar](#) [Contraer](#) [Actualizar](#)

▼ [Expedientes](#) (8)

- ▶ [Impuestos y tasas](#) (5)
- ▶ [Certificaciones](#) (2)
- ▶ [Otros procedimientos tributarios](#) (1)

Además, le pueden interesar los siguientes servicios:

- [Consultar declaraciones presentadas](#)
- [Consultar notificaciones y comunicaciones no leídas](#)
- [Consultar sus domiciliaciones](#)
- [Consultar sus asientos registrales](#)



Elige tu situación laboral

Sube la siguiente documentación

Firmar los anexos sin enviar documentación



Ahora, necesitamos tus datos de contacto

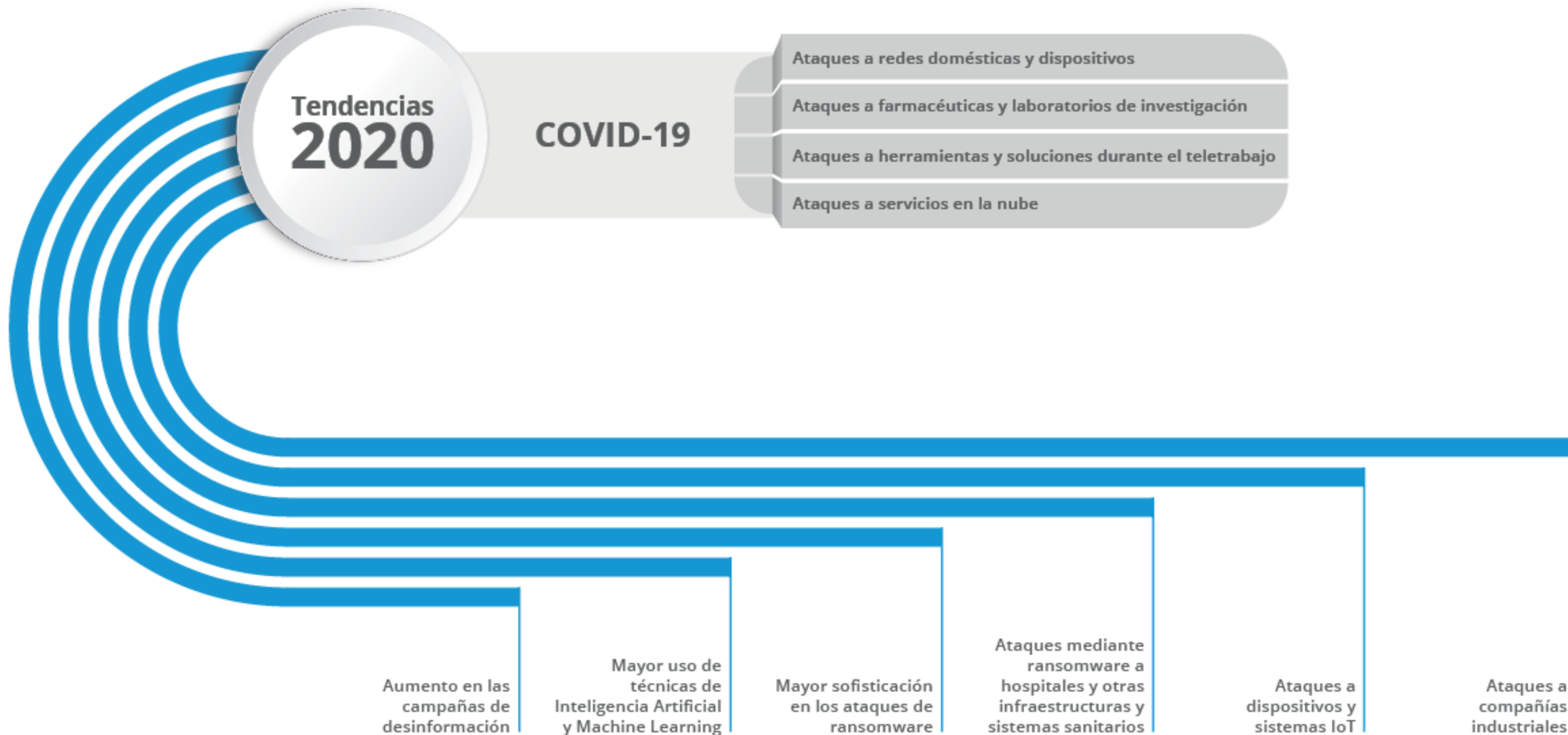
Tu email *

Ej: nombre@unsitio.com

Repite tu email *

Tu teléfono móvil *

Repite tu teléfono móvil *



ESTRATEGIA NACIONAL DE CIBERSEGURIDAD

LÍNEA DE ACCIÓN 3

Reforzar las capacidades de investigación y persecución de la cibercriminalidad, para garantizar la seguridad ciudadana y la protección de los derechos y libertades en el ciberespacio.

Esta línea de acción responde al Objetivo II de la Estrategia.

MEDIDAS

1. Reforzar el marco jurídico para responder eficazmente a la cibercriminalidad, tanto en lo relativo a la definición de tipos penales como en la regulación de adecuadas medidas de investigación.
2. Fomentar la colaboración y participación ciudadana, articulando instrumentos de intercambio y transmisión de información de interés policial, y promoviendo el desarrollo de campañas de prevención de la cibercriminalidad orientadas a ciudadanos y empresas.
3. Reforzar las acciones encaminadas a potenciar las capacidades de investigación, atribución, persecución y, en su caso, la actuación penal, frente a la cibercriminalidad.
4. Fomentar el traslado a los organismos competentes de la jurisdicción penal de la información relativa a incidentes de seguridad que presenten caracteres de delito, y especialmente de aquellos que afecten o puedan afectar a la provisión de los servicios esenciales y a las infraestructuras críticas.

5. Procurar a los operadores jurídicos el acceso a información y recursos materiales que aseguren una mejor aplicación del marco jurídico y técnico relacionado con la lucha contra la cibercriminalidad, y que les dote de mayores capacidades para la investigación y enjuiciamiento de los hechos ilícitos que correspondan.
6. Fomentar el intercambio de información, experiencia y conocimientos, entre el personal con responsabilidades en la investigación y persecución de la cibercriminalidad.
7. Asegurar a los profesionales del Derecho y a las Fuerzas y Cuerpos de Seguridad del Estado el acceso a los recursos humanos y materiales que les proporcionen el nivel necesario de conocimientos para la mejor aplicación del marco legal y técnico asociado.

Impulsar la coordinación de las investigaciones sobre cibercriminalidad y otros usos ilícitos del ciberespacio entre los distintos órganos y unidades con competencia en esta materia.

Fortalecer la cooperación judicial y policial internacional.

Operadores jurídicos



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

Ayúdanos a perseguir los delitos en la red.

[DENUNCIAR EL DELITO](#)



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?

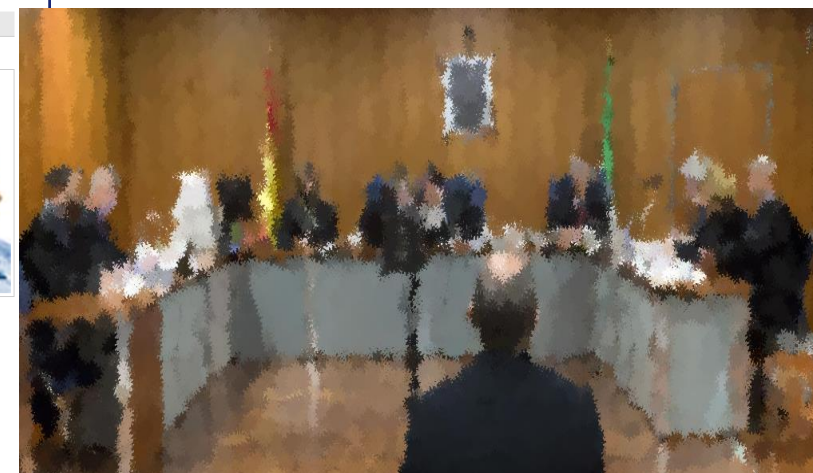
La Brigada Central de Investigación Tecnológica es la Unidad policial destinada a responder a los retos que plantean las nuevas formas de delincuencia. Pornografía infantil, estafas y fraudes por Internet, fraudes en el uso de las comunicaciones, ataques cibernéticos, piratería...

La Brigada Central de Investigación Tecnológica está encuadrada en la Unidad de Investigación Tecnológica (C.G.P.J.) . que es el órgano de la Dirección General de la Policía encargado de la investigación y persecución del ciberdelito de ámbito nacional y transnacional, Actuará como Centro de Prevención y Respuesta E- Crime de la Nacional de Policía.

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.



Comisaría General de Policía Judicial



CONSTITUCIÓN ESPAÑOLA

2. § [Constitución Española](#) (parcial)

CIBERDELINCUENCIA

- 43. § [Ley Orgánica del Código Penal](#) (parcial)
- 44. § [Ley Orgánica reguladora de la responsabilidad penal de los menores](#) (parcial)
- 45. § [Ley de Enjuiciamiento Criminal](#) (parcial)

NORMATIVA DE SEGURIDAD NACIONAL

- 3. § [Ley de Seguridad Nacional](#)
- 4. § [Consejo Nacional de Ciberseguridad](#)
- 5. § [Mecanismos para garantizar funcionamiento integrado Sistema de Seguridad Nacional](#)
- 6. § [Estrategia de Seguridad Nacional](#)
- 7. § [Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica](#)
- 8. § [Reglamento de Evaluación y Certificación de Seguridad de Tecnologías de la Información](#)
- 9. § [Comité de Seguridad de los Sistemas de Información de la Seguridad Social](#)
- 10. § [Comité de Seguridad de las Tecnologías de la Información](#)
- 11. § [Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica](#)
- 12. § [Real Decreto-ley de seguridad de las redes y sistemas de información](#)
- 13. § [Ley reguladora del Centro Nacional de Inteligencia](#)
- 14. § [Ley Orgánica reguladora del control judicial previo del Centro Nacional de Inteligencia](#)
- 15. § [Ley sobre secretos oficiales](#)
- 16. § [Desarrollo de las disposiciones de la Ley sobre Secretos Oficiales](#)
- 17. § [Ley Orgánica de los estados de alarma, excepción y sitio](#)
- 18. § [Ley de Secretos Empresariales](#)
- 19. § [Estrategia Nacional de Ciberseguridad 2019](#)

INFRAESTRUCTURAS CRÍTICAS

- 20. § [Ley que establece medidas para la protección de las infraestructuras críticas](#)
- 21. § [Reglamento de protección de las infraestructuras críticas](#)
- 22. § [Contenidos de Planes de Seguridad del Operador y de Planes de Protección Específicos](#)

NORMATIVA DE SEGURIDAD

- 23. § [Servicios Centrales y Periféricos de la Dirección General de la Policía](#) (parcial)
- 24. § [Ley Orgánica de protección de la seguridad ciudadana](#)
- 25. § [Ley de Seguridad Privada](#)
- 26. § [Reglamento de Seguridad Privada](#)

EQUIPO DE RESPUESTA A INCIDENTES DE SEGURIDAD

- 27. § [Ley de servicios de la sociedad de la información y de comercio electrónico](#) (parcial)
- 28. § [Centro Criptológico Nacional](#)
- 29. § [Organización básica de las Fuerzas Armadas](#) (parcial)
- 30. § [Desarrollo de la organización básica del Estado Mayor de la Defensa](#) (parcial)

PROTECCIÓN DE DATOS

- 46. § [Ley Orgánica de Protección de Datos Personales y garantía de los derechos digitales](#)
- 47. § [Reglamento de la Ley Orgánica de protección de datos de carácter personal](#)
- 48. § [Reglamento Europeo relativo a protección en el tratamiento de datos personales](#)

RELACIONES CON LA ADMINISTRACIÓN

- 49. § [Ley del Procedimiento Administrativo Común de las Administraciones Públicas](#) (parcial)
- 50. § [Ley de Régimen Jurídico del Sector Público](#) (parcial)

TELECOMUNICACIONES Y USUARIOS

- 31. § [Ley de servicios de la sociedad de la información y de comercio electrónico](#)
- 32. § [Medidas contra el tráfico no permitido y el tráfico irregular con fines fraudulentos](#)
- 33. § [Distintivo público de confianza en los servicios de la sociedad de la información](#)
- 34. § [Ley de acceso electrónico de los ciudadanos a los Servicios Públicos](#)
- 35. § [Desarrollo parcial de la Ley de acceso electrónico de los ciudadanos a los servicios públicos](#)
- 36. § [Ley reguladora de determinados aspectos de los servicios electrónicos de confianza](#)
- 37. § [Expedición del documento nacional de identidad y sus certificados de firma electrónica](#)
- 38. § [Ley General de Telecomunicaciones](#)
- 39. § [Reglamento sobre el uso del dominio público radioeléctrico](#)
- 40. § [Protección del dominio público radioeléctrico](#)
- 41. § [Ley de conservación de datos relativos a comunicaciones electrónicas y redes públicas](#)
- 42. § [Formato de entrega datos conservados por los operadores](#)

Constitución

Artículo 18

Se garantiza el derecho al honor, a la intimidad personal y familiar y a la propia imagen.

El domicilio es inviolable. Ninguna entrada o registro podrá hacerse en él sin consentimiento del titular o resolución judicial, salvo en caso de flagrante delito.

Se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial.

La ley limitará el uso de la informática para garantizar el **honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos**.

Artículo 17

1. Toda persona tiene derecho a la libertad y a la seguridad. [...]

CÓDIGO PENAL

Artículo 202.

1. El particular que, sin habitar en ella, entrare en morada ajena o se mantuviere en la misma contra la voluntad de su morador, será castigado con la pena de prisión de seis meses a dos años.

2. Si el hecho se ejecutare con violencia o intimidación la pena será de prisión de uno a cuatro años y multa de seis a doce meses.

Artículo 197 bis.

1. El que por cualquier medio o procedimiento, vulnerando las **medidas de seguridad establecidas** para impedirlo, y **sin estar debidamente autorizado**, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, será castigado con pena de prisión de seis meses a dos años.



CÓDIGO PENAL

Artículo 264.

1. El que por cualquier medio, sin autorización y de **manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos**, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave, será castigado con la pena de prisión de seis meses a tres años. [...]

2.ª Haya ocasionado daños de especial gravedad o afectado a un número elevado de sistemas informáticos.[...]

Artículo 197.

2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, **utilice o modifique, en perjuicio de tercero**, datos reservados de carácter personal o familiar de otro que se **hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado**. Iguales penas se impondrán a quien, sin estar autorizado, **acceda por cualquier medio a los mismos y a quien los altere** o utilice en perjuicio del titular de los datos o de un tercero.



CÓDIGO PENAL

Artículo 197.

1. El que, **para** descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, **se apodere** de sus papeles, cartas, **mensajes de correo electrónico o cualesquiera otros documentos o efectos personales**, **intercepte** sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses.

Artículo 197 bis.

2. El que mediante la utilización de artificios o instrumentos técnicos, y sin estar debidamente autorizado, **intercepte transmisiones no públicas de datos informáticos** que se produzcan desde, hacia o dentro de un sistema de información, incluidas las emisiones electromagnéticas de los mismos, será castigado con una pena de prisión de tres meses a dos años o multa de tres a doce meses.



CÓDIGO PENAL

Artículo 264. [...]

5.ª El delito se haya cometido utilizando alguno de los medios a que se refiere el artículo 264 ter.

Artículo 264 ter.

[...] sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los dos artículos anteriores:

- a) un programa informático, concebido o adaptado principalmente para cometer alguno de los delitos a que se refieren los **dos artículos anteriores**; o
- b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.

Artículo 197 ter.

[...]sin estar debidamente autorizado, produzca, adquiera para su uso, importe o, de cualquier modo, facilite a terceros, con la intención de facilitar la comisión de alguno de los delitos a que se refieren los **apartados 1 y 2 del artículo 197 o el artículo 197 bis**:

- a) un programa informático, concebido o adaptado principalmente para cometer dichos delitos; o
- b) una contraseña de ordenador, un código de acceso o datos similares que permitan acceder a la totalidad o a una parte de un sistema de información.



CÓDIGO PENAL

Artículo 264.

[...]

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante la **utilización ilícita de datos personales** de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero.

Username :

Password :

Artículo 401.

El que usurpare el **estado civil** de otro será castigado con la pena de prisión de seis meses a tres años.

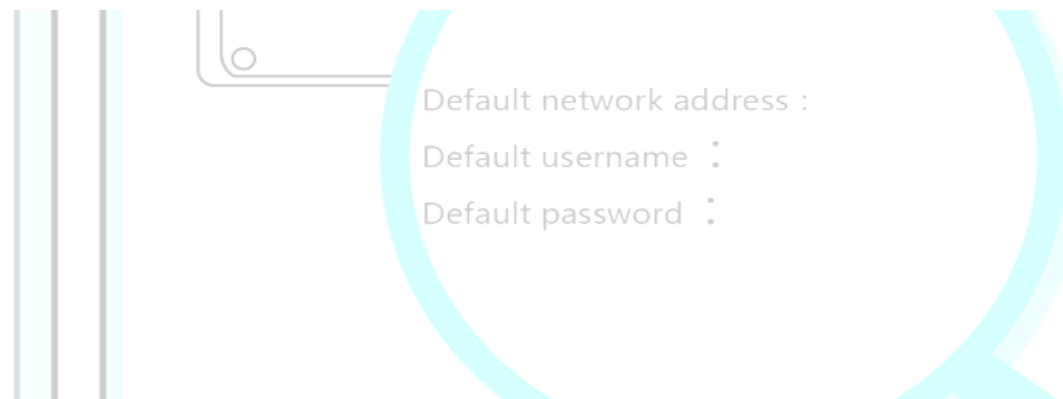
Artículo 403.

1. *El que ejerciere actos propios de una profesión sin poseer el correspondiente título académico expedido o reconocido en España de acuerdo con la legislación vigente, incurrirá en la pena de multa de doce a veinticuatro meses. Si la actividad profesional desarrollada exigiere un título oficial que acredite la capacitación necesaria y habilite legalmente para su ejercicio, y no se estuviere en posesión de dicho título, se impondrá la pena de multa de seis a doce meses.*

2. [...] :

a) *Si el culpable, además, se atribuyese públicamente la cualidad de profesional amparada por el título referido.*

b) *Si el culpable ejerciere los actos a los que se refiere el apartado anterior en un local o establecimiento abierto al público en el que se anunciare la prestación de servicios propios de aquella profesión.*



Artículo 264 bis.

1. Será castigado con la pena de prisión de seis meses a tres años el que, **sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático** ajeno:

- a) realizando alguna de las conductas a que se refiere el **artículo anterior**;
- b) **introduciendo o transmitiendo datos**; o
- c) **destruyendo, dañando, inutilizando, eliminando o sustituyendo un sistema informático**, telemático o de almacenamiento de información electrónica.

Si los hechos hubieran **perjudicado de forma relevante la actividad normal** de una empresa, negocio o de una Administración pública, se impondrá la pena en su mitad superior, pudiéndose alcanzar la pena superior en grado.

2. Se impondrá una pena de prisión de tres a ocho años y multa del triplo al décuplo del perjuicio ocasionado, cuando en los hechos a que se refiere el apartado anterior hubiera concurrido alguna de las circunstancias del apartado 2 del artículo anterior.

3. Las penas previstas en los apartados anteriores se impondrán, en sus respectivos casos, en su mitad superior, cuando los hechos se hubieran cometido mediante **la utilización ilícita de datos personales de otra persona para facilitarse el acceso al sistema informático o para ganarse la confianza de un tercero**.

CÓDIGO PENAL



Artículo 201.

1. Para proceder por los delitos previstos en este capítulo **será necesaria denuncia de la persona agraviada o de su representante legal**. Cuando aquélla sea menor de edad, persona con discapacidad necesitada de especial protección o una persona desvalida, también podrá denunciar el Ministerio Fiscal.

¿Los agraviados puede ser conscientes?



<https://www.osi.es/es>

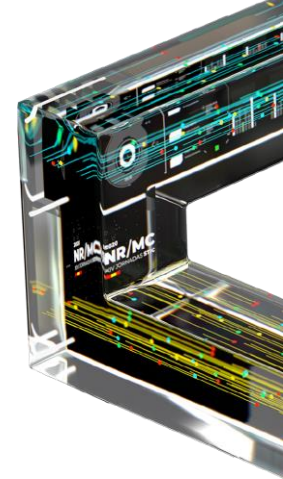
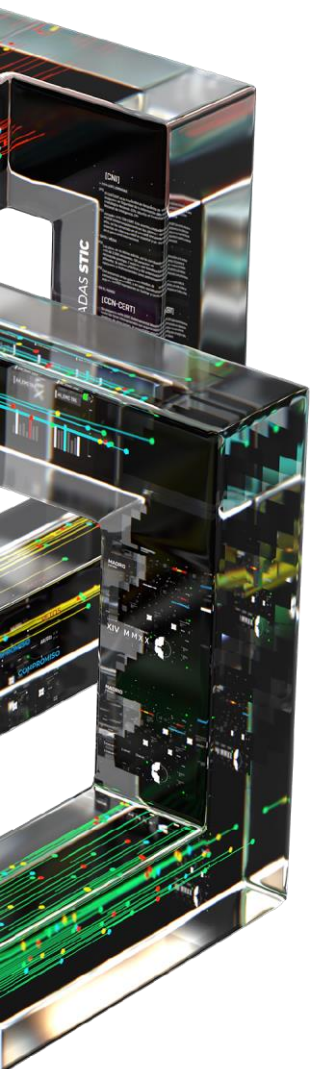
PERSEGUIBILIDAD...

PRUEBA



#XIVJORNADASCCNCERT





MUCHAS GRACIAS

#XIVJORNADASCCNCERT