INSTITUTO NACIONAL DE CIBERSEGURIDAD

GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

MÓDULO 10

Canales de ayuda y de denuncia

ÍNDICE

1. Canales de ayuda 4

2. Canales de denuncia 12

2.1 ¿De qué canales de denuncia disponemos y qué podemos denunciar? 12

1. Canales de ayuda

La llegada de la era digital ha traído consigo innumerables avances para la ciudadanía en lo que respecta al ocio, relaciones con las administraciones públicas, profesionales, académicos, etc., así como el impacto en los modelos de negocio de las empresas y profesionales y los cambios de hábitos en los procedimientos de gestión y tramitación.

Estas transformaciones vertiginosas han traído consigo cambios en nuestra concepción sobre la seguridad en la Red y en la manera en la que debemos navegar por ella. La ciberseguridad es, hoy en día, uno de los temas más importantes en lo que respecta a las garantías en los derechos y libertades de las personas físicas, el análisis de las vulnerabilidades de los activos de las empresas y la seguridad de las estructuras críticas del Estado.

La seguridad 100% online es un concepto teórico difícilmente alcanzable; aun así, debemos conocer los mecanismos y canales de ayuda que existen para poder afrontar los riesgos asociados al propio tratamiento de nuestros datos en Internet.

En nuestro país disponemos de diferentes entidades públicas, agencias y observatorios encargados de acercar el concepto de la ciberseguridad a la ciudadanía, empresas y a profesionales. Además de la labor pedagógica, en lo que respecta a los riesgos de navegar por Internet, disponen de una serie de canales de ayuda con la misión de poder ayudar a resolver problemas técnicos, legales, psicosociales e inquietudes en general en materia de ciberseguridad.

Las entidades a las que podemos dirigirnos para pedir ayuda en materia de ciberseguridad son:

1. **AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS (AEPD)**

¿En qué podemos ayudarte?

- AYUDA A LA CIUDADANÍA

Dentro de la legislación española y el Reglamento Europeo ya mencionado en módulos anteriores, se recogen los derechos que tenemos los ciudadanos en lo que respecta al tratamiento de nuestros datos, es decir, somos dueños de nuestros datos y debemos conocer lo que hacen las entidades, profesionales y terceras personas con ellos en Internet. La Agencia Española de Protección de Dados (AEPD) protege tus derechos de acceso, rectificación, limitación, oposición, supresión (‘derecho al olvido’), portabilidad y oposición al tratamiento

de decisiones automatizadas. Este canal de la AEDP te ayuda a saber cuándo debes ejercer tus derechos, cuáles son y qué formularios oficiales debes utilizar.

Debemos tener en cuenta que, en primer lugar, hay que ponerse en contacto con la entidad responsable para ejercer esos derechos. En el caso de que esa entidad no responda en un plazo establecido, o consideramos que la respuesta no es adecuada, se puede interponer una reclamación en la AEPD.

Podemos hacerlo a través de dos vías:

- *A través de la sede electrónica.*
- *Llamando al teléfono 900 293 183.*

Si necesitamos ayuda, o si nuestra consulta se refiere a un asunto competencia de alguna de las autoridades autonómicas que disponen de servicios propios en materia de protección de datos, podemos contactar con estos directamente:

- País Vasco
- Cataluña
- Andalucía

➢ AYUDA A LOS MENORES

Debemos poner especial atención con la recogida, tratamiento, cesión y destrucción de datos de menores. Cabe recordar que los menores de 14 años requieren obligatoriamente el consentimiento de sus padres o tutores legales para el tratamiento de sus datos. Mientras que, entre los 14 y los 18 años, podrán consentir el tratamiento de sus datos personales, salvo que exista una ley o norma que exija la asistencia de padres o tutores legales, como puede ser el caso de la asistencia clínica psiquiátrica, por ejemplo.

Podemos usar varias vías de contacto para resolver cuestiones y solicitar ayuda sobre menores:

- Enviando un correo electrónico a canaljoven@aepd.es.
- Por teléfono al 900 293 621.
- Por WhatsApp al 616 172 204.

Además, disponemos de materiales de ayuda en lo que respecta a cuestiones relacionadas con los menores en el enlace: https://www.tudecideseninternet.es/aepd/. Aquí encontraremos información sobre el tratamiento de datos en los centros educativos, cómo controlar las publicaciones en Internet, recomendaciones sobre el acoso digital a menores, mecanismos de control parental o el mal uso de las redes sociales por los menores.

- AYUDA A LOS RESPONSABLES DE TRATAMIENTO:

Debemos recordar que la figura del responsable del tratamiento de datos es la persona física o jurídica o autoridad pública que decide sobre el tratamiento de datos personales.

Esta figura jurídica debe ser garante en los cumplimientos legislativos para así garantizar los derechos y las libertades de las personas físicas.

Para ello, se encuentran a disposición de los responsables varias herramientas de ayuda:

- Facilita RGPD: es la ***herramienta*** proporcionada por la Agencia para facilitar la ***adecuación*** al Reglamento General de Protección de Datos en aquellos tratamientos de riesgo bajo. Cumplimentando el formulario con los datos de tu actividad, la herramienta arroja un paquete de documentos para su uso. Esos documentos deberán utilizarse en las actividades de tratamiento que desempeñe la entidad o profesional, como por ejemplo, en la toma de datos a clientes, contratación de servicios con terceros, carteles de vídeo vigilancia, etc.
- Gestiona RGPD: es un asistente para la realización de análisis de riesgos y evaluación de impacto.
- Facilita EMPRENDE: en el caso de ser una persona emprendedora del sector tecnológico, se puede utilizar esta herramienta como ayuda al cumplimiento legislativo en materia de protección de datos
- Comunica-Brecha RGPD: en los casos en los que se tenga constancia o sospechas de haber sufrido una brecha de seguridad en la que se han vulnerado los sistemas de seguridad, se puede utilizar esta herramienta de ayuda que nos indicará los pasos a seguir, la tipificación de la brecha, la comunicación a los afectados, etc.

- Evalúa-Riesgo RGPD: es una herramienta de ayuda para determinar si hay que realizar una evaluación de impacto y gestión de riesgos.
- Canal del DPD: para aquellos profesionales que desempeñan la función de Delegado de Protección de Datos, está a su disposición este canal de ayuda para la realización de consultas directas a la Agencia.

Además de todas estas herramientas, existen a disposición del usuario para su consulta y descarga, un listado de guías e infografías de interés en las que se abordan con mayor profundidad temas concretos relacionados con el tratamiento de los datos, sus riesgos, recomendaciones, videovigilancia, transferencias internacionales, compras seguras por Internet, etc.

2. INSTITUTO NACIONAL DE CIBERSEGURIDAD (INCIBE)

INCIBE cuenta con un canal de ayuda enfocado a resolver y aclarar cuestiones a ciudadanos, menores, empresas y profesionales, en lo que respecta al uso de Internet y las tecnologías, así como recomendaciones en materia de ciberseguridad.

Un equipo multidisciplinar de expertos asesora y atiende las cuestiones en horario de 8 a 23h los 365 días del año, de manera gratuita y confidencial. Los canales de contacto disponibles son:

- Atención telefónica llamando al 017.
- WhatsApp
- Telegram
- Formulario web
- Atención presencia en León (bajo cita previa)

Por cualquiera de las vías mencionadas, nos pueden ayudar sobre casos de suplantación de identidad, ciberacoso, estafa digital, control parental y acceso de menores, entre otros.

Además, INCIBE-CERT, como centro de respuesta a incidentes de seguridad de referencia para los ciudadanos y entidades de derecho privado en España, operado por INCIBE, tiene dentro de sus funciones:

- ofrecer soporte técnico y proporcionar información para ayudar en la resolución de los incidentes de ciberseguridad dentro su ámbito de actuación
- emplear técnicas de detección temprana de incidentes, notificando a los afectados, para que puedan tomar medidas,
- mantener el contacto con los proveedores de Internet y otros CERT (nacionales e internacionales), notificando el incidente, a fin de que se puedan tomar medidas que limiten o impidan su continuidad.

Cualquier ciudadano puede reportar un incidente de seguridad siguiendo las pautas especificadas en : Respuesta a incidentes.

3. OFICINA DE SEGURIDAD DEL INTERNAUTA (OSI)

La Oficina de Seguridad del Internauta de INCIBE (www.incibe.es/ciudadania) tiene como principal misión la de proporcionar información y soporte para resolver incidencias en materia de seguridad que puedan surgir al navegar en entornos digitales.

Gracias a los talleres, guías y recursos de descarga de la propia web de OSI, se pretende ayudar a concienciar en la importancia que tiene navegar seguro por Internet, para así evitar riesgos que contravengan nuestros intereses personales, eliminando las vulnerabilidades que puedan existir en los procesos telemáticos.

Para favorecer esta circunstancia, desde la OSI se ofrecen:

- Guías, consejos y recomendaciones de ciberseguridad sobre temáticas básicas de ciberseguridad: configuración de dispositivos, copias de seguridad, conexiones seguras, privacidad, compras online, etc.
- Talleres sobre ciberseguridad

- Herramientas para proteger tus dispositivos (PC, *smartphone*, *tablet* etc.) abordando asuntos como la seguridad y protección en los accesos a Internet, copias de seguridad, cifrado y gestor de contraseñas, antivirus, entre otros.
- Tests de autoevaluación relacionados con la ciberseguridad: cuentas seguras *online*, compras seguras, cómo identificar fraudes, redes wifi seguras, noticias falsas, etc.
- Juegos para aprender y poner a prueba de una manera lúdica aspectos importantes de ciberseguridad.

4. OBSERVATORIO NACIONAL DE TECNOLOGÍA Y SOCIEDAD (ONTSI)

La ONTSI tiene la misión de generar conocimiento y valor en las instituciones públicas, en el desarrollo empresarial y el saber de la ciudadanía en lo que respecta al desarrollo tecnológico y el apoyo de los recursos digitales en la economía, los servicios públicos, el empleo, los derechos y libertades de los ciudadanos, la seguridad en la Red y la igualdad en el acceso a los recursos tecnológicos.

Para ello, sirve de ayuda generando estudios, realizando publicaciones, indicadores, analizando políticas, estrategias y tendencias, identificando buenas prácticas en ciberseguridad y, además, procesa, difunde e intercambia conocimiento a través de las siguientes herramientas.

- Publicaciones
- Indicadores
- Biblioteca digital
- Servicio de alertas en el que puedes suscribirte y recibir novedades en materia de ciberseguridad.

5. CENTRO CRIPTOLÓGICO NACIONAL (CCN-CERT)

Se trata de la entidad competente para incidentes que afecten a entidades públicas y tiene el objetivo de mejorar la ciberseguridad en España. Es el centro de alerta y respuesta que ayuda y responde rápida y eficientemente ante los ciberataques, así como a afrontar de forma activa las ciberamenazas.

Aunque está muy focalizado al ámbito de las alertas y mecanismos de respuesta frente a ciberataques a las estructuras públicas, también tiene función de ayuda al ciudadano, empresas y profesionales mediante:

- Guías técnicas para desarrollos empresariales y de divulgación general en temas como la seguridad en la telefonía móvil, seguridad en Windows, seguridad en el uso del *Bluetooth*, seguridad en entornos y aplicaciones web, etc.
- Formación: mediante la plataforma ÁNGELES que permite realizar itinerarios formativos en materia de ciberseguridad.
- Soluciones y ayuda en ciberseguridad: se trata de medidas que garantizan la seguridad de los sistemas y ayudan para la mejora de la gestión de la ciberseguridad de una organización, permitiendo una defensa eficiente frente a ciberataques.

6. ASOCIACIÓN DE INTERNAUTAS

La asociación pretende defender los intereses de los internautas frente a las compañías de telecomunicaciones, proveedores y empresas informáticas, así como generar contenido que pueda ayudarles en los procesos telemáticos y en lo que respecta a la seguridad de esos procesos.

Entre otras actuaciones disponen de:

1. Sistema de ayuda a la comprobación de la fiabilidad de la contraseña.
2. Sistema generador de contraseñas.

7. ASOCIACIÓN DE USUARIOS EN INTERNET

Asociación que pretende promover el desarrollo de Internet, de la Sociedad de la Información y de las nuevas tecnologías, así como ayudar a la ciudadanía en lo que respecta a la defensa de los intereses y derechos de los usuarios en Internet. Además, tiene como objetivo el fomento del buen uso de Internet y de su aplicación en el ámbito del hogar, de la empresa y profesionales.

La Asociación de Usuarios de Internet se ha unido al Pacto Digital para la Protección de las Personas. Esta iniciativa lanzada por la Agencia Española de Protección de Datos (AEPD) persigue promover la privacidad a través de políticas de sostenibilidad, compatibilizando el derecho fundamental a la protección de datos con la innovación, la ética y la competitividad empresarial.

8. AUTOCONTROL

Asociación centrada en los procesos de verificación y validación de la publicidad para que sea conforme a los preceptos legales.

Como ayuda, ofrecen asesoramiento a las empresas a través de herramientas que proporcionan asistencia técnica y jurídica sobre el uso de las *cookies*, asesoramiento ético y legal y sobre cumplimiento normativo en materia publicitaria en las páginas web. Además, disponen de cursos y seminarios relacionados con la normativa publicitaria en Internet.

2. Canales de denuncia

En la actualidad, son muchos los tipos de fraudes que ciudadanos, empresas y profesionales podemos sufrir en los entornos digitales. Afortunadamente, gracias a los avances tecnológicos, así como a las labores de comunicación y difusión de la información por parte de las administraciones públicas y de entidades privadas, la concienciación y los mecanismos de respuesta que tenemos en la actualidad son más efectivos y contundentes a la hora de reportar o defendernos de un acto irregular en Internet.

Aun así, se dan circunstancias complejas en las que se atenta directamente contra los derechos y libertades de las personas físicas, así como los intereses de las empresas y profesionales. Es por ello que, en España, disponemos de una serie de canales de denuncia que nos permiten poner en conocimiento actos o conductas que pudieran ser delictivas. Es más, a veces se comenten delitos (por ejemplo, en las redes sociales o con aplicaciones de mensajería instantánea) sin saber que se están cometiendo. La falta de formación e información sobre lo que se puede o no hacer en los entornos digitales deja al descubierto multitud de delitos que deben ser perseguidos.

2.1 ¿De qué canales de denuncia disponemos y qué podemos denunciar?

A continuación, se detallan los principales canales que existen en la actualidad:

- La **Policía Nacional** dispone de una Brigada Central de Investigación Tecnológica (BCIT) encargada de tramitar, perseguir y erradicar las conductas delictivas on-line. En su página web se recogen las siguientes actuaciones que se pueden denunciar (https://www.policia.es/_es/tupolicia_conocenos_estructura_dao_cgpoliciajudicial_bcit.php):
  - *"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".*

¿Dónde podemos denunciar?

1. Mediante el formulario de contacto en el que aparece un listado de delitos para seleccionar:

   https://www.policia.es/_es/colabora_informar.php?strTipo=CGPJDT

2. Si estás en Cataluña, puedes hacerlo a través de la Unidad Central de Delitos Informáticos de los Mossos d'Esquadra en este enlace:

   https://mossos.gencat.cat/ca/temes/Internet-xarxes-socials-i-aplicacions/

3. Si estás en Navarra, puedes hacerlo a través del Grupo de Apoyo Tecnológico de la Policía Foral de Navarra en este enlace:

   https://www.navarra.es/es/tramites/on/-/line/Denuncias-penales-o-administrativas

4. Si estás en el País Vasco, puedes hacerlo a través de la Sección Central de Delitos en Tecnologías de la Información (SCDTI) de la Ertzaintza en este enlace:

   https://www.ertzaintza.euskadi.eus/lfr/web/ertzaintza/interposicion-denuncia

- La **Guardia Civil** (https://www.guardiacivil.es/es/servicios/index.html) cuenta con un grupo específico denominado Grupo de Delitos Telemáticos (GDT) encargado de detectar y perseguir cualquier delito realizado en entornos telemáticos así como dar trámites a las denuncias que se puedan interponer por parte de ciudadanos, empresas y profesionales. Este equipo especializado se refuerza con otros Equipos de Investigación Tecnológica

repartidos por distintas provincias para dar cabida a las investigaciones presenciales por temas de estafas online, piratería, etc.

¿Qué podemos denunciar?

- Usurpaciones de identidad.
- Amenazas y coacciones mediante escritos, vídeos o audios.
- Accesos ilícitos a sistemas informáticos o a información confidencial.
- Bloqueo de sistemas informáticos o bases de datos
- Revelación y difusión de secretos atentando a nuestra intimidad.

¿Dónde podemos denunciar?

Mediante Sede Electrónica: https://www.guardiacivil.es/es/servicios/denuncias/denuncia_electronica/index.html

Debemos consignar todos los datos identificativos, que luego se verificarán mediante la exhibición del DNI, NIE o Pasaporte.

A continuación, debemos exponer la cronología de lo sucedido aportando documentación, pantallazos, reseñas digitales, etc. Debemos ser concisos y usar argumentario claro y entendible para así facilitar la labor investigadora.

- La **Agencia Española de Protección de Datos** (AEPD) dispone de un canal prioritario (https://www.aepd.es/es/canalprioritario) cuya misión es la de poder solicitar la retirada de publicaciones en Internet hechas sin autorización de las personas afectadas, que contengan fotografías, videos o audios de contenido sexual o violento.

  https://sedeagpd.gob.es/sede-electronica-web/vistas/formNuevaReclamacion/nuevaReclamacion.jsf?QID=Q600&ce=0

  Si, por otro lado, eres menor de 18 años y tienes conocimiento de que se está publicando en Internet contenido audiovisual de carácter sexual y/o violento sin la autorización de la persona afectada, se puede contactar al través del sistema #PuedesPararlo:

https://sedeagpd.gob.es/sede-electronica-web/vistas/formCanalPrioritarioMenores/canalprioritario.jsf

Si estás recibiendo comunicaciones relacionadas con publicidad y/o mercadotecnia, primero debes contactar con la persona o entidad ejerciendo tu derecho de oposición para no recibir más comunicaciones comerciales o tu derecho de supresión en caso no tener relación vinculante con ese proveedor o considerar un tratamiento ilícito. Si no responden favorablemente en el plazo legal conferido de 1 mes o si la respuesta no es la satisfactoria, para dejar de recibir publicidad, puedes interponer una reclamación directamente en la Sede Electrónica de la AEPD.

https://sedeagpd.gob.es/sede-electronica-web/vistas/infoSede/tramitesCiudadano.jsf

Los sistemas de captación de imágenes y sonido (videocámaras) han de ajustarse a las previsiones contenidas en la normativa de protección de datos. Si se considera que una videocámara no está debidamente señalizada, se realizan grabaciones en el ámbito laboral, se disponen en zonas de tránsito, etc. y se ha contactado con el propietario de las mismas y no se ha obtenido respuesta, podremos interponer una reclamación también a través de la sede electrónica de la Agencia Española de Protección de Datos en el enlace anterior.

- **AUTOCONTROL** dispone de un canal para interponer una reclamación por motivos publicitarios ante el Sistema de Tramitación de Reclamaciones por Protección de Datos y Publicidad:
  - Si eres consumidor final (gratuito).

    https://privada.autocontrol.es/servicio/reclamacion/noregistrado/create/reclamacion
  - Si eres una entidad (debes ser socio o estar suscrito).

    https://privada.autocontrol.es/login
  - Protección de Datos: centrado exclusivamente en reclamaciones relacionadas con el uso de los datos en el ámbito publicitario con las empresas de Telecomunicaciones.

    https://www.autocontrol.es/reclamacion-proteccion-datos/

- El **Instituto Nacional de Ciberseguridad** (**INCIBE)** tiene entre sus funciones la de actuar como Equipo de Respuesta de Seguridad Informática (CERT) prestando servicios frente a incidentes de seguridad que pueden ser notificados por empresas y ciudadanos. El servicio se ofrece 24h al día los 7 días de la semana durante todo el año. Para ello, existe un buzón en el que se pueden trasladar casos relacionados con estafas on-line, instalación de *software* malicioso, bloqueo de bases de datos, etc., tanto si eres ciudadano como si eres empresa.

  - incidencias@incibe-cert.es
  - Formulario: https://www.incibe-cert.es/notificaciones

- El **CCN-CERT** colabora con todos los organismos públicos y empresas de España en la detección, notificación, evaluación y protocolo de respuesta frente a incidentes de seguridad de la información o ataques a sus sistemas por parte de ciberdelincuentes. Se puede trasladar un incidente por dos vías principales:

  - Por correo electrónico a la dirección incidentes@ccn-cert.cni.es
  - A través del programa LUCÍA https://www.ccn-cert.cni.es/soluciones-seguridad/lucia.html

- La **Oficina de Atención al Usuario de Telecomunicaciones** perteneciente al Ministerio para Transformación Digital y de la Función Pública tiene como misión principal tramitar y resolver controversias que puedan existir entre los usuarios de telecomunicaciones y los operadores.

  Todos los usuarios de telecomunicaciones pueden interponer reclamación mediante: https://usuariosteleco.mineco.gob.es/reclamaciones/Paginas/reclamaciones.aspx o denuncias sobre tarificaciones indebidas: https://usuariosteleco.mineco.gob.es/Paginas/denuncias.aspx

- Las **REDES SOCIALES y SISTEMAS DE MENSAJERÍA INSTANTÁNEA** disponen de mecanismos de denuncia en caso de recibir calumnias, insultos, difusión de contenido sexual o violento, datos de menores, etc. Vamos a destacar las más conocidas:

WhatsApp	En Android, puedes ir a WhatsApp > Más opciones > Ajustes > Ayuda > Contáctanos y en iPhone, puedes ir a WhatsApp > Configuración > Ayuda > Contáctanos. Ahí podremos describir nuestra situación y aportar capturas. Además, podemos seleccionar al usuario que nos molesta y clicar en "Bloquear y Reportar" con la posibilidad de que la plataforma lo elimine de la aplicación. https://www.whatsapp.com/contact/?lang=es&subject=messenger
Facebook	Seleccionas a la persona que te está difamando o la publicación que quieras denunciar. En caso de una publicación a la que quieras denunciar, bastaría con pulsar en los tres puntos que aparecen en la publicación y seleccionas "denunciar anuncio". En caso de seleccionar a la persona que está difamando, pulsa sobre el nombre del perfil y puedes denunciarlo directamente o buscar ayuda y seguir las instrucciones que aparecen en pantalla. Si alguien está publicando contenido violento o indeseado o si está realizando contenido difamatorio sobre tu persona, puedes ir directamente al perfil de esa persona, pulsar en los 3 puntos del límite superior derecho y elegir "denunciar". https://es-es.facebook.com/help/171757096241231
X (Twitter)	La casuística es más amplia y aparecen descritas todas las opciones en el siguiente enlace: https://help.twitter.com/es/safety-and-security/report-abusive-behavior#:~:text=Ve%20al%20post%20que%20deseas,o%20Con%20todos%20en%20X
TIKTOK	En el siguiente enlace aparecen descritas las maneras de denunciar un perfil o un vídeo en concreto: https://support.tiktok.com/es/safety-hc/report-a-problem/report-a-user

Si, por otro lado, estás recibiendo acoso por Internet mediante amenazas, injurias, difamaciones, etc. o eres víctima de un fraude o delito:

- Contacta directamente con la entidad o servicio que esté implicado, tipo red social, foro de opinión, soporte de correo, etc. En general, suele funcionar y dan trámite a la reclamación.
- Dirígete a una Oficina Municipal de Información al Consumidor (OMIC). Su función principal es la de mediar en los conflictos o disconformidades que existan entre los consumidores y los proveedores de bienes y servicios. http://aplicaciones.consumo-inc.es/cidoc/default.aspx
- Denuncia directamente ante las Fuerzas y Cuerpos de Seguridad del Estado siguiendo las indicaciones detalladas con anterioridad.