PLAN COMERCIO SEGURO

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
MINISTERIO DE ECONOMÍA, COMERCIO Y EMPRESA

POLICÍA NACIONAL

ÍNDICE

1 PRESENTACIÓN

En 2024 se cumplen once años desde la puesta en marcha, por la Dirección General de la Policía, del Plan Comercio Seguro, destinado a la mejora, con carácter permanente, de la seguridad del sector comercial español, desde la corresponsabilidad de todas las instituciones públicas y privadas implicadas. Desde sus inicios han contado con la colaboración de la Secretaría de Estado de Comercio.

El carácter estratégico del sector comercial es indiscutible, tanto por su aportación al PIB y al empleo, como por su vertiente social en sus funciones de abastecimiento y de cohesión y vertebración del territorio. Por ello, la mejora de la competitividad del sector es prioritaria. Dentro del Plan de Recuperación, la Secretaría de Estado de Comercio ha movilizado 415 millones de euros en ayudas para mejorar la competitividad del sector comercial español. Además, se ha puesto en marcha la Plataforma Comercio Conectado, punto de encuentro del sector comercial y red de colaboración a nivel nacional que ofrece herramientas para ayudar a los comercios a adaptarse la digitalización y la transición verde; a ello se añaden las convocatorias anuales de los Premios Nacionales de Comercio Interior que premian especialmente la labor del pequeño comercio, y las del Concurso de ideas tecnológicas que premia las soluciones que puedan ser incorporables en cualquiera de los procesos propios de la actividad comercial minorista y por último, el convenio que cada año se firma entre el Ministerio de Economía, Comercio y Empresa y la Cámara Oficial de Comercio, Industria, Servicios y Navegación de España para el desarrollo de programas de apoyo a la competitividad del comercio minorista, que se ejecuta a través de la red de Cámaras.

El desarrollo de la actividad comercial en condiciones de seguridad es importante tanto para los propios comerciantes como para los consumidores. Se trata de un sector clave que presta un servicio esencial pero que es altamente vulnerable por su capilaridad y su alto nivel de exposición, siendo objeto de programas y planes específicos de prevención policial, que cuentan con la participación ciudadana como una pieza fundamental de la seguridad en el comercio.

Poner a disposición del sector recomendaciones y consejos que garanticen la seguridad del servicio y del establecimiento es una iniciativa de gran valor para nuestros comercios.

Amparo López Senovilla
Secretaria de Estado de Comercio

Francisco Pardo Piqueras
Director General de la Policía

Rafael Torres
Presidente de la CEC

2 MEDIDAS DE SEGURIDAD

Existen diversos sistemas y medidas de seguridad destinados a la protección de personas y bienes de los que pueden dotarse los establecimientos en función de los fines de prevención o protección pretendidos. En este sentido, la normativa de seguridad privada contempla como medidas de seguridad las de carácter físico, electrónico, informático, de tipo organizativo o de seguridad personal.

Cuando se disponga de sistemas de seguridad electrónica que se encuentren conectados a una central receptora de alarmas (CRA) o a un centro de control o videovigilancia, estos habrán de ser instalados y mantenidos por empresas de seguridad privada autorizadas por la Dirección General de la Policía o, en su caso, por las administraciones autonómicas correspondientes.

El desarrollo de actividades como la vigilancia y protección de bienes y personas o el transporte de seguridad de objetos valiosos tendrá que ser realizado, en su caso, por empresas de seguridad debidamente autorizadas.

No obstante, como recomendaciones que ayuden a mejorar la seguridad de su establecimiento y faciliten las labores de prevención y posteriores tareas de investigación de delitos, se sugieren las siguientes:

2.1 MEDIDAS DE SEGURIDAD EN EL ESTABLECIMIENTO COMERCIAL

Tenga en cuenta las siguientes

SUGERENCIAS GENERALES:

- No confíe en «supuestos expertos de seguridad».
- Cuando se contraten servicios de instalación de sistemas de seguridad electrónica conectados a una central receptora de alarmas -CRA- o centro de control o videovigilancia, previamente la empresa de seguridad privada debe hacer entrega de un proyecto del sistema.
- Cuando se realicen servicios de vigilancia y protección de bienes y personas o transporte de fondos y objetos valiosos, antes de formalizar el contrato, las empresas de seguridad deberán determinar que el servicio a prestar es acorde a los riesgos estimados.
- Respecto a bienes especialmente valiosos, se aconseja que sean protegidos con medidas de seguridad física (puertas blindadas, cajas fuertes, etc.) y externamente, con medidas de seguridad electrónica, que permitan la detección de los delincuentes.
- Los sistemas de seguridad que registren datos de carácter personal tendrán que cumplir con lo señalado por la normativa específica sobre protección de este tipo de datos y, en su caso, con lo dispuesto por la Ley de Seguridad Privada.
- Es obligatorio informar mediante carteles de la instalación de cámaras de seguridad y que, únicamente, tendrán acceso a estas las personas autorizadas.
- La empresa de seguridad encargada de la conexión de un sistema de seguridad a una CRA le dará las indicaciones para el uso correcto de los sistemas instalados.

- Nunca facilite sus claves. Los delincuentes pueden tratar de averiguar los códigos de desbloqueo de las diferentes medidas interpuestas, con objeto de acceder a su establecimiento.
- Avise inmediatamente a la Policía y siga sus indicaciones si advierte manipulaciones en las medidas dispuestas (cámaras, cerraduras, etc.).
- Revise periódicamente el estado y correcto funcionamiento de los elementos de seguridad (cámaras, volumétricos, grabador de imágenes, etc.)
- En el caso de que ocurra un hecho denunciable, conserve toda la información con la que cuente (imágenes grabadas, números de tarjeta, etc.), avise inmediatamente a la Policía y siga sus indicaciones.
- Confíe en la profesionalidad del personal de seguridad privada -en caso de contar con dicho servicio- porque está avalada por la Policía Nacional mediante las habilitaciones correspondientes

Y DE FORMA MÁS ESPECÍFICA, SIGA LAS SIGUIENTES RECOMENDACIONES:

- Si su establecimiento es susceptible de sufrir «alunizajes», instale medidas específicas preventivas como: bolardos, maceteros grandes, muros medianeros reforzados, cristal de seguridad, verjas metálicas por el interior del escaparate, etc.

Y de forma más específica

SIGA LAS SIGUIENTES INSTRUCCIONES:

- Los «sistemas emisores de humos» impiden la visibilidad dentro del establecimiento, por lo que constituyen un importante elemento disuasorio.
- Instale puertas de seguridad en los accesos peatonales. En el resto de accesos (ventanas, respiraderos, tragaluces, patios interiores, etc.), se recomienda instalar rejas y/o persianas de seguridad.
- Instale, en la medida de lo posible, cerraduras, escudos protectores y bombines de seguridad certificados.
- Instale un sistema de grabación de imágenes acorde a las dimensiones del establecimiento. Se recomienda la grabación de las imágenes en un disco duro situado dentro de una caja o armario de seguridad, cuya capacidad permita conservarlas durante un plazo de 30 días.
- Mejore la calidad, mantenimiento y ubicación de cámaras de CCTV (resolución, enfoque, vías de acceso y zona caja), evitando planos cenitales, contraluces y zonas de poca visibilidad o cuya visión se dificulte por carteles de publicidad, impidiendo la plena identificación de los/as autores/as.
- Confeccione un listado con la marca, modelo y número de serie de las máquinas expendedoras de tabaco, recreativas o de cualquier otro tipo, al objeto de aportarlos en las denuncias en caso de sustracción.
- Instale balizas ocultas entre las mercancías almacenadas que permitan el seguimiento y localización en caso de robo.
- Fuera del horario comercial, sospeche de los saltos de alarma sin motivo aparente. Pueden ser provocados de forma reiterada para que se baje la guardia al pensar que se trata de un fallo en el sistema.

2.2 MEDIDAS DE SEGURIDAD EN LA DISTRIBUCIÓN DE PRODUCTOS

Como es conocido, las medidas de seguridad destinadas a la protección de personas y bienes también pueden incorporarse a los instrumentos de distribución y/o a las propias mercancías.

El ataque a los productos de comercio fuera de lugares cerrados (establecimientos o depósitos de mercancías) suele llevarse a cabo con la sustracción de los mismos a lo largo del itinerario, basándose las modalidades delictivas fundamentalmente:

- En paradas de larga duración, generalmente motivadas por el obligado descanso de los transportistas.

- En paradas cortas, en momentos de carga y descarga.

- Durante el trayecto en marcha, por los conocidos «surferos» o delincuentes que abordan los camiones, vulnerando la caja durante la marcha.

Para paliar este tipo de hechos delictivos **SE RECOMIENDA:**

- Disponer de sistemas que permitan la geolocalización del transporte y de medidas de seguridad que protejan la carga, entre ellas, la conexión del sistema de seguridad del vehículo a una CRA.
- Para el transporte de mercancías muy valiosas, valorar la contratación de empresas de seguridad autorizadas para el desarrollo de esta actividad específica.
- Mantenga una discreción absoluta respecto de la cuantía y valor de los pedidos que realice, de su origen o de la empresa que los transporta.
- Extreme las medidas de seguridad en los centros logísticos y de almacenamiento de mercancías.
- Modifique las rutas y las rutinas -si es transportista-, y en lo posible, no dé a conocer el contenido de su carga.
- Comunique inmediatamente a Policía Nacional y siga sus instrucciones, en caso de observar algo anómalo.

2.3 MEDIDAS DE SEGURIDAD DE LOS PRODUCTOS COMERCIALIZADOS

En relación con los productos o mercancías del establecimiento,

SE RECOMIENDA:

- Instale sistemas de protección mecánicos o electrónicos en los artículos que están en venta.
- Exhiba los objetos muy valiosos dentro de escaparates, vitrinas cerradas con llave o empleando elementos de sujeción, evitando su colocación cerca de los accesos del establecimiento.
- Elabore periódicamente un inventario de la mercancía existente para detectar posibles hurtos.

2.4 MEDIDAS DE SEGURIDAD ORGANIZATIVAS

Si su empresa no tiene un departamento de seguridad,

LAS MEDIDAS a tener en cuenta son:

- Implante normas y procedimientos que permitan minimizar los riesgos de pérdida desconocida.
- Establezca un adecuado nivel de comunicación y formación con los empleados, informando a estos sobre las normas de seguridad y los procedimientos de control de sus actividades en caja, en los almacenes, con los proveedores, etc.
- Identifique claramente si las pérdidas detectadas se deben a errores de gestión, antes de sospechar de hurto interno o externo.

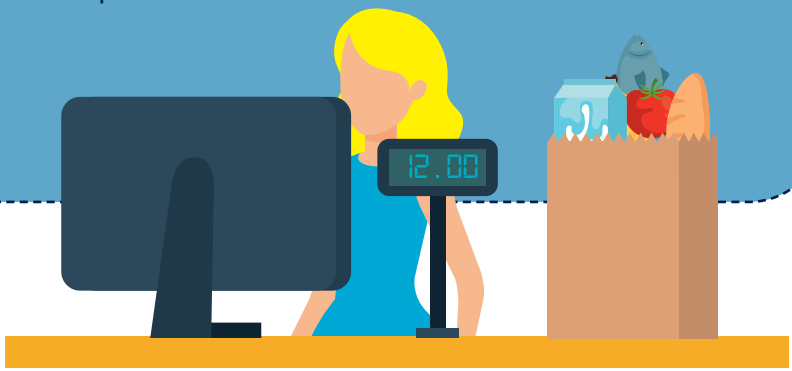
Si se está planteando la constitución de un departamento de seguridad, puede solicitar información a Policía Nacional a través del correo **redazul@policia.es**

2.5 MEDIDAS DE PREVENCIÓN

LAS MEDIDAS a tener en cuenta son:

- Observe si hay personas que permanecen en actitud vigilante o que tomen nota de sus movimientos, así como que entren en su comercio curioseando, haciendo preguntas y con pocas intenciones de comprar.
- Desconfíe de las personas que entren en el establecimiento con un casco de moto puesto, ya que se trata de una práctica habitual para cometer robos en establecimientos comerciales de áreas metropolitanas.
- Manténgase alerta cuando entren en el establecimiento grupos numerosos, ya que pueden actuar de forma coordinada para cometer delitos. Igualmente, preste especial atención cuando el establecimiento se encuentre lleno de clientes, ya que los delincuentes aprovechan esta situación para cometer hurtos.
- Priorice el uso de medios de pago electrónicos para evitar acumular grandes cantidades de dinero en la caja. Fije una cantidad y vaya retirando el exceso de efectivo, reservando lo necesario para garantizar el cambio.
- Deposite el dinero en un lugar seguro (caja fuerte o similar), igual que los objetos de valor.

- Cierre la puerta de acceso al establecimiento antes de hacer caja, realizando esta acción en diferentes horas de manera aleatoria (antes del cierre del establecimiento), acompañado por alguien -si es posible- y donde el público no pueda verlo.
- Mantenga especial atención a los productos que tengan mayor valor y sean de fácil reventa, sobre todo en las temporadas en las que se dispara el consumo.
- Asegúrese de que, durante sus horas de cierre, no ha quedado nadie ajeno al establecimiento en su interior (lavabos, almacén, oficina, etc.).
- Advierta a los comerciantes de los alrededores, asociaciones y gremios profesionales sobre *modus operandi*, características de autores, etc. para que estén precavidos. De esta manera, se podrán evitar hechos ilícitos similares en otros comercios.
- Desconfíe de quienes, sin previo aviso, se personen a revisar o mantener instalaciones, como empleados de empresas de servicios. De producirse el aviso previo, confirme mediante llamada telefónica a la empresa instaladora/suministradora, con especial atención a las empresas de instalación de redes de Internet.



2.6 MEDIDAS DE SEGURIDAD EN LA GESTIÓN DE FONDOS Y SISTEMAS DE PAGO

Si su empresa no tiene un departamento de seguridad,

LAS MEDIDAS a tener en cuenta son:

- Mantenga actualizados los terminales punto de venta (TPV) para que la información que se incluya en la transacción comercial sea segura.
- Recuerde que existen herramientas (*software*, etc.) y aplicaciones para el TPV, web, *smartphone*, etc. que pueden detectar patrones de compra inusuales.
- Asegúrese de que los medios y las pasarelas de pago se contraten con entidades y empresas bancarias reconocidas.
- Recuerde que las tarjetas son de uso personal e intransferible.
- Sospeche de las personas que intenten ocultar su imagen, ya que podrían tratar de evitar su identificación. Conocer a los clientes es una forma de protección contra el fraude.

- Desconfíe de las compras compulsivas o muy abundantes donde solo prima el valor de los objetos.
- No efectúe la operación si duda de su legalidad. Si es posible, avise discretamente a la Policía Nacional o a su servicio de seguridad, evitando en todo momento la confrontación con la persona.

En cuanto al dinero en efectivo,

LAS MEDIDAS a tener en cuenta son las siguientes:

- En relación con los BILLETES, es recomendable disponer de detectores de billetes falsos y/o de otros medios o dispositivos similares.
- En relación con las MONEDAS, compruebe que se trata de monedas de curso legal ya que existen monedas de otros países con una apariencia muy similar a los euros.

A la hora de realizar el ingreso en efectivo en el banco o caja,

TENGA EN CUENTA lo siguiente:

- Escoja una oficina bancaria próxima al establecimiento.
- Evite llevar mucho dinero en una única entrega a las entidades bancarias, es preferible efectuar varios ingresos para evitar llevar la totalidad de la recaudación.
- No realice el ingreso siempre el mismo día ni a la misma hora, evitando rutinas e impidiendo que los delincuentes dispongan de pautas que les faciliten cometer el delito.
- Para evitar tirones, reparta el dinero en varios lugares de sus ropas o pertenencias. Procure no llevar el dinero en bolsas de mano o bandoleras colgadas del hombro, sino en bolsillos interiores de la ropa.
- Durante el trayecto, evite hablar con personas desconocidas y manténgase atento a la presencia de personas con actitud vigilante, que le observen.
- Recuerde que, en función de la cantidad, el transporte de fondos es una actividad reservada a las empresas de seguridad privada habilitadas para ello.

¿QUÉ HACER SI SOSPECHA QUE EL BILLETE ES FALSO?

- No aceptarlo, retenerlo y avisar a la Policía Nacional o a su servicio de seguridad. Eluda, en cualquier caso, el enfrentamiento con la persona, evitando riesgos y/o discusiones cuando le informe de que el billete podría ser falso y pudiera haber sido víctima de una estafa.
- No oponerse. Si la persona quiere irse del establecimiento sin esperar la llegada de la Policía, fíjese en sus rasgos característicos, ropa cualquier otro detalle (descripción física, tatuajes, cicatrices, acento, etc.) y/o vehículos, para facilitarlos posteriormente a la Policía.

¿QUÉ HACER CON UN BILLETE FALSO?

- Ponga en conocimiento de la Policía, mediante una denuncia, que ha recibido un billete falso y entréguelo en comisaría.
- No se desprenda del billete falso intentando pagar con él, ya que estaría incurriendo en una infracción penal.

2.7 MEDIDAS DE SEGURIDAD EN EL COMERCIO ELECTRÓNICO

La Policía Nacional, junto con la Agencia Española de Protección de Datos (AEPD), Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN) y el Instituto Nacional de Ciberseguridad (INCIBE) ha elaborado una guía y unas fichas de compra segura en internet, sobre buenas prácticas dentro del comercio electrónico, que resultan de utilidad, no solo a los ciudadanos como consumidores y usuarios de los servicios de comercio *online*, sino también a las empresas que desarrollan su actividad en este ámbito.

Es posible acceder a las mismas en **www.policia.es** siguiendo la ruta **COLABORA -CONSEJOS DE SEGURIDAD- COMERCIO SEGURO**

INCIBE dispone en su página web de diversas soluciones de seguridad que pueden ser de interés para las PYMES y **PUEDEN CONSULTARSE EN LOS SIGUIENTES ENLACES:**

https://www.incibe.es/empresas/guias/guia-ciberseguridad-comercio-electronico

https://www.incibe.es/empresas/que-te-interesa/protege-tus-clientes

https://www.incibe.es/empresas/que-te-interesa/desarrollar-cultura-en-seguridad

https://www.incibe.es/empresas/que-te-interesa/fraude-gestion-identidad-online

https://www.incibe.es/empresas/formacion/ciberseguridad-para-micropymes-y-autonomos

Además, con **LAS SIGUIENTES MEDIDAS**
se pretende proteger tanto el negocio como los datos de los clientes:

- Preparación del negocio con la creación de una identidad comercial, identificando lo que se vende y la forma en que se van a realizar los pagos, así como la tramitación de los pedidos en la plataforma con el máximo nivel de seguridad posible.
- Para la creación de una plataforma de comercio electrónico, se deben contratar empresas de servicios web reconocidas y poner atención en los servicios y medidas de seguridad incluidas.
- Si se crea una página web propia, se debe decidir la configuración del sistema de venta *online* o encargar dichos servicios a terceras empresas de reconocido prestigio.
- Desconfíe de comunicaciones que aparentemente proceden de la empresa que gestiona su portal de venta *online* y que faciliten un enlace para acceder a la parte privada del mismo. Podría tratarse de una argucia para captar las credenciales y modificar el portal de ventas sin su consentimiento. Compruebe con la empresa la veracidad del mensaje, utilizando otra vía diferente.
- Para la realización de la venta *online*, cuente con el apoyo de una entidad adquirente que facilite una pasarela de pago en la plataforma, estableciendo el método más idóneo (tarjetas bancarias, transferencias, órdenes de cobro a la entrega, etc.).
- Contrate los medios y pasarelas de pago con entidades bancarias, financieras o de pago reconocidas.
- Estudie con su proveedor de servicios las opciones de seguridad (*software*, contraseñas, *firewall* y antivirus) y cómo mantener actualizada tanto, la página web, como el servidor donde se encuentra alojada.

- Observe las señales de advertencia, teniendo en cuenta que existen herramientas que controlan la actividad comercial y permiten establecer patrones para averiguar si la operativa realizada es genuina o no.
- En la protección contra el fraude hay que conocer a los clientes, identificándolos y autenticando las transacciones, para permitir los pagos con facturas, soluciones prepago y determinar los métodos de envío.
- Fomente la cultura de ciberseguridad entre los empleados, sobre medidas y peligros, a través de formación y hábitos de protección para el comercio y el consumidor.
- Para el envío de los productos, contrate compañías de logística de confianza, seguras y de reconocido prestigio, exigiendo siempre la confirmación de la entrega al destinatario final, mediante la firma del albarán o factura.
- Realice el tratamiento de los datos personales de los clientes de acuerdo con la Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales y la Ley de Servicios de la Sociedad de la Información (LSSI).

Como medidas para evitar el fraude o el perjuicio al comercio electrónico es fundamental tener en cuenta **LOS SIGUIENTES ASPECTOS:**

- En el momento de realizar los pagos a los proveedores, desconfíe de los cambios en los números de teléfono de contacto, correos electrónicos o de cuentas bancarias habituales. Estos cambios han de ser confirmados con el proveedor en persona o telefónicamente con un interlocutor de confianza (no enviando un correo electrónico).
- Monitorice las redes sociales en busca de una posible suplantación corporativa en comercio electrónico (plataformas similares) o de plataformas asociadas a su empresa o comercio que no hayan sido creadas por usted.

Denuncie tales hechos en los motores de búsqueda y póngalos en conocimiento del área policial especializada de **DELITOS TECNOLÓGICOS**, a través de **www.policia.es**, siguiendo la ruta **CONTACTA-DELITOS TECNOLÓGICOS**

https://www.policia.es/_es/colabora_informar.php

2.8 MEDIDAS DE SEGURIDAD FRENTE A FALSIFICACIONES Y COMPETENCIA DESLEAL

El fenómeno de las falsificaciones es un problema en nuestra sociedad actual, que pone en peligro la salud del comercio. El comerciante se enfrenta a un delito contra la propiedad industrial si pone a la venta productos falsificados.

Por todo ello,
LAS SIGUIENTES RECOMENDACIONES:

- Exija a su proveedor/distribuidor transparencia en la transacción comercial, solicitando siempre factura en la que consten todos los datos fiscales.
- Desconfíe de precios por debajo del nivel habitual de mercado, ya que puede ser un claro indicador de mercancía falsificada.
- Contacte con los proveedores a través de sus páginas y plataformas oficiales. Sospeche si las imágenes de los productos no son nítidas o no se muestran claramente los logotipos de la marca.
- La demora en la recepción del producto de más de 10 días puede ser un indicador de que la mercancía no es original.
- Examine la mercancía en el momento de la entrega para evitar problemas en la reclamación por incumplimiento de contrato.
- Avise a la Policía si detecta alguna actividad irregular de comercio.

¿QUÉ HACER ANTE UN PRODUCTO FALSIFICADO?

Cuando, a pesar de seguir las recomendaciones anteriormente indicadas, se encuentre con algún producto falsificado dentro de su inventario, siga los siguientes pasos, que servirán para identificar tanto al falsificador como a otros comerciantes afectados:

- Trate de identificar el origen del producto y todos los detalles relacionados con su adquisición.
- No deseche el producto ni lo destruya. Denuncie el hecho a la Policía Nacional.
- No trate de venderlo en ningún caso porque podría conllevar algún tipo de responsabilidad penal.

En caso de duda sobre cómo actuar frente a la sospecha de una falsificación puede visitar la página web de la Oficina Española de Patentes y Marcas, o directamente puede enviar su consulta al correo electrónico,

https://stopfalsificaciones.oepm.es

especializada en la lucha frente a falsificaciones o, directamente, envíe su consulta al correo electrónico **stopfalsificaciones@oepm.es.**

3 ACTUACIÓN ANTE UNA SITUACIÓN QUE NO OFREZCA GARANTÍAS

En alguna ocasión puede encontrarse en su establecimiento con clientes que tengan cierta actitud vigilante o que, aparentemente, estén controlando los movimientos de los trabajadores del establecimiento. Desconfíe de estas situaciones ya que pueden estar a la espera de cometer un delito (hurto, robo, estafa, etc.).

LAS MEDIDAS a tener en cuenta son:

- Ponga esta situación en conocimiento del personal de seguridad privada, en caso de contar con este servicio. Si no dispone del mismo, póngalo en conocimiento de la Policía Nacional, aportando sus rasgos característicos, ropa y cualquier otro detalle (descripción física, tatuajes, cicatrices, acento, etc.) de la persona/s que han accedido al establecimiento y que puedan facilitar su identificación.
- No deje sus objetos personales (bolso, móvil, etc.) al alcance del público
- Advertir con rótulos, en la entrada del establecimiento, que las mercancías que salgan del mismo podrán ser comprobadas.
- Ante personas con actitud que no le generen confianza, tome medidas de autoprotección de forma rápida y discreta, tales como: cerrar la puerta principal ante un intento de acceso al establecimiento, simular que se está efectuando una llamada informando del hecho, etc.
- Evite siempre la confrontación. No se enfrente nunca al delincuente, especialmente cuando este se encuentre armado.

4 FORMAS DELICTIVAS MÁS COMUNES

EL HURTO

El hurto consiste en apropiarse de una cosa mueble ajena, sin utilizar la fuerza sobre las cosas ni violencia o intimidación sobre las personas.

***Modus operandi* más usuales que pueden darse en su establecimiento:**

- **Chicle:** este tipo de hurto se da sobre todo en joyerías. El delincuente pega un chicle bajo el mostrador y cuando le muestran las piezas, hurta una y la pega en el chicle. Si el trabajador no se percata, posteriormente un cómplice recoge la pieza pegada al chicle.

- **Muleta:** los delincuentes se sirven de cualquier instrumento (pañuelo, periódico, revista, bolsa, etc.) para distraer al comerciante, ocultando el objeto que se quiere sustraer.

- **Bolsa con el interior recubierto de papel de aluminio:** estas bolsas de fabricación casera evitan el funcionamiento de los chips de seguridad instalados en los artículos al pasar por el arco detector de la puerta del establecimiento.

- **Distracción del trabajador:** los delincuentes actúan en grupo y, mientras unos distraen y engañan al vendedor, otros consuman el hurto.

- **Uso de ganzúas e imanes:** se usan para retirar las alarmas de las prendas.

- **Hurto mágico:** tras pagar con un billete de alto valor un producto de bajo coste y recibir el correspondiente cambio, el delincuente -generando confusión- muestra disconformidad y solicita la devolución del billete, consiguiendo finalmente quedarse con el billete entregado y con parte del cambio.

- **Hurto con menores:** se accede al interior de un establecimiento con menores de edad y, mientras los autores distraen a la víctima, los menores aprovechan para acceder a zonas privadas (zona de almacén, vestuario o zona de mostrador).

- **Piqueros:** son grupos de personas habilidosas, que introducen su mano en bolsos con el fin de apoderarse de la cartera u objetos de valor de los clientes.

- **Hurto de efectos por personas vistiendo ropa amplia:** consiste en ocultar bajo la ropa los objetos sustraídos en el interior del establecimiento.

EL ROBO

El robo consiste en apropiarse de una cosa mueble ajena, utilizando la fuerza sobre las cosas o la violencia o intimidación sobre las personas.

Desconfíe de visitas inesperadas de técnicos que alegan revisión rutinaria o avería de instalaciones. Pueden ser delincuentes que estudian el establecimiento, los alrededores, los sistemas de seguridad u obtener los códigos de seguridad de los cajetines de las alarmas y acceder en días posteriores

ESTAFAS

La estafa es un delito consistente en provocar un perjuicio económico o patrimonial a alguien mediante engaño.

En el marco virtual habría que tener muy presente las técnicas de ingeniería social empleada por los delincuentes como paso previo a la comisión de la estafa y cuyo principal exponente es el ***phishing***. Las modalidades más habituales serían las realizadas mediante el envío de correos electrónicos, llamadas de teléfono (*vishing*) o mensajes de texto (*smishing*), donde se suplantan identidades corporativas o entidades financieras.

De esta forma, se hace creer a las víctimas que se están poniendo en contacto con ellas por problemas o incidencias, para obtener credenciales de acceso *online*, información bancaria y personal, que serán utilizadas *a posteriori* para cometer las estafas.

Tenga presente que el número de teléfono que aparece en la pantalla de su terminal puede no corresponderse con el titular real de la línea (*spoofing*), siendo una técnica habitual utilizada por los delincuentes.Hay que mantener una actitud vigilante respecto a las estafas, rehuyendo en general las ofertas de negocios fáciles.

TIPO DE ESTAFAS MÁS USUALES DE LAS QUE PUEDE SER OBJETO:

- **En el pago:** el estafador compra un objeto pagando con un billete de gran valor y engaña al comerciante para quedarse con el billete y el cambio. Además, hay que vigilar las monedas ya que las hay con apariencia similar a los euros, pero que no son de curso legal ni tienen el mismo valor.

- **A través de plataformas de envío de dinero instantáneo:** se debe comprobar que recibe una «notificación de ingreso» y no una «solicitud de envío» de dinero.

- **Cambio de códigos de barras:** consiste en cambiar el código de barras de artículos de precio elevado por el código de barras de artículos más baratos.

- **QRishing:** sustitución del código QR original por otro fraudulento, el cual redirige a una página web que imita la apariencia de un sitio legítimo, donde se suele solicitar el ingreso de datos personales y/o financieros.

- **Anuncios fraudulentos:** sobre subastas, ventas de segunda mano, falsas ofertas de empleo, alquileres vacacionales, etc. Desconfíe del pago fuera de las plataformas donde se anuncian.

- **Creación de páginas web falsas:** simulando ser un comercio *online* cuando en realidad es un fraude, ya que nunca llega a entregarse el producto o servicio adquirido, dado que detrás de dicha página web no existe ningún soporte comercial. Desconfíe de las páginas que no ofrecen métodos de pago seguro.

- **Suplantación de identidad corporativa:** el delincuente crea una página web similar a una ya existente o con los datos de una empresa real que no dispone de página web.

- **Estafa a través de correo electrónico comprometido:** se trataría de una especie de usurpación de identidad virtual, donde los delincuentes acceden a las cuentas de correo electrónico de las víctimas, desde las cuales envían mensajes con la finalidad de obtener algún tipo de beneficio (transferencias bancarias, compra de productos, etc.).

- **Fraude al CEO:** a través de diversas técnicas (ingeniería social, *malware*,

etc.), los delincuentes obtienen información sobre la actividad de la empresa que utilizan posteriormente para obtener beneficio económico a su favor. En relación con las transferencias bancarias suelen captar la forma en que la empresa realiza las mismas para simular nuevas transacciones en su provecho.

- ***Sim-swapping*:** duplicación de la tarjeta SIM para el acceso fraudulento a la banca *online*. Suelen comenzar con un «*phishing*» en el que tratan de captar las claves de acceso a la cuenta electrónica para, posteriormente, solicitar un duplicado de la tarjeta SIM, suplantando la identidad de la víctima. De esta forma, los mensajes de seguridad bancarios son remitidos a los delincuentes, permitiéndoles completar las transacciones económicas fraudulentas. La víctima puede detectar esta estafa porque su teléfono móvil se queda de forma repentina sin cobertura.

- ***Suplantación de proveedores*:** los delincuentes se hacen pasar por compañías de suministros y servicios y reclaman facturas atrasadas o impagos, con la amenaza del corte de los mismos si no se realiza el pago. En caso de duda, haga las comprobaciones necesarias por los canales oficiales de su distribuidor.

5 ACTUACIÓN ANTE HECHOS DELICTIVOS

Si tiene conocimiento o ha sido víctima de la comisión de un delito, avise inmediatamente a la Policía Nacional llamando al 091 (llamado CIMACC, Centro Inteligente de Mando, Coordinación y Control) y espere su llegada.

Además, debe tener en cuenta
LAS SIGUIENTES RECOMENDACIONES:

- No acceda al interior de un establecimiento para verificar los hechos hasta que no haya llegado la Policía Nacional, dado que todavía podría encontrarse en el interior alguna persona ajena al mismo.
- No manipule los objetos que haya podido tocar el autor de los hechos para facilitar la obtención de posibles pruebas que puedan identificar al delincuente.
- Facilite a la Policía Nacional el mayor número de datos del suceso y del presunto autor, así como la dirección y el modo de huida empleado (vehículo, a pie, transporte público, etc.).
- Solicite a los testigos que esperen a la llegada de la Policía Nacional. En caso contrario, pedirles sus datos y un teléfono de contacto para que puedan ser localizados.
- No manipule el servidor o dispositivo que haya sido utilizado para cometer un posible delito telemático, de cara a no modificar las posibles evidencias electrónicas.

6 FORMALIZACIÓN DE LAS DENUNCIAS POLICIALES

Las denuncias pueden formalizarse:

- **En dependencia policial de manera presencial.**
- **Por Internet en la «Oficina Virtual de Denuncias de la Policía Nacional».** Es posible acceder dentro de **www.policia.es** siguiendo la ruta **DENUNCIAS - EN LÍNEA.**

https://denuncias.policia.es/OVD/

- **Denuncias *in situ*.** Al objeto de agilizar la tramitación de denuncias de determinados hechos delictivos sin necesidad de desplazarse a una dependencia policial, se ha puesto en marcha el **«Protocolo de Denuncias *in situ*»,** al que podrán adherirse los establecimientos que cumplan con los requisitos necesarios.
- Si quiere información sobre dichos requisitos, puede solicitarla enviando un correo a **redazul@policia.es**

HECHOS NO DENUNCIABLES POR INTERNET

a través de la Oficina Virtual de Denuncias de la Policía Nacional:

- Si los hechos se han cometido mediante violencia (física o intimidación) o son de naturaleza sexual, por requerir un tratamiento singularizado y una atención directa, inmediata, especializada y personalizada a la víctima.
- Si el autor/es del hecho puede ser identificados o reconocido físicamente.
- Si se tiene constancia de la existencia de testigos que pudieran haber presenciado el delito.
- Si la víctima del hecho es menor de edad.
- Si ha habido ya intervención policial en el lugar de los hechos.
- Si el delito se está cometiendo en ese momento, debe comunicarlo de inmediato a través del teléfono 091.

A través de los formularios habilitados en el apartado **CONTACTA** de la página web **www.policia.es**

https://www.policia.es/_es/colabora_informar.php

podrá contactar con las áreas policiales especializadas y realizar cualquier consulta o informar de la comisión de cualquier ilícito penal.

El envío de dicha información en ningún caso tendrá la consideración de denuncia. Si un ciudadano se siente víctima de un delito, debe interponer una denuncia a través de los canales expuestos anteriormente.

Síguenos en y en **policia.es**

DL: M 18556-2024

Editor:
Ministerio de Economía, Comercio y Empresa
NIPO (papel/electronico): 221-24-065-3/ 221-24-066-9
Ministerio del Interior
NIPO (papel/electronico): 126-24-078-8/ 126-24-079-3

Diseño grafico:
Área de Publicaciones de la Policia Nacional

Impresión y encuadernación:
Centro de Impresión Digital y Diseño de la Secretaría de Estado de Comercio

Papel:
Exterior: estucado brillo ecológico (150g)
Interior: offset ecológico FSC/TCF (100g)

POLICÍA NACIONAL

Oficina Española de Patentes y Marcas

Confederación Española de Comercio

GOBIERNO DE ESPAÑA

MINISTERIO DEL INTERIOR

MINISTERIO DE ECONOMÍA, COMERCIO Y EMPRESA