FRAUDE Y GESTIÓN DE LA IDENTIDAD ONLINE

Colección

PROTEGE TU EMPRESA

GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa

ÍNDICE

1- INTRODUCCIÓN 03
2- IDENTIDAD ONLINE EN COMERCIO ELECTRÓNICO 04
2.1. AMENAZAS EN COMERCIO ELECTRÓNICO 05
3- FALSOS TÓPICOS SOBRE LA SEGURIDAD DEL COMERCIO ELECTRÓNICO 08
3.1. IDENTIFICACIÓN INEQUÍVOCA DE CUALQUIER SERVICIO CORPORATIVO 09
3.2. PROTECCIÓN DE LA INFORMACIÓN DE LOS CLIENTES 11
3.3. DETECCIÓN DEL FRAUDE 13
4- IDENTIDAD ONLINE EN REDES SOCIALES 15
5- RECOMENDACIONES DE SEGURIDAD 17
5.1. USO DE CERTIFICADO DIGITAL DE SERVIDOR SEGURO 18
5.2. MEDIOS DE PAGO ADECUADOS 20
5.3. DETECCIÓN DE FRAUDES 23
5.4. MEDIDAS PARA EVITAR EL FRAUDE 25
6- REFERENCIAS 26

ÍNDICE DE FIGURAS

Ilustración 1: Comprobación de certificado digital 19
Ilustración 2: Distintos tipos de pasarelas de pago 21

1. INTRODUCCIÓN

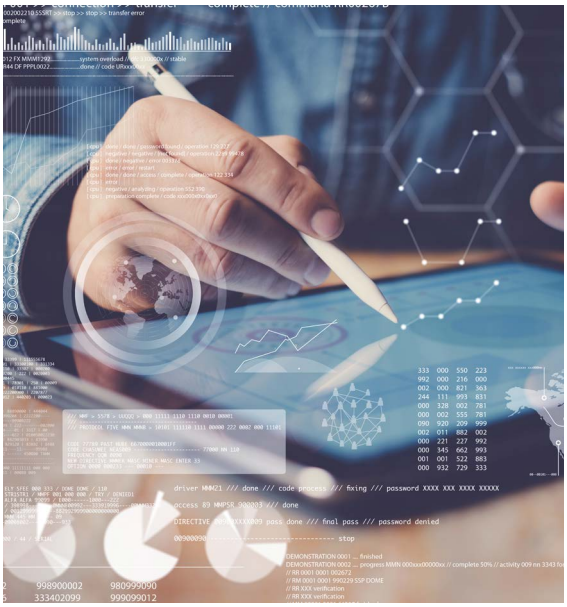
Con el auge de Internet como entorno comercial, es esencial para cualquier empresa tener presencia, comunicarse con los potenciales clientes y ofrecer sus productos o servicios a través de este medio. Por ello es trascendental saber gestionar la identidad corporativa online con el fin de que la empresa adquiera y mantenga su buena reputación.

La **identidad online** de una organización hace referencia a toda la información que hay publicada en Internet: web corporativas, blogs, redes sociales, etc. También se alimenta de las aportaciones o comentarios que clientes o usuarios hacen en Internet. Toda organización puede comunicar unos valores o rasgos que la definen y la diferencian de su competencia.

Cualquier persona que se ponga en contacto con nosotros debe tener la certeza de que realmente está contactando con nuestra compañía. Igualmente las empresas deben poder identificar a quienes interactúan con ellas, sean clientes u otras empresas y la veracidad de los documentos que intercambian (tarjetas bancarias, contratos,...). Sin embargo, el **fraude** (en forma de todo tipo de engaños y estafas) y la **suplantación de identidad** online están a la orden del día y nos afectan tanto a nosotros como empresa como a nuestros clientes.

Estas amenazas no pueden ser pasadas por alto por ninguna empresa, ya que no hablamos sólo de pérdidas económicas o de los perjuicios directos de un incidente de este tipo sino que pueden conllevar una degradación considerable de la imagen corporativa y la confianza de los clientes.

Del mismo modo, si pensamos ofrecer **comercio electrónico** para la venta de productos o servicios, debemos adoptar medidas de protección específicas contra el fraude. En este caso, no sólo nos preocupa que el usuario pueda identificar comunicaciones o servicios ilegítimos, sino que debemos identificar fraudes y facilitar a los clientes, en la medida de lo posible, mecanismos para mantener la seguridad en su trato con nosotros.



2. IDENTIDAD ONLINE EN COMERCIO ELECTRÓNICO

La identidad en comercio electrónico es esencial para la empresa. Por ello las tiendas online además de vigilar las posibles compras fraudulentas, han de estar preparadas para evitar:

- que nos suplanten con el consiguiente daño a nuestra identidad y potencialmente a nuestros clientes;
- que nuestra imagen quede dañada por falta de disponibilidad o por no proteger adecuadamente los datos de nuestros clientes con las consiguientes sanciones legales;
- que nos difamen o utilicen nuestra marca para actividades delictivas.

Como responsables del servicio, debemos:

- Proteger a nuestros clientes:
  - Asegurándoles una conexión que puedan verificar como legítima y segura a cualquiera de nuestros servicios.
  - Proporcionando medios que protejan la información personal que aportan (direcciones postales, correo electrónico,...) y las transacciones.
- Proteger nuestros servicios:
  - Reduciendo la posibilidad de tramitar pedidos fraudulentos (con tarjetas robadas, por ejemplo).
  - Evitando sufrir ataques contra nuestros servicios online que los dejen inactivos o que aprovechen nuestros servidores para actividades ilícitas (suplantar un banco por ejemplo para robar credenciales o distribuir *malware* con anuncios o enlaces ocultos).
- Proteger nuestra imagen y marca:
  - Identificando posibles fraudes realizados empleando nuestra imagen corporativa en cualquier medio.
  - Evitando sanciones por incumplimiento legal. Mostrando claramente nuestro respeto con los derechos de los consumidores y su privacidad, tanto en nuestras comunicaciones comerciales como en nuestras páginas.

2.1. AMENAZAS EN COMERCIO ELECTRÓNICO

Las principales amenazas que pueden dañar nuestra imagen e identidad tienen por objetivo tanto los usuarios de páginas web, y en particular los de tiendas online, como las propias páginas y tiendas. Son las siguientes:

- ***Phishing***: El usuario recibe una comunicación (por correo electrónico, mensajes al móvil o en redes sociales) destinada a engañarle para que conecte a un servicio fraudulento con el fin de obtener su información de pago o credenciales de acceso al servicio legítimo. También se llama *phishing* al ataque que recibe un sitio web legítimo para alojar una página fraudulenta (por ejemplo las que suplantan a bancos o a tiendas conocidas).
- ***Pharming***: Similar al *phishing*, pero en este caso la víctima no tiene que pulsar en un enlace fraudulento, sino que es redirigida al sitio fraudulento al intentar acceder a un sitio legítimo de la manera habitual. Esto es posible gracias a la modificación de la información proporcionada por los servidores de servicios de nombres de Internet o DNS (que almacenan la información acerca de nombres de dominio y su correspondiente dirección IP). Tras modificar esta información, cuando las víctimas le piden al DNS la «traducción» de los nombres de dominio a las direcciones IP, la información devuelta les redirige a un servidor fraudulento.
- ***Botnets***: Se trata de *malware* que se instala en equipos de los usuarios y aprovecha los recursos de muchos equipos de «víctimas» de forma coordinada por los ciberdelincuentes para la realización de ataques dirigidos como: envío de ***spam***, distribución de ***malware*** o **ataques DoS**, o de denegación de servicio (consisten en saturar de peticiones, para dejar no accesible, un servidor o un sitio web). No sólo los equipos de nuestros clientes sino también los equipos que alojan nuestra web o tienda online, de resultar infectados, pueden formar parte de una *botnet*.
- **Fuga de datos**: Las páginas y tiendas online albergan datos de clientes que los delincuentes pueden vender en el mercado negro. Si estos consiguen entrar en los servidores que albergan nuestra página o nuestra tienda, podrán conseguir estos datos para comerciar con ellos. Para conseguir entrar en nuestros servidores utilizan técnicas, bien de **ingeniería social** (engaños a personas para conseguir las credenciales de administrador), o bien explotando vulnerabilidades del software o fallos de configuración. Estos ataques pueden llegar a ocasionar sanciones económicas por el incumplimiento de la legislación en materia de protección de datos personales.

- **Fraude** en distintas modalidades, por ejemplo:
  - **Envío urgente**, en el que el usuario nos apremia a enviar el producto y nos envía una fotocopia de un justificante de pago que resulta ser falso, realizamos el envío sin comprobar el ingreso (que no se ha realizado).
  - **Triangulación**, en la que el cliente es derivado a una falsa página, igual que la nuestra, en la que tramita un pedido, realizando el pago. El delincuente realiza luego este pedido en nuestra tienda con una tarjeta robada. Enviaremos el producto al cliente, que no percibirá que ha (hemos) sido objeto de un fraude.
  - **Reenvío** o ***reshipping***, donde el defraudador, que ha comprado con una tarjeta robada, utiliza un mulero para recibir el paquete y evitar así ser descubierto.
  - **Toma de control de cuentas de cliente**, por la que acceden a una cuenta de un cliente de nuestra tienda con las credenciales robadas (por una fuga de datos por ejemplo o con un correo de *phishing* e ingeniería social), modifican los datos de envío o el número de teléfono para así poder realizar el fraude.
  - **Fraude amigo**: En este caso el proceso de compra es legítimo, el pago, la entrega, etc. Sin embargo, una vez realizadas todas las actividades, el cliente declara la compra como fraudulenta en su banco, y el vendedor recibe una petición de devolución, no pudiendo recuperar la mercancía, se haga efectiva o no.

- **Contra la marca y el nombre de dominio (propiedad industrial):**

  - **Utilización no consentida de nuestra marca.** En este caso utilizan nuestro *slogan* o nuestra marca con alguna modificación para aprovecharse de nuestra reputación.

  - **Registro abusivo de nombres de dominio.** Los delincuentes registran uno o varios nombres de dominio que coinciden total o parcialmente con la marca de la empresa, impidiendo a esta última utilizar dichas denominaciones en su negocio. Este tipo de ataque es utilizado para extorsionar a la empresa o para aprovecharse de su reputación atrayendo clientes a las páginas con esos nombres de dominio dónde podrán obtener beneficios por la publicidad incluida.

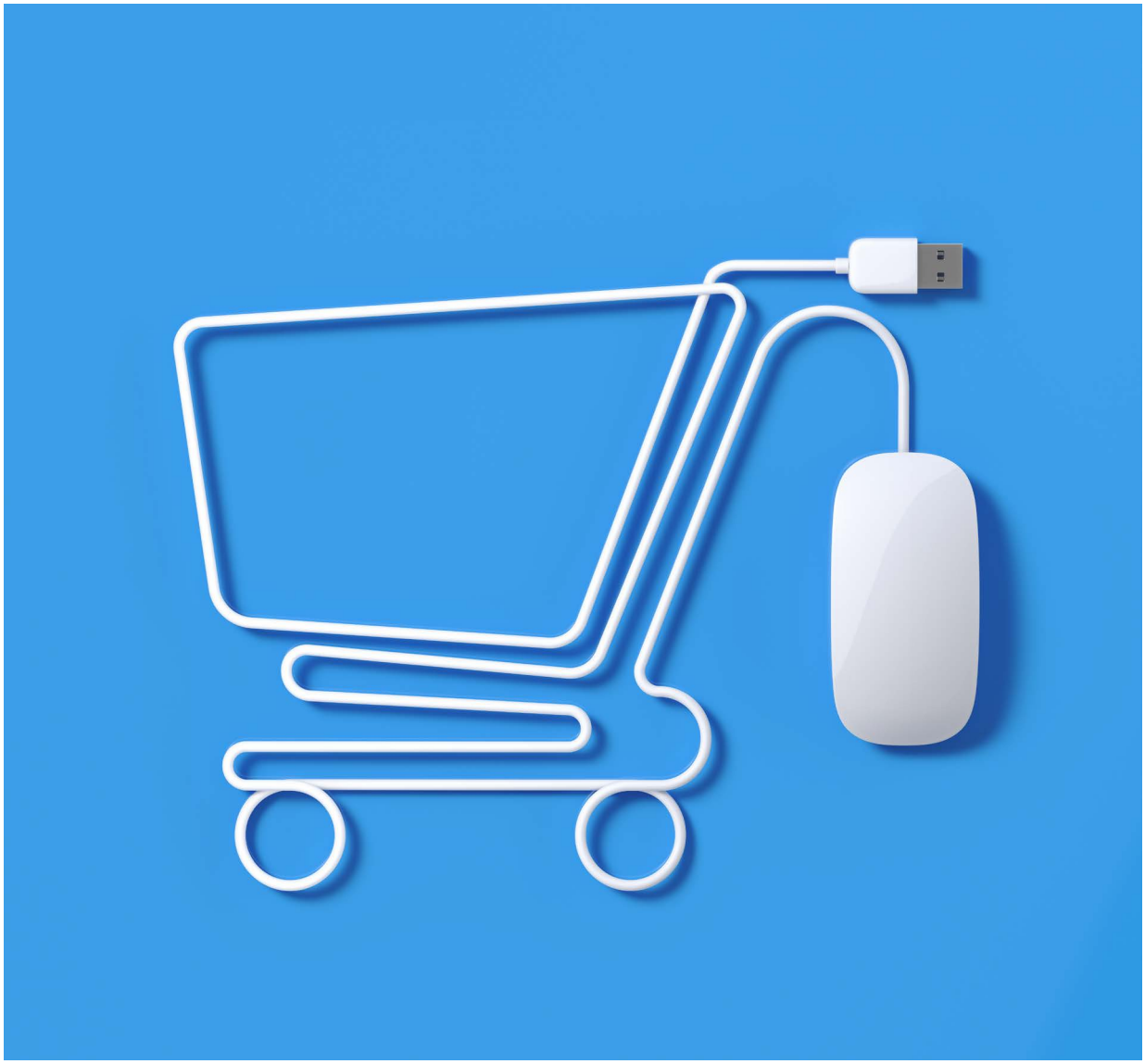
- **Incumplimiento legal.** Cualquier incumplimiento puede llevar a sanciones, con el consiguiente daño de imagen.

  - Toda actividad económica en Internet está regulada por la **LSSI** (Ley 34/2002 de 11 de julio de Servicios de la Sociedad de la Información y del Comercio Electrónico). Además, el desarrollo de esta ley obliga a las páginas web a informar sobre las ***cookies*** propias y ajenas que se utilicen. Las *cookies* son ficheros de texto con datos que facilitan el acceso, personalizar el servicio o analizar el comportamiento del usuario.

  - Por otra parte las tiendas online y otras web que recogen datos personales están sujetas al **RGPD** (Reglamento General de Protección de Datos) **[4]**.

3. FALSOS TÓPICOS SOBRE LA SEGURIDAD DEL COMERCIO ELECTRÓNICO

Existen una serie de tópicos o ideas preconcebidas relacionadas con el comercio electrónico que, de tanto repetirse, son dadas por ciertas sin serlo. **Debemos evitar caer en las afirmaciones que aun siendo falsas, se han dado como ciertas** en lo que a comercio electrónico se refiere; por ello es importante conocer cuál es la verdadera situación respecto a los tópicos más comunes.



3.1. IDENTIFICACIÓN INEQUÍVOCA DE CUALQUIER SERVICIO CORPORATIVO

El primero de nuestros objetivos es facilitar al cliente la **identificación inequívoca** de cualquier servicio corporativo publicado a través de Internet.

Estas son algunas falsas creencias relativas a la identificación de empresas y servicios:

> **FALSO:** "Es complicado que el usuario se confunda, tenemos una imagen corporativa conocida e identificable, nuestro servicio es popular y nuestro sitio web para comercio electrónico es muy característico".

Que nuestro producto o servicio sea conocido y nuestra plataforma de comercio electrónico sea popular y empleada por un elevado número de clientes, no impide que se pueda suplantar la identidad del mismo. Al contrario, un ciberdelincuente preferirá suplantar la identidad de un sitio reconocido y de confianza que uno que no disponga de tan buena reputación. Construir un sitio web fraudulento idéntico al original es muy sencillo.

> **FALSO:** "En cualquier caso, los usuarios conocen nuestro dominio, nos publicitamos con él y es nuestra seña de identidad".

Es posible que los usuarios conozcan y distingan el nombre de dominio de nuestro comercio online. Sin embargo, los nombres de dominio se traducen por direcciones IP que, finalmente, son las que se emplean en las conexiones con los servidores. Un usuario podría ser víctima de distintos engaños, por ejemplo:

- El usuario recibe un mensaje, supuestamente desde una de nuestras cuentas de correo, con un enlace que tiene una grafía muy parecida a nuestro nombre de dominio (con alguna letra cambiada), el usuario lo da por bueno y creyendo conectar con nuestra página conecta con otra que nos suplanta, robándole las credenciales o vendiéndole productos que no son los nuestros.

- Se le presenta (en una página o en un mensaje) un enlace con nuestra grafía pero nuestro sitio ha sido atacado y han suplantado nuestra identidad, llevándole a otra página donde puede ocurrirle lo anterior.
- El usuario recibe, en nuestro nombre, un enlace acortado que no verifica y le lleva a un sitio malicioso.

Por ello es necesario permitir que nuestros clientes puedan, sobre todo al introducir algún dato o realizar una compra, verificar nuestra identidad y la seguridad de la conexión a nuestros servicios. Para ello nuestra web debe tener un certificado como veremos más adelante. De esta forma contribuimos a evitar que puedan ser víctimas de un fraude.

El que un usuario sea víctima de fraude electrónico tiene repercusiones negativas para nuestra empresa, ya que:

- Degrada tanto nuestra imagen corporativa como la sensación de confiabilidad y seguridad del cliente.
- Si se obtienen las credenciales de acceso de la víctima a uno de nuestros servicios, éstas pueden ser empleadas para realizar actividades fraudulentas (podrían suplantarle y comprar en su nombre, enviarle *spam* o *phishing*,...).

3.2. PROTECCIÓN DE LA INFORMACIÓN DE LOS CLIENTES

Debemos **facilitar medios para la protección de la información de los clientes**. Para ello, nos haremos las siguientes preguntas: ¿Hemos implantado todas las medidas contra el fraude online? ¿Protegemos adecuadamente la información personal y de pago de nuestros usuarios?

Estas son las principales afirmaciones falsas relativas a la protección de la información:

> **FALSO:** "La información de los usuarios de mi servicio está perfectamente protegida en nuestros servidores, que están en nuestro bunker dentro de nuestras instalaciones".

Aunque los datos se almacenen con elevadas medidas de seguridad, la información es más vulnerable cuando se está transmitiendo a través de redes públicas como Internet. Por ello tenemos que ofrecer a nuestros clientes:

- accesos seguros cuando hacen *login* en nuestra página o en nuestra tienda online que nos permitan evitar que sus credenciales sean robadas;
- comunicaciones cifradas cuando introducen o envían cualquier tipo de datos.

> **FALSO:** "Una vez hemos recibido los datos del pago con tarjeta del cliente se envía el producto. Al tener los datos de la tarjeta no tenemos ningún riesgo de fraude".

Aunque se reciba el pago por una transacción online, esto no significa que la operación sea segura. Por ello al contratar medios y pasarelas de pago tendremos que comprobar:

- la identificación inequívoca de la entidad financiera (certificado);
- la confidencialidad de las comunicaciones garantizada mediante protocolos de cifrado seguros;
- el cumplimento de los estándares de seguridad de los datos para transacciones financieras.

Como medida básica **evitaremos** utilizar métodos de pago en los que nosotros (en nuestra web) tengamos que **tomar o conservar datos financieros de nuestros clientes.** Estos datos son el objetivo de delincuentes que trafican con ellos. Las pasarelas de pago seguras interactúan directamente con el usuario, evitando riesgos innecesarios.

No sólo es importante que el cliente identifique inequívocamente nuestro servicio y que nosotros le identifiquemos, además tenemos que asegurarnos de que todas las comunicaciones que crucemos con él sean confidenciales y seguras.

En caso contrario, sería posible que un ciberdelincuente capturara las credenciales de acceso de los clientes al servicio, información de pago, contacto o de preferencias. Esta información podría ser empleada para realizar nuevos fraudes contra nosotros o nuestros clientes.

3.3. DETECCIÓN DEL FRAUDE

Debemos mantener mecanismos para la detección del fraude para evitar, en la medida de lo posible, que se tramiten pedidos fraudulentos como legítimos, sea cual sea el contexto del mismo. Como empresas podemos ser víctimas de fraude de varias formas: compras con tarjetas o números de tarjetas robadas, identidades falsas, clientes que niegan haber recibido el producto, o los que dicen haberlo devuelto y nunca llega.

La pregunta que debemos plantearnos es: ¿se puede hacer algo para identificar el fraude antes de que sea demasiado tarde?

Estas son las principales creencias falsas relativas al fraude:

> **FALSO:** "Únicamente realizamos el envío del producto cuando recibimos la confirmación del pago, lo que nos asegura cobrar la mercancía".

Hasta que no se haga **efectivo** el pago de una transacción no se debe realizar la entrega, aunque esto provoque perjuicios al cliente. Sin embargo, esto tampoco nos garantiza no ser víctimas de fraude, ya que es posible que los bancos reclamen el dinero para devolverlo a su legítimo propietario, sin que se pueda recuperar el producto o servicio prestado.

> **ENGAÑOSO:** "Hemos restringido el uso de métodos de pago a aquellos que implican un menor nivel de riesgo, como las transferencias bancarias".

Si limitamos los métodos de pago a los que suponen menor riesgo para el vendedor, se reduce el riesgo de fraude. Sin embargo estas formas de pago **transfieren todo el riesgo al comprador**, pudiendo afectar esto a las ventas y, sobre todo, a la fidelización de los clientes que no nos conozcan.

> **FALSO:** "Disponemos de un perfil público y oficial en las principales redes sociales de nuestro interés, en los que tenemos un número considerable de seguidores. Se trata de una herramienta de fidelización de clientes y captación de algunos nuevos, no lo consideramos de vital importancia para el negocio".

En la actualidad, la mayoría de las empresas tienen un perfil o página en las redes sociales, con el fin de publicitarse y formar imagen corporativa. Este tipo de medios son determinantes, y también pueden ser utilizados para suplantarnos y engañar a nuestros clientes como en los conocidos casos de:

- falsos cupones de descuento de los supermercados o tiendas de ropa que redirigen a los clientes a falsas páginas dónde robarle sus credenciales;
- las falsas notificaciones de paquetería que en realidad descargan *malware*.

4. IDENTIDAD ONLINE EN REDES SOCIALES

En referencia directa a las redes sociales, debemos identificar y controlar las posibles **suplantaciones de identidad** que se puedan producir.

En este caso estamos hablando de riesgos tanto económicos como de reputación, que pueden venir dados por:

- suplantación del perfil;
- creación de perfiles falsos en redes sociales en las que no tenemos presencia;
- divulgación de mensajes falsos con perfiles similares al oficial;
- robo de credenciales en redes sociales y divulgación de mensajes difamatorios u ofensivos.

En estos casos, aunque los efectos secundarios implican un coste económico, los riesgos se pueden materializar y causar impacto en forma de:

- **Pérdida de clientes:** pérdidas causadas por problemas de seguridad en el servicio.
- **Pérdidas de imagen corporativa:** pérdida de confianza de los clientes potenciales, con la consecuente disminución de oportunidades de negocio por problemas de reputación.

Debemos monitorizar activamente la actividad relacionada con la imagen corporativa en las redes sociales, tanto si disponemos de un perfil oficial en las mismas como si no.

Actualmente gran cantidad de empresas disponen de un gestor de redes sociales o *Community Manager*, que se encarga de dinamizar los perfiles en redes sociales y hacer las publicaciones pertinentes en las mismas. El encargado de controlar e interactuar en las redes sociales, debe ser una persona experimentada en el uso de Internet y las redes sociales, que mantenga siempre una actitud positiva, neutral y sin participar en polémicas. No obstante, si nuestra presencia en Internet no es vital para nuestro negocio, este control puede llevarse de manera sencilla.

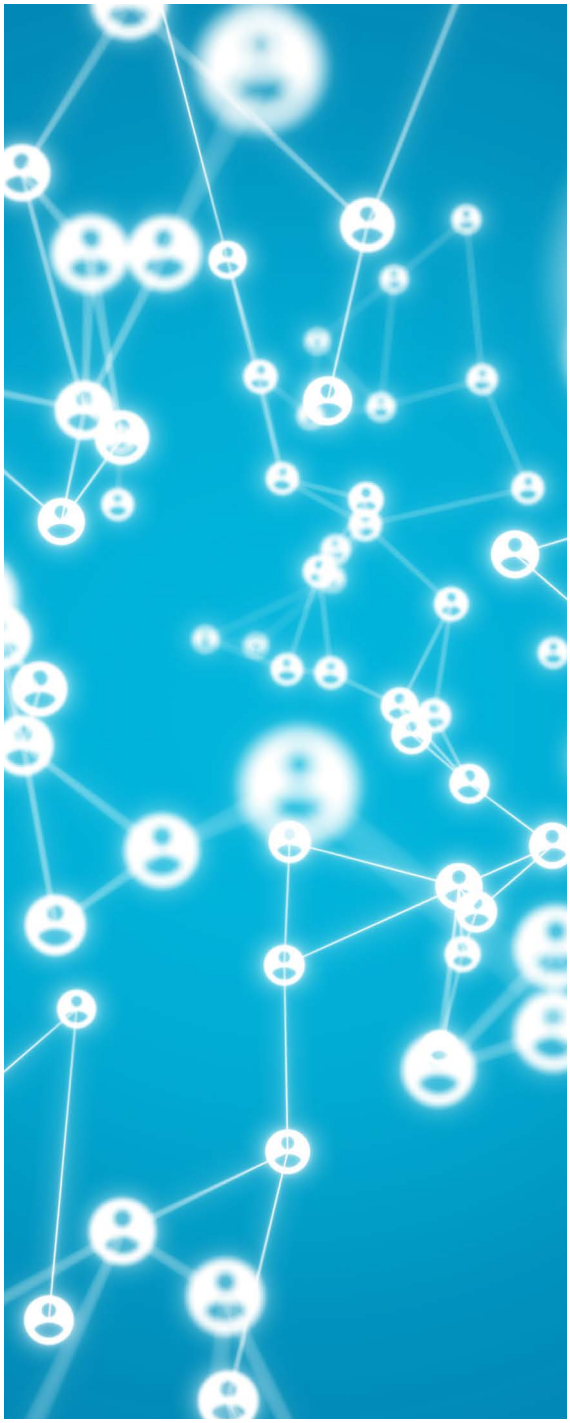
Debe ser competencia del gestor de redes sociales el controlar cualquier tipo de fraude:

- Verificar periódicamente los contenidos relacionados con la entidad en las redes sociales.
- Detectar posibles copias o usos no autorizados de las marcas o distintivos comerciales.
- En el caso de que se esté suplantando la identidad de nuestra organización, se debe recurrir directamente al soporte de la red social en cuestión.
- En caso de que el contacto con la red social no proporcione una solución al

problema, y existan indicios de un fraude económico, debe ponerse en conocimiento de las Fuerzas y Cuerpos de Seguridad del Estado **[1]**.

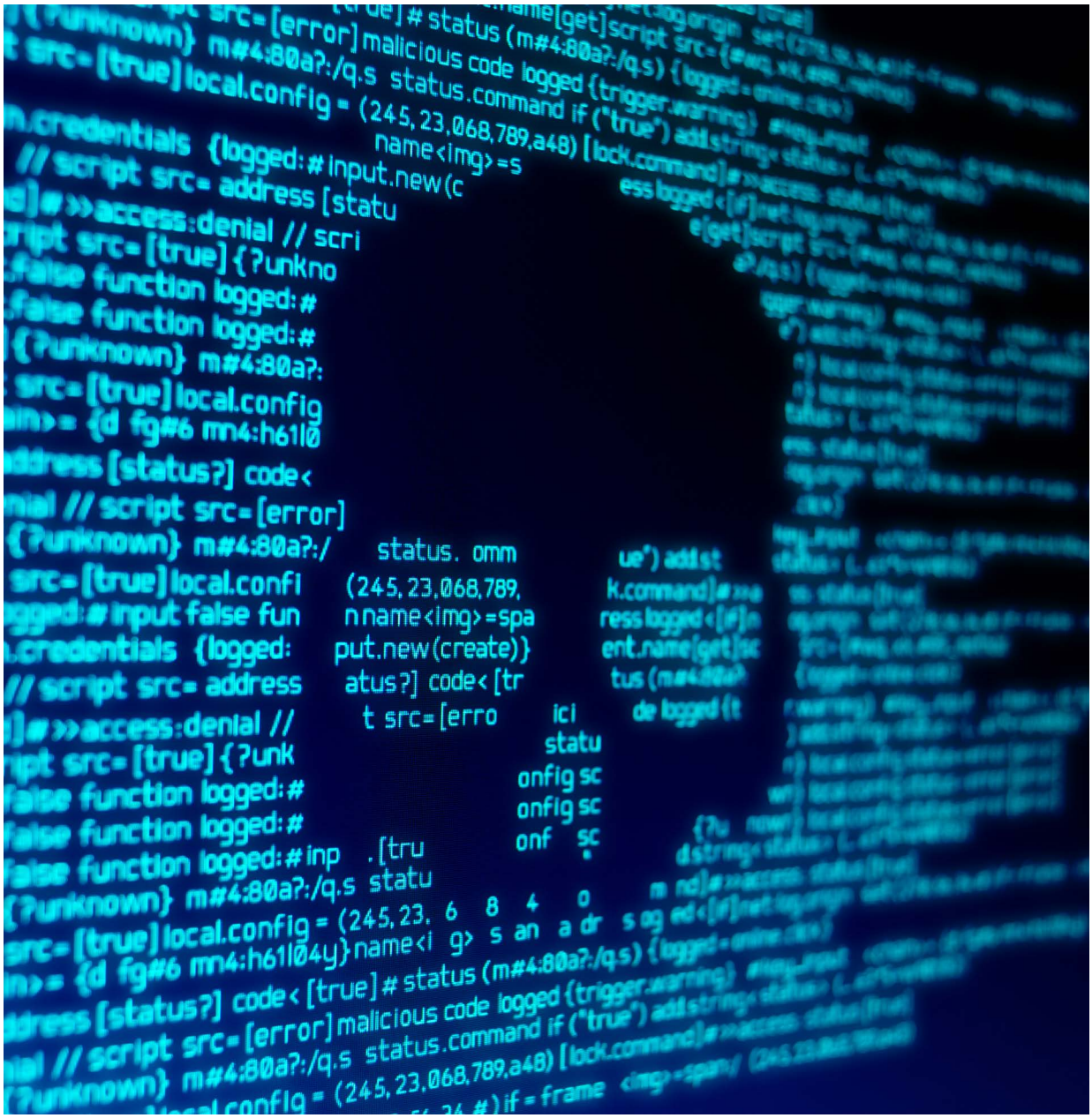
Es recomendable que para la gestión de los perfiles de las redes sociales sigamos los siguientes consejos:

- Proteger las cuentas con contraseñas complejas, que sean robustas, es decir, que tengan más de ocho caracteres y aparezcan mayúsculas, minúsculas, símbolos especiales (*/-+&%$) y números.
- Cambiar las claves de manera periódica.
- No actualizar los perfiles corporativos desde entornos no confiables: wifis públicas, ordenadores compartidos, etc.
- Compartir la clave de forma segura con dos o más personas, para evitar problemas de disponibilidad.
- Cambiarlas siempre que alguna persona con acceso a los perfiles deje la organización.



5. RECOMENDACIONES DE SEGURIDAD

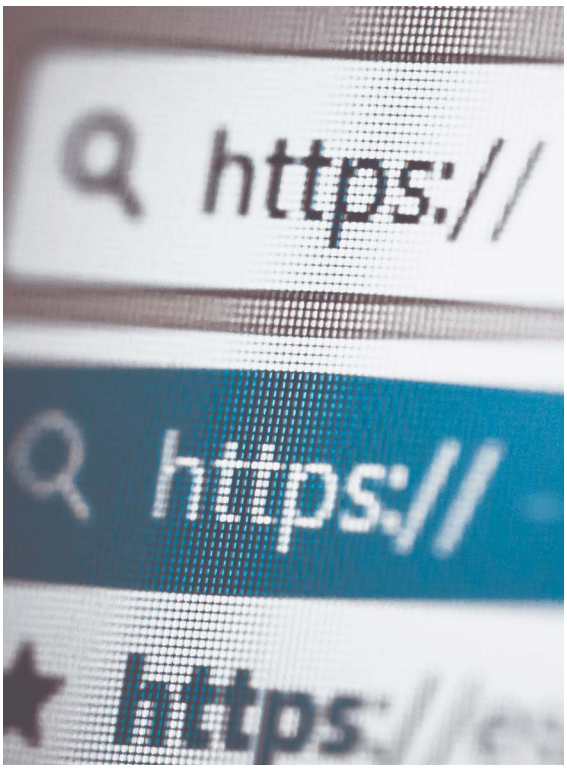
A continuación se detallan algunas recomendaciones básicas de seguridad destinadas a prevenir el fraude online.



5.1. USO DE CERTIFICADO DIGITAL DE SERVIDOR SEGURO

Esta recomendación de seguridad va dirigida específicamente a la identificación inequívoca de nuestro sitio web en Internet, y a la protección de la información en la comunicación con nuestros clientes. Esta medida consiste en hacer que nuestra página web o tienda online utilice el protocolo **HTTPS**, con conexiones cifradas y autenticadas, mediante certificados emitidos por entidades de confianza. El uso de **certificados digitales** aporta las siguientes ventajas:

- Asegura la **confidencialidad e integridad de la información** durante la transmisión, ya que emplea un método para cifrar todos los datos que intercambian el usuario y la página web. Este tipo de tecnología, conocida como SSL/TLS, es un estándar de facto en Internet, y es completamente compatible con cualquiera de los navegadores comerciales.
- Emplea criptografía de clave pública, que permite establecer una **conexión cifrada** desde la primera comunicación con el servidor, asegurando que toda la información que se intercambie desde el establecimiento de la conexión mantiene, además de la confidencialidad, su **integridad**, impidiendo que sea alterada.
- Permite que el cliente pueda reconocer nuestra identidad. Es lo que se conoce como **autenticación**. Cuando un cliente se conecta a nuestra página web, lo hace tecleando la dirección web o URL de la misma (por ejemplo www.tiendaonline.es). Esta dirección se traduce automáticamente en una dirección IP (una dirección IP es una serie de números que nos permiten llegar al servidor de las páginas buscadas), que es donde realmente el usuario está accediendo. Esta traducción de la dirección web en una dirección IP, se realiza empleando servicios independientes que podrían estar manipulados (*pharming*), por lo que sin saberlo, el cliente podría estar conectando con un servicio frau-



dulento. Por tanto, el hecho de que un usuario teclee nuestra dirección en su navegador no implica que necesariamente esté accediendo a nuestra página.

- Como usuarios, podemos verificar la seguridad del certificado digital haciendo clic en el **candado** que aparece junto a la dirección web en barra de búsqueda del navegador. De esta forma comprobaremos que la web a la que estamos accediendo con el navegador es legítima y es segura.

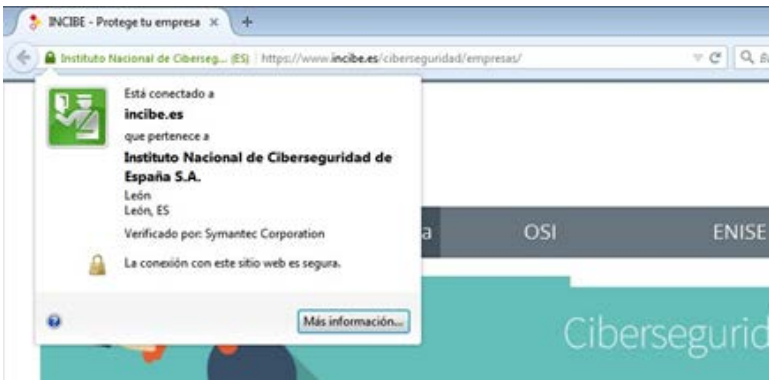


Ilustración 1
Comprobación de certificado digital

Este certificado debe estar emitido por una entidad de confianza, ya que cualquiera con un ordenador personal puede generar un certificado (autofirmado) para cualquier dominio, lo cual no tiene ninguna validez. También es recomendable que la entidad de confianza verifique nuestra identidad mediante una auditoría, lo que se mostrará con el **color verde** en la barra de direcciones del navegador. Estos certificados tienen una vigencia que debemos verificar, pues tener un certificado caducado deteriora nuestra imagen al mostrarle el navegador esta información al usuario.

Los servicios de certificados por entidades de confianza tienen un coste asociado. No obstante disponer de un certificado, vigente y emitido por una entidad de confianza garantiza al cliente que está conectando con un servicio legítimo y que no se trata de una suplantación de identidad.

Una **entidad de confianza** es una autoridad de certificación reconocida. El término **autoridad de certificación reconocida** se emplea para asegurar que dicha autoridad cumple con un conjunto de requisitos que garantizan que aplica las medidas de seguridad y control necesarias para emitir certificados digitales.

5.2. MEDIOS DE PAGO ADECUADOS

Esta recomendación de seguridad va dirigida a implementar medios de pago que nos protejan en la medida de lo posible contra el fraude.

- Una opción es permitir únicamente la realización de pagos con métodos que tengan un bajo riesgo de fraude, como el pago mediante **transferencia bancaria.** Sin embargo, este tipo de métodos trasladan el riesgo del fraude al propio cliente y puede restar competitividad a nuestro negocio.
- Otra opción de pago es hacerlo **contra reembolso**, que consiste en que el cliente hace efectivo el pago a la entrega del producto o servicio. Con este método, la empresa asume el coste del transporte del producto o servicio sin haberlo cobrado antes, y está expuesto a que se produzca una entrega fallida, ya sea porque el cliente rechace el producto, o bien porque los datos del supuesto comprador son falsos.
- Otra solución adecuada para la pyme es delegar la tramitación de los pagos en terceros. Estos pueden ser:

  » Pasarelas de pago que funcionan para el cliente como un monedero virtual. Son por ejemplo PayPal, Google Wallet o Amazon Payments. Para la empresa supone, además de tener que pagar una tasa, no tener que pedir datos bancarios al cliente pues estos los gestiona la pasarela de pago directamente con el cliente final.

  » TPV virtual (Terminal de Punto de Venta Virtual) proporcionadas por las entidades bancarias, dónde el cliente puede pagar con su tarjeta de crédito o débito. Para la empresa supone una cuota mensual y un porcentaje de las ventas.

  La ventaja en estos casos es que otorgan garantías antifraude tanto al comprador como al vendedor y nos evitan almacenar los datos de pago de los clientes, rebajando la criticidad de los datos almacenados y ahorrando costes en seguridad de la información.

Ilustración 2
Distintos tipos de pasarelas de pago

Antes de contratar uno de estos servicios debemos tener claras las condiciones generales respecto al fraude y en lo posible elegir aquellas que ofrezcan a nuestros clientes mayores garantías.

Para negocios con un alto volumen de ventas, es más recomendable optar por una **validación directa del pago**. Esta opción debe ser tomada con cautela y analizada seriamente, primero por la criticidad de la información que hay que almacenar, y en segundo lugar porque deberemos implantar todas las medidas anti-fraude necesarias. Entre otros, es imprescindible cumplir medidas de seguridad alineadas con estándares internacionales como PCI-DSS **[2]** si vamos a gestionar tarjetas de crédito.

En caso de que se opte por esta última opción, se deben tener en cuenta las siguientes medidas de seguridad contra el fraude antes de aceptar el pedido:

- **Solicitar CVV (Card Verification Value):** Adicionalmente a los datos habituales incluidos en la tarjeta, se solicita un código de seguridad de 3 dígitos que se encuentra en el dorso de la misma, aportando un nivel superior de seguridad.

- **Requerir Secure 3D (Visa y Mastercard):** Se trata de un servicio prestado por estas compañías que básicamente consiste en solicitar información adicional a la que habitualmente se requiere (como el **CVS**, **CID** o código de validez de la tarjeta, que es un código de tres cifras que se encuentra en la parte trasera de la tarjeta). Es una buena opción porque no se basa únicamente en información contenida en la tarjeta y mejora los niveles de seguridad. Sin embargo, utilizar solamente este tipo puede limitar enormemente la capacidad de algunos clientes para comprar en la tienda.

Es fundamental seleccionar diversos medios de pago adecuados para el comercio online, ya que se deben dar distintas posibilidades al comprador, siempre con cautela y conociendo los riesgos asociados a cada uno.

5.3. DETECCIÓN DE FRAUDES

Debemos hacer comprobaciones sobre los pedidos, de modo que podamos mitigar en la medida de lo posible la gestión y envío de un pedido fraudulento.

Estas comprobaciones se deben realizar en tiempo real cuando se tramita el pedido, por lo que lo habitual es emplear sistemas automatizados, aunque no debemos renunciar a realizar comprobaciones manuales en los casos más complejos.

Existen algunas comprobaciones habituales que es recomendable realizar y que están basadas en los casos más habituales de fraude:

- **Clientes Nuevos:** Este conjunto de clientes son los que mayor riesgo suponen, ya que carecemos de información previa. Debemos revisarlos con mayor detalle y establecer un criterio para evaluar su criticidad, ya que no existe un método infalible para la detección del fraude. Un indicador posible podría ser la cuantía del pedido ligado al destino del mismo, considerando mayor riesgo en envíos internacionales.
- **Clientes conocidos:** En este caso, es una buena práctica verificar que el pedido realizado está alineado con los pedidos anteriores en cuantía y dirección de envío. Una desviación considerable será un buen indicador de fraude.
- **Localización:** Debemos contrastar la dirección de envío con otros datos, ya que en muchas ocasiones este es un indicador muy fiable para la detección del fraude. Se puede contrastar la dirección de envío con:
  - La ubicación de registro de la tarjeta de crédito empleada.
  - La localización de la **IP** que realiza la conexión.
  - La configuración regional del dispositivo que realiza la compra.
  - Verificar la cadena que se genera como *fingerprint* de cada conexión.
- **Coincidencia de datos:** verificar si se realizan pedidos de distintos clientes pero con una dirección de envío común. Este caso también es habitual y es muy susceptible de ser un fraude.
- **Contactar con el cliente para validar el pedido:** Una simple llamada telefónica puede ayudar a detectar el propio fraude si se tienen dudas razonables.
- **Emplear servicios de pago que mantienen registros de fraude:** Existen servicios online que permiten realizar consultas con los datos del pagador para ver su reputación, especialmente en el ámbito de las empresas.

De forma complementaria a estas comprobaciones, se recomienda el establecimiento de listas negras o blancas. Éstas mantienen un conjunto de clientes considerados fraudulentos o legítimos respectivamente, manteniendo un histórico de los indicios de fraude que se hayan podido detectar con anterioridad.

5.4. MEDIDAS PARA EVITAR EL FRAUDE

Además debemos realizar comprobaciones adicionales antes de aceptar el pedido, ya que en caso de fraude, con tarjetas robadas por ejemplo, la entidad financiera podría denegar el ingreso cuando vaya a hacerse efectivo y nunca se cobraría el producto enviado o el servicio prestado. Para evitarlo tomaremos las siguientes medidas **[3]**:

1. Retener, para revisar manualmente, los pedidos de más de cierto importe y los sospechosos:

- que se realizan a última hora de la noche o a primera de la mañana;
- que se originan en el extranjero;
- que tienen direcciones de entrega en apartados de correos;
- realizados desde correos electrónicos anónimos;
- que solicitan entrega urgente;
- que piden muchas unidades de un producto o varios;
- aquellas en las que el domicilio de entrega difiere del domicilio del pago;
- intentos de compras con el mismo número de tarjeta y diferentes fechas de caducidad;
- aquellos en las que el cliente llama muchas veces

2. Crear una base de datos de pedidos fraudulentos

3. Crear una red con empresas del sector para compartir estos pedidos fraudulentos

4. Comprobar los teléfonos contra bases de datos de teléfonos

5. Contactar con las entidades financieras ellas tienen muchos datos de tarjetas fraudulentas

6. Confirmar el teléfono del cliente llamándole

7. Registrar y revisar las llamadas de clientes y las conversaciones

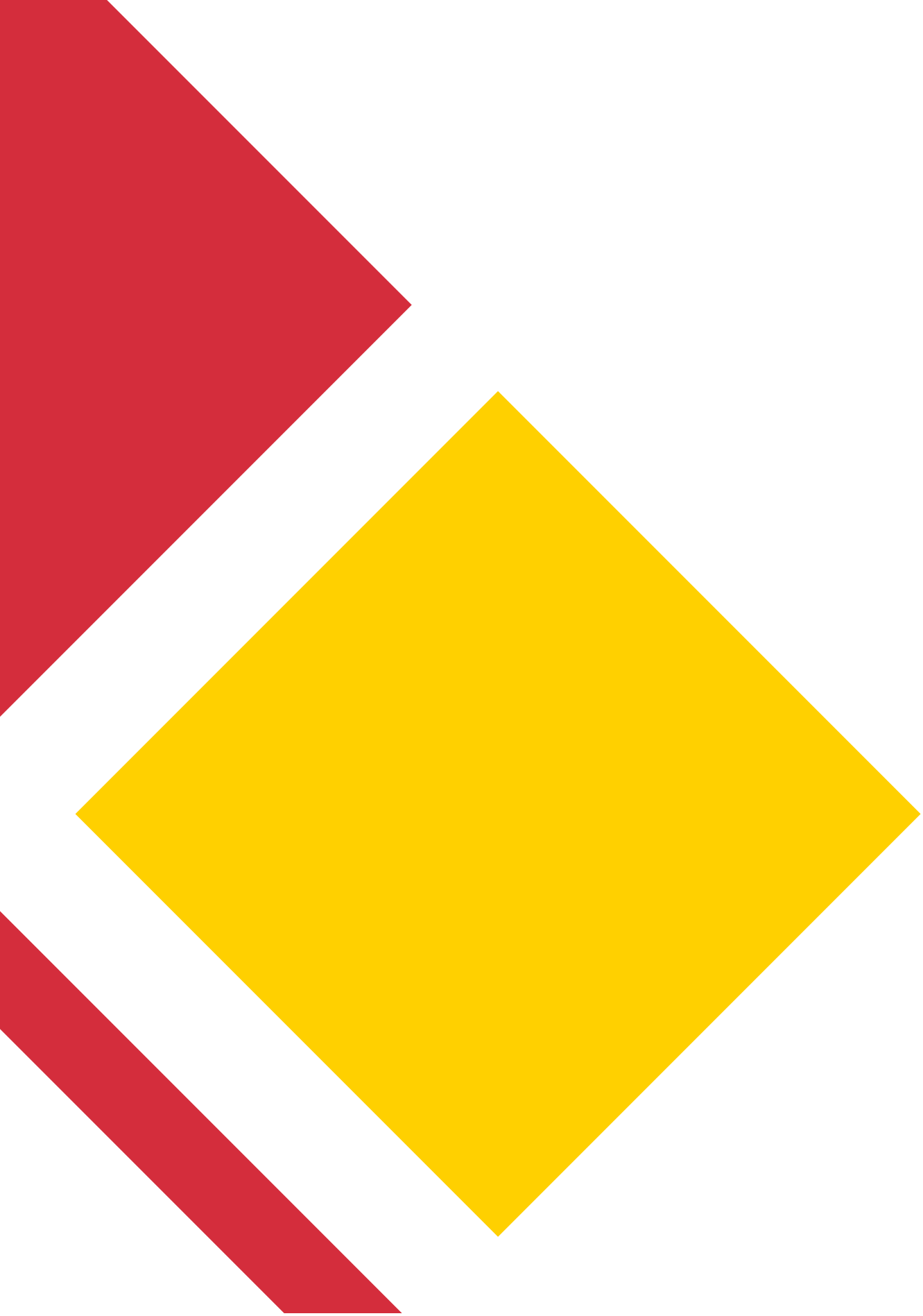
6. REFERENCIAS

[Ref - 1]. **INCIBE, Gestión de Fraude Electrónico -** https://www.incibe-cert.es/respuesta-incidentes

[Ref - 2]. **PCI (2016) *Payment Card Industry Data Security Standard* (PCI-DSS) - Estándar de seguridad de datos para la industria de tarjeta de pago -** www.pcisecuritystandards.org/document_library?agreements=pcidss&association=pcidss

[Ref - 3]. **INCIBE, *Checklist* de buenas prácticas al recibir un pedido -** https://www.incibe.es/sites/default/files/contenidos/dosieres/fraude-gestion-identidad-online/fraude-electronico-checklist-buenas-practicas-pedidos.pdf

[Ref - 4]. **INCIBE, Ganar en competitividad cumpliendo el RGPD: una guía de aproximación para el empresario -** https://www.incibe.es/protege-tu- empresa/guias/ganar-competitividad-cumpliendo-el-rgpd-guia-aproximacion-el-empresario



GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

protege tu empresa