Universidad de Valladolid

ESCUELA DE INGENIERÍAS INDUSTRIALES

UNIVERSIDAD DE VALLADOLID

ESCUELA DE INGENIERIAS INDUSTRIALES

Grado en Ingeniería de Organización Industrial

Análisis de problemas de seguridad en las tiendas online

Autor:

Baruque Martínez, Carlota

Tutor(es):

Gonzalo Tasis, María Margarita
Departamento de Informática (A y TC, CC e AI, L y SI)/Lenguaje y Sistemas Informáticos

Valladolid, Junio 2022

RESUMEN

El presente Trabajo de Fin de Grado tiene como objetivo analizar la seguridad de las tiendas online y el comercio electrónico.

A lo largo del documento se realiza un recorrido a través del comercio electrónico, su aparición, clasificación, características y demás conceptos, que prosigue con el análisis de los diferentes tipos de seguridad. Estas diversas perspectivas acerca de la seguridad exponen los activos que deben protegerse y permite analizar las amenazas a las que se enfrenta el comercio electrónico.

Todos estos conceptos analizados han servido de base para llevar a cabo la construcción de una tienda online segura que cumple con los estándares de la industria.

PALABRAS CLAVE

Comercio electrónico, tienda online, seguridad de la información, ciberseguridad, pasarela de pago.

ABSTRACT

The aim of this Final Degree Project is to analyse the security of online shops and e-commerce.

Throughout the document, a journey is made through the meaning of e-commerce, its emergence, classification, characteristics and other concepts, which continues with the analysis of the different types of security. These different perspectives on security expose the assets to be protected and allow for an analysis of the threats faced by e-commerce.

The analysis of these concepts have served as the basis for the construction of a secure online shop that complies with industry standards.

KEYWORDS

e-Commerce, e-tailer, information security, cybersecurity, payment gateway.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO 1. INTRODUCCIÓN Y OBJETIVOS

1. INTRODUCCIÓN Y OBJETIVOS

El auge del comercio electrónico ha supuesto un aumento del número de pequeños comerciantes que deciden abrir su tienda online, pero ha traído consigo también el aumento de los ataques cibernéticos. Se estima una pérdida de datos causada por ataques informáticos por valor de entre 2.000 y 50.000 euros anuales para las PYMES en España (González, 2021). En muchos casos supone el cierre de estas.

El robo de datos puede venir provocado tanto por una escasa protección de la seguridad de la empresa como por la falta de conocimientos básicos de ciberseguridad de las personas que la gestionan. El problema de la pequeña empresa es que no suelen disponer de profesionales encargados del control de la seguridad e incluso se subcontrata la construcción de la web a una empresa externa, al carecer ellos mismos de los conocimientos necesarios para su desarrollo.

El objetivo que persigue este trabajo es adquirir los conocimientos suficientes sobre el comercio electrónico y la seguridad de las infraestructuras tecnológicas que este utiliza. De este modo, tras identificar las amenazas a las que se ve expuesto este tipo de negocio, ser finalmente capaces de desarrollar una tienda online segura.

Para la consecución de estos objetivos, se ha construido una tienda online operativa basada en una empresa ficticia. En esta, se han aplicado los criterios de seguridad trabajados, obteniendo como resultado una tienda online segura.

Además de estos objetivos, mediante este trabajo, también se pretende concienciar a los usuarios acerca de los peligros de internet y proporcionarles recursos para llevar a cabo transacciones seguras.

1.1 ESTRUCTURA DEL DOCUMENTO

El documento se compone de 6 capítulos, constituyendo este el primero de ellos. En el se recoge una breve introducción al tema del trabajo además de su justificación y los objetivos perseguidos con este.

En el capítulo dos, se realiza un estudio acerca de el comercio electrónico, su surgimiento y situación actual, así como una descripción de las características y tipos existentes centrándose en el supuesto a estudiar.

El capítulo 3 ofrece una visión sobre qué es un sistema de información ya que es la herramienta que sustenta el funcionamiento de una tienda online, a partir de esto se identifican los elementos que lo componen y se aborda la seguridad de cada uno de ellos de forma diferenciada. Además, en este capítulo se introduce el concepto de seguridad percibida y se explica de forma simplificada qué es la privacidad de datos.

En el cuarto capítulo se identifican los activos a proteger en una tienda online y se realiza un análisis acerca de las diferentes amenazas a las que se enfrentan estas empresas. Para cada uno de los supuestos se propone una posible forma de protección.

En el quinto y último capítulo, se expone el caso de aplicación. En este se presenta la empresa creada y su objeto de negocio, así como los pasos seguidos para la construcción del sitio web y la elección de la pasarela de pago con la que se va a trabajar. El desarrollo del trabajo finaliza con la descripción de la estructura de seguridad confeccionada para la tienda online y un manual para la instalación de la tienda.

CAPÍTULO 2. COMERCIO ELECTRÓNICO

2. COMERCIO ELECTRÓNICO

2.1. APARICIÓN DEL E-COMMERCE

Cada vez que en la historia ha sucedido una transformación económica o tecnológica, esta ha sido desencadenada por el descubrimiento de una nueva forma de energía o producción.

En el siglo XVIII durante la Primera Revolución Industrial la energía de vapor fue la impulsora de la mecanización de la producción. En la Segunda revolución industrial los artífices del cambio fueron los avances en las comunicaciones y los transportes que sucedieron a finales del siglo XIX. Actualmente, todos los cambios tecnológicos que se han venido produciendo desde finales de los años 90 han dado comienzo a la conocida como "Era de la información".

En la trasformación actual, el agente que ha desencadenado el cambio es la información. El poder que esta proporciona ha propiciado cambios tales como la migración de los medios de generación de capital, transfiriéndose del sector industrial hasta el sector servicios, surgiendo una economía basada en el conocimiento.

El orden de prioridades en el mercado ha sufrido un cambio, llevando a otorgar mayor importancia a trabajos relacionados con el procesamiento y el almacenamiento de información que a los anteriormente más valorados, relacionados con la producción de bienes materiales.

Los cambios en el paradigma de la fabricación de bienes han venido produciéndose desde finales del siglo XX y han atraído la atención a la productividad y la eficiencia como nuevas claves de diferenciación para el desarrollo empresarial en el mercado. El objetivo actual de las compañías es la reducción máxima de los costes y una búsqueda continua de innovación respaldada por la nueva tecnología. La consecución de este objetivo ha traído consigo un gran reto que consiste en la coordinación entre la información y la tecnología.

A raíz de este reto, surge un nuevo concepto conocido como tecnologías de la información (IT). De las múltiples definiciones de este término, las dos siguientes destacan las claves principales para entender cual es realmente la función de las ITs.

"Aquellas tecnologías comprometidas en la operación, recolección, transporte, recuperación, almacenamiento, presentación y transformación de la información en todas sus formas..." (Boar, 1997)

"Toda la tecnología que es empleada por una organización para recolectar, procesar y diseminar información en todas sus formas. Por lo tanto, los componentes de las tecnologías de la información incluirán hardware (escáner, impresora, ordenador, etc.), software (sistemas operativos, lenguajes de desarrollo de aplicaciones, programas de oficina, etc.) ..." (Sarosa, 2003).

El punto en común que se puede extraer de estas dos definiciones es que cuando se trabaja con información todas las herramientas usadas, que posean componentes tecnológicos se convierten en tecnologías de la información. Debido a la importancia y vulnerabilidad que adquiere cada una de ellas dentro del proceso, es vital tener un control exhaustivo de ellas.

La combinación de las IT junto con el desarrollo masivo de internet, accesible para el usuario en los años 2000, provocó la aparición de lo que hoy se conoce como *ecommerce* o comercio electrónico. Puede darse una definición simple al concepto de comercio electrónico asociándolo a la compraventa de productos o servicios a través de medios informáticos, pero veamos algunas definiciones que amplían y precisan un poco más el concepto.

El ecommerce es el uso de las tecnologías de la información y las telecomunicaciones, que soportan las transacciones de productos o servicios entre las empresas, entre estas y particulares o con el Estado. (Malca, 2001).

Otra definición nos da la Ley 34/2002 del 11 de julio, de servicios de la sociedad de la Información y de comercio electrónico, estos son servicios prestados a distancia, por vía electrónica y a petición individual del destinatario. Igualmente se incluyen los servicios no remunerados por sus destinatarios cuando constituyan una actividad económica para el prestador de servicios. (Liberos, 2010).

Una particularidad observada en estas definiciones es que, en ningún momento se habla del método de pago utilizado, es decir, cuando la oferta y la aceptación de esta se realiza de forma on-line esto ya se incluye dentro del comercio electrónico, lo que quiere decir que en realidad el pago, si lo hubiera, no debe necesariamente hacerse de dicha forma.

2.2 SITUACIÓN ACTUAL DEL E-COMMERCE

En esta última década y sobre todo en los últimos años ha habido un incremento en la creación de nuevas empresas relacionadas con el ecommerce y aquellas que ya existían, han visto incrementada su facturación. Las barreras de geolocalización se han roto y poco a poco, lo que comenzaron como pequeñas compañías como es el caso de Amazon o SHEIN, han ido expandiendo su actividad a través de la red informática, llegando a casi todos los países del mundo y convirtiéndose así en gigantes multinacionales.

Lógicamente, este no ha sido el caso de todas las empresas que en su día comenzaron su camino en internet, la realidad para la mayoría de las PYMES era diferente. El uso de estas plataformas estaba principalmente reservado a grandes empresas y el comercio minorista no veía una oportunidad de expansión y desarrollo en el uso de tiendas online.

A la entrada de la nueva década del 2010 la dinámica cambió y trajo consigo una nueva realidad que se refleja en los siguientes datos publicados por el INE.

"*En 2019 en España un 46,9% de la población entre 16 y 74 años compraron online en los últimos 3 meses, una media ligeramente inferior a la de la UE que se situaba en el 52%.*" (Boletín informativo del Instituto Nacional de Estadística, 2020).

Si estos números que nos brindaba el final de la década ya eran esperanzadores para la venta online de las PYMES, la entrada del 2020 trajo consigo un cambio en el modelo del mercado mundial.

Debido a la necesidad de adaptación, se produjo una gran rotura mundial de las barreras del comercio electrónico afectando en gran medida a los pequeños empresarios. La tendencia de consumo online sufrió un crecimiento nunca visto, *en junio de 2020, las ventas del comercio minorista por este canal fueron un 71,2% superiores al mismo mes del año anterior* (Boletín informativo del Instituto Nacional de Estadística, 2020).

Una parte importante de ingresos para muchos negocios españoles se encuentra actualmente en sus ventas por internet.

2.3 ESTRUCTURA DEL COMERCIO ELECTRÓNICO

Una vez conocida la importancia que ha cobrado este tipo de negocio tanto en nuestro país como en el mundo, es imprescindible entender cómo funciona realmente este proceso, en qué se apoya y qué herramientas se utilizan para su creación.

La infraestructura que permite a un negocio de comercio electrónico funcionar es en su origen la misma que la de uno tradicional, pero con algunos recursos adicionales.

Esta nueva infraestructura se representa dividida en cinco secciones:

- Infraestructura de servicios comerciales comunes: directorios, catálogos, tarjetas inteligentes de seguridad o autentificación y instituciones intermediarias en pago electrónico.

- Infraestructura de interfaces: bases de datos de consumidores, agendas de clientes y aplicaciones.

- Infraestructura de mensaje y distribución de información: Intercambio electrónico de datos (EDI), correo electrónico y protocolo de transferencia de hipertexto (HTML)

- Infraestructura para publicidad y lenguajes multimedia: VRML, HTML, XHTML, Java Script.

- Infraestructura de red: Internet (VAN, LAN, WAN), intranet, extranet.

Esta división se justifica haciendo referencia a los elementos con los que interacciona. Estos elementos son personas, políticas, estándares técnicos o protocolos y entidades u organizaciones.

Lo que se entiende en este contexto por **personas**, se refiere a cualquiera que tenga relación con la compraventa del producto o servicio, vendedores, compradores e intermediarios.

En el caso de las **políticas** se tratan de las normas por las que se rige la transacción, refiriéndose tanto a las políticas privadas de la compañía como a las normas legales que hay que cumplir o lo que en las empresas software se llama reglas de negocio.

Desde el punto de vista del vendedor, aparecen además los **estándares técnicos y protocolos,** estos proporcionan la seguridad necesaria para llevar a cabo las transacciones y reducen el peligro que conlleva el uso de diferentes medios de pago. Por último, intervienen también en la actividad otras **entidades y organizaciones** aparte del propio mercante, como puede ser socios, gobierno o la propia empresa.

Al plantearse construir una tienda online, debido a que existen múltiples opciones para la infraestructura deben tenerse en cuenta las particularidades del negocio, para lo que es necesario realizar un proceso de selección de herramientas preciso y que tenga en cuenta la capacidad de este.

2.4 TIPOS DE COMERCIO ELECTRÓNICO

Conocer los diferentes tipos de negocios que existen puede ser muy conveniente a la hora de identificar los recursos que van a ser necesarios para gestionarlo de forma eficiente.

Debido a que existen muchas clasificaciones referidas a los comercios electrónicos comenzar está basándonos en los agentes que intervienen, puede ser una herramienta que facilite el proceso. Existen cinco variantes en esta división que se describen brevemente a continuación:

B2C (Business to consumer)

La venta se realiza directamente de empresa a comprador, el producto es adquirido por la empresa a través de proveedores y el articulo se vende sin realizar sobre él modificación alguna al cliente por un precio superior.

B2B (Business to business)

Este tipo de negocio está incluido en una transacción B2C, el proveedor que vende mercancía al vendedor. La empresa vendedora suele ser mayorista y la compradora en cambio realiza ventas al pormenor. La compra, el proceso de órdenes y la gestión de inventarios suelen gestionarse de forma online, aunque el pago suele realizarse utilizando medios tradicionales.

Este tipo de ecommerce suele ser planteado a largo plazo, las relaciones entre las dos compañías se plantean para ser duraderas.

C2C (Consumer to consumer)

La venta entre particulares es la forma de comercio electrónico más antigua que conocemos. Son plataformas que utilizando anuncios actúan como mercados y ponen en contacto a usuarios y les ayudan a negociar. Actualmente un buen ejemplo de este tipo de comercio electrónico es Vinted.

B2B2C (Business to business to consumer)

Este modelo agrupa el B2B y el B2C, el negocio que proporciona el servicio o producto es puesto en contacto con el comprador a través de otra empresa que actúa de escaparate (suele ser un nombre con reconocimiento).

Este modelo consigue reducir riesgos, aumentar el número de potenciales clientes al que llegar, pero el objetivo final será conseguir transformar el negocio a B2C.
Esta forma de trabajar es característica de la multinacional Amazon, que actúa de escaparate para vendedores más pequeños amparándoles bajo su reputación.

B2E (Business to employee)

Una empresa realiza intercambios comerciales con sus trabajadores, beneficiándose ambas partes de la operación. Los trabajadores consumen los productos de la empresa para la que trabajan y a cambio esta les realiza un descuento en la operación.

El problema de esta clasificación es que está relativamente desfasada e incompleta ya que, únicamente tiene en cuenta a los actores que intervienen en la actividad despreciando cómo la empresa obtiene sus ingresos.

A raíz de esto, ha surgido una forma de diferenciación mucho más completa para el mundo del e-Business, que precisamente se basa en el modelo de negocio empleado. Pero ¿Qué es un modelo de negocio?

“Un modelo de negocio operativo es la lógica nuclear de la organización para crear valor. El modelo de negocio de una empresa orientada a los beneficios explica cómo ésta hace dinero.” (Linder, 2000).

Es decir, el concepto que diferencia a los tipos de modelo es la forma en la que negocio genera beneficios a través de internet. A raíz de esto aparece la siguiente clasificación:

Etailers

Tiendas online o también conocidas como *pure players.* Su propio nombre describe el modelo, etailers se trata de una combinación entre *electronic* y *tail*, este último proveniente *de retailer* cuyo significado es minorista.

Es un distribuidor que pone a la venta diferentes productos que adquiere a través de proveedores, trabajando como una tienda tradicional, pero utilizando el canal online en vez de el físico.

El beneficio obtenido proviene del margen de precio entre la compra al proveedor y el de venta.

Bricks & Clicks

Consiste en una mezcla entre la tienda física y la online. El propietario decide ampliar su mercado incluyendo una tienda a online a la tradicional consiguiendo una expansión a un coste relativamente bajo. Además, la apertura de una tienda online amplia la venta, sin restricciones en el horario o la localización del cliente.

En este modelo los beneficios provienen de la expansión y desaparición de esas limitaciones.

Marketplace

Este concepto puede describirse como el mercado que tiene lugar en la plaza de cualquier ciudad, pero siendo ampliado geográficamente. Existe una plataforma, la plaza, que actúa como punto de encuentro entre vendedores y compradores, mercado. Esta web pone en contacto a mayoristas o minoristas que publican sus productos, con los clientes que quieren comprar.

La forma en la que este tipo de webs obtienen beneficios varía, una de ellas consiste en el cobro de cuotas de suscripción a los vendedores por el servicio de escaparate que se brinda, otro de los orígenes es el cobro de una comisión por cada venta realizada y además suelen ofrecer posibilidades de posicionamiento y publicidad de los productos por el que se cobra una pequeña cantidad de dinero.

Sharing economy

Funciona como el C2C y funciona de forma similar al *marketplace,* pero en este caso el uso está reservado a particulares. Estos comparten los recursos que no utilizan con otros usuarios para poder compartir gastos o conseguir beneficios, además ponen al alcance de todos servicios y productos antes reservados únicamente para profesionales.

El beneficio se obtiene a través del cobro de porcentajes por transacción además de herramientas de posicionamiento y publicidad dentro de la plataforma.

Comparadores

Estas webs no proveen directamente ningún producto, sino que ofrecen un servicio de comparación entre diferentes proveedores del mismo servicio o producto, facilitando a los compradores la decisión y proporcionando información respecto a las características de estos proveedores y lo que venden. La compra no se realiza en la web del comparador, sino que se redirige a la web del proveedor para realizar la transacción.

Los beneficios se obtienen gracias a conceptos como el CPL (coste por lead), las empresas pagan por la generación de clientes potenciales, que están interesados en sus productos y dejan algún tipo de interacción en la página como puede ser la registrarse en esta. Se utilizan además otras formas cobro como son los ingresos compartidos.

Afiliados

El marketing de afiliados tan en auge actualmente trabaja como una página donde se promociona e incita a la compra de productos y servicios de otras tiendas. Habitualmente mediante anuncios se realizan campañas publicitarias para captar potenciales compradores y se recibe una compensación económica por las ventas realizadas. Sin embargo, existen otras formas de generación de ingresos, que son las mismas que las que emplean los comparadores.

Aunque a veces es difícil clasificar un negocio en una de las categorías e incluso es posible que los consumidores no puedan diferenciarlos, el uso de esta etiqueta de modelo de negocio favorece a la gestión técnica de la información con la que trabaja.

En el caso de este estudio, al trabajar con el modelo de tienda online o *etailer*, es conveniente profundizar un poco más en el y explicar más detalladamente sus características.

2.5 TIENDA ONLINE

Las conocidas con su término en inglés pure-players, son realmente habituales en el mercado global, cada vez más emprendedores deciden construir su negocio prescindiendo de la parte física de este y por ende de sus costes asociados.

Al no contar con las ventajas que aporta la tienda tradicional, como la posibilidad de adquirir el producto inmediatamente, poder observar este antes de comprarlo o la atención al cliente personalizada, es necesario que el negocio ofrezca un valor añadido para conseguir que sea rentable a medio plazo. Existen dentro del comercio online tres variables comúnmente empleadas para este fin: el precio, la comodidad y el amplio catálogo.

El margen de beneficio bruto que obtiene el propietario de este negocio es la diferencia entre el precio de compra al proveedor y el de venta al cliente. Al descontar los costes variables que pueden venir derivados de, por ejemplo, la logística o la comisión por transacción, aparece el beneficio neto. Siempre que el beneficio neto sea superior a los costes fijos derivados del almacenamiento, el mantenimiento de la web, etc. el negocio será a largo plazo rentable.

2.5.1 AGENTES INTERVINIENTES

A lo largo del proceso de comercio electrónico que se lleva a cabo en una tienda online, aparecen una serie de agentes que participan de forma directa en la transacción y que desempeñan diferentes funciones. Para que este proceso sea exitoso es necesario que todos los agentes intervinientes lleven a cabo sus tareas correctamente.

Aunque no existe un consenso sobre cuales son los agentes principales, pues se pueden distinguir diferencias según la fuente consultada, si existen tres agentes que son un denominador común para todas.

El **comerciante**, que ofrece sus productos o servicios a través de Internet, directamente relacionado está el **cliente** que es el que adquiere a través de la plataforma web los productos o servicios ofertados. Una vez llevado a cabo el

proceso de selección del producto por parte del cliente llega el momento de realizar el pago, en este punto entra en juego el siguiente agente, la **entidad financiera** que se encarga de llevar a cabo la transacción y se asegura de que el vendedor reciba el dinero abonado por el comprador.

Esta selección principal de agentes deja fuera a otros que no están actúan directamente en la transacción y que están más relacionados con el suministro de la tecnología que permite llevar a cabo el proceso. Pudiendo ser considerados como agentes secundarios, están el **operador de comunicaciones**, que pone en contacto al cliente con el vendedor de forma remota, el **operador logístico** que se encarga de poner en contacto de manera física a estos dos agentes, realizando por ejemplo la entrega del producto adquirido al cliente y, por último, el **proveedor de servicio o acceso a internet,** que proporciona a ambos, comprador y vendedor, el acceso telemático.

2.5.2 VENTAJAS E INCONVENIENTES

Algunas de las ventajas e inconvenientes que el comercio electrónico trae consigo, son muy sencillas de imaginar, pero es conveniente observar con detenimiento algunas de estas para poder explotar y minimizar sus respectivos efectos. Es además importante diferenciar entre quien es el agente afectado, comprador o vendedor.

En primer lugar, algunas de las **ventajas** que percibe el **vendedor** al trabajar con una tienda online son expuestas a continuación:

- Eficiencia y flexibilidad. La tienda online permite realizar pruebas y cambios de productos, precio y estrategias en tiempo real, obteniendo los resultados reales de cómo estos afectan a los potenciales clientes y permitiendo tomar acciones correctoras inmediatas. La flexibilidad de cambio permite, por ejemplo, el lanzamiento de un nuevo producto y su adición a la base de datos. Estas características facilitan notablemente el desarrollo de estrategias de marketing y operaciones internas.

- Eliminación de limitaciones geográficas. La ampliación al mercado global permite la accesibilidad a cualquier cliente, independiente de donde se ubique gracias a las empresas de envíos pueden realizarse entregas rápidas y seguras a prácticamente cualquier lugar.

- Disponibilidad. El horario se amplia a las 24 horas del día, los 365 días al año, lo que implica una posibilidad de generación de ingresos permanente.

- Redes sociales. Es posible realizar un plan de publicidad y darse a conocer a través de las redes sociales de forma gratuita o con una mínima inversión. Es posible incluso, el envió de boletines informativos y ofertas personalizadas a los clientes a través de los perfiles de la tienda o el correo electrónico.

- Reducción de riesgo. La inversión inicial y el costo del mantenimiento es mucho menor a la de un comercio tradicional. Además, el miedo a realizar cambios y variar estrategias es menor pues el dinero puesto en juego también lo es.

- Fuente de información. A través de la página web puede recopilarse información fundamental acerca de las preferencias de los clientes que pueden utilizarse para aumentar ventas y mejorar la rentabilidad.

- Gestión virtual. La posibilidad de tener toda la documentación informatizada y su modificación de manera inmediata es disponer de información veraz a tiempo real.

En el caso de la persona que adquiere el producto o servicio, el **cliente**, las principales **ventajas** son:

- Información. Acceso a gran cantidad de información acerca de cada producto, sus especificaciones o precios, facilitando la comparación de estos.

- Personalización. Una vez habiendo hecho una búsqueda o compra en una página, los datos acerca de preferencias quedan registrados y se realizan sugerencias y ofertas en función a tus gustos.

- Disponibilidad. Se puede realizar una compra las 24 horas del día, los 365 días al año.

- Accesibilidad. Posibilidad de comprar marcas o productos que carecen de tienda física cerca de su localización e incluso de comparación de calidad y precios para escoger el mejor proveedor.

- Flexibilidad en el pago. A diferencia del comercio tradicional que limita las formas de pago a efectivo y tarjeta de crédito (aunque actualmente algunas están añadiendo Bizum como posibilidad), el pago por internet plantea una infinidad de posibles vías de pago además de las tradicionales. Algunas de ellas son contra-reembolso, transferencias, PayPal, etc.

- Comodidad. Puedes realizar una compra sin necesidad de desplazarte, desde la comodidad de tu casa y recibirla dentro de tu preferencia horaria.

A parte de esta serie de ventajas, también existen una serie de **inconvenientes** que afectan tanto a cliente como vendedor pero que podrían considerarse más bien como retos. Son los siguientes:

- Nuevas tecnologías de la información. Implica una inversión en tecnología, tanto su creación como su mantenimiento, aunque la gestión no es compleja de realizar, sí lo es su orientación y la adquisición de nuevos conocimientos si nunca se ha trabajado con estos medios. Un mal planteamiento o uso de estas herramientas puede dificultar la experiencia del usuario durante la compra.

- Captación de clientes. Aunque la tienda online te dé acceso sin barreras de ubicación a cualquier cliente, esto también implica que el resto de las compañías también lo tienen, es necesario buscar un punto diferenciador. Tener acceso a tantas opciones e información a veces dificulta y retrasa la toma de decisiones.

- Gestión de la seguridad. El acceso a gran cantidad de datos puede ser útil bien administrado, pero implica a su vez una gran responsabilidad para con los clientes. Es necesario tanto una buena seguridad como la percepción de esta por los compradores, que exponen sus datos personales a posibles usuarios con malas intenciones.

- Compatibilidad. Es necesaria una buena evaluación de compatibilidad entre los programas de gestión de ecommerce elegidos y los formatos de bases de datos o ficheros con los que se trabaja, ya que puedan llegar ser necesario una adaptación de estos complicando la construcción y funcionamiento de la tienda online. Un mal diseño web puede conllevar la incompatibilidad con algunos servidores o incluso dispositivos.

- Incertidumbre legislativa. A pesar de que el ecommerce ya esta a la orden del día, la realidad es que existe un espacio en blanco legislativo que no termina de regular la actividad en su totalidad, por lo tanto, tampoco se respaldan completamente los derechos de los compradores.

2.6 PASARELAS DE PAGO

El momento de realizar el pago es el momento más crítico en una tienda online. El proceso puede romperse únicamente por la desconfianza que el consumidor sienta a la hora de introducir sus datos bancarios. Por ello, además de por inferir directamente en los ingresos generados por la empresa, la selección de la pasarela de pago adecuada es crucial al construir una tienda online.

2.6.1 FUNCIONAMIENTO DE UNA PASARELA DE PAGO

Una pasarela de pago es una aplicación software que permite a una tienda online la transferencia segura de información bancaria del cliente a la red encargada del procesamiento del pago.

A la hora de realizar una compra online, el flujo de información atraviesa una serie de aplicaciones, que pertenecen a diversas entidades. Cada entidad es responsable de que la información en su poder se almacene o transmita de forma segura.

A continuación, se explica de manera detallada la ruta realizada por la información desde que sale del cliente hasta que la tramitación del pago concluye.

Solicitud de pago (Cliente - Pasarela de pago)

En primer lugar, el cliente accede a la tienda online a través de un navegador web, esta es la primera entidad que manipula la información suministrada. El navegador encripta los datos y los envía a el servidor web en el que se aloja la tienda online.

La aplicación de la pasarela de pago, integrada en la tienda online, envía la información idealmente encriptada al sitio web de la pasarela de pagos.

Una vez esto sucede, la información pasa a manos de entidades externas a la tienda.

Para asegurar la seguridad de esta comunicación es necesario que el sitio web del comerciante posea un certificado Secure Socket Layer (SSL) que encripte la información de todo el sitio web de la tienda.

Obtención de permiso (Pasarela de pago – Banco emisor)

La pasarela de pago se pone en contacto con el procesador de pagos empleado por el banco adquiriente, es decir, el del comerciante, para hacerle llegar la información bancaria del cliente.

El procesador de pago transmite los datos a la asociación de tarjetas a la que pertenezca la tarjeta del comprador, que suele tratarse de MasterCard o Visa, que redirige la transacción al banco emisor de la tarjeta.

Una vez el banco del cliente recibe la solicitud, esta comprueba si existen fondos suficientes para poder hacer frente al pago. La respuesta, es enviada en forma de código que indica si ha sido aceptada o no, es transmitida hasta llegar a la tienda web.

Proceso de cobro (Pasarela de pago – Banco adquiriente)

En caso de que el proceso se haya realizado correctamente y que la respuesta obtenida haya resultado afirmativa, se envía la autorización del comerciante a través del procesador de pagos hasta el banco adquiriente. El banco deposita los nuevos fondos en la cuenta comercial del vendedor que posteriormente pueden ser transferidos a la cuenta bancaria del comerciante.

2.6.2. FACTORES QUE TENER EN CUENTA

A la hora de seleccionar con que pasarela de pago trabajar es importante dar prioridad a algunos aspectos, con el objetivo de adecuar la elección a las necesidades propias de cada tienda online.

Métodos de pago disponibles

Existen tres aspectos importantes relativos a la elección de las formas de pago disponibles.

La primera, la fiabilidad y seguridad que proporcionan a las partes intervinientes.

En segundo lugar, la adecuación de estos al sector del mercado al que se dirige la tienda. La edad, el nivel de ingresos o incluso el área geográfica hacen que los

clientes tengan preferencia hacia determinados métodos de pago, no es lo mismo que el mercado objetivo sean personas de mediana edad, más reticentes a la compra online a que sean jóvenes, ya acostumbrados a estas transacciones.

Por último, la variedad, más posibilidades implican más opciones de acierto con las preferencias del potencial comprador.

Los principales métodos de pago que barajan las pasarelas de pago son:

A. Tarjetas de crédito

El medio de pago más extendido en el comercio online. La mayoría de las transacciones se llevan a cabo directa o indirectamente a través de estas.

VENTAJAS	DESVENTAJAS
Universalidad	Validación de datos compleja
Integración sencilla	Cancelación de pago post-venta
Fácil gestión	Cargos de devolución de pago
Cobro inmediato	Fraude
Comisiones bajas	

Tabla I. Ventajas y desventajas de las tarjetas de crédito

B. PayPal

Compañía nacida digitalmente, permite al usuario pagar desde una cuenta de la propia entidad, en la que tiene asociado uno o varios medios de pago. PayPal trabaja con medios de pago como tarjeta o transferencia bancaria además del monedero electrónico. En este, se almacena un saldo asociado a la cuenta y se puede retirar en cualquier momento.

VENTAJAS	DESVENTAJAS
Uso muy extendido	Pérdida de control en la compra
Confianza al no proporcionar datos	Comisiones y tasas altas
Global	
Integración sencilla	
Buena experiencia usuario	
Seguridad y soporte técnico	

Tabla II. Ventajas y desventajas de PayPal

C. Transferencia bancaria online

Es una versión de la tradicional transferencia bancaria, pero en este caso el pago se realiza instantáneamente y se omite la información de la cuenta receptora, que está incluida en la pasarela de pago. Los bancos emisores suelen hacer uso del sistema de seguridad 3D secure o algún sistema de doble verificación.

VENTAJAS	DESVENTAJAS
Bajas comisiones al vendedor	Necesaria activación del cliente
Bajo coste o nulo	Integración compleja
Seguridad en ambos sentidos	Incremento de pasos de procesamiento
Universalidad	Falta de estandarización entre entidades bancarias
Rapidez	

Tabla III. Ventajas y desventajas de las transferencias online

D. Transferencia bancaria tradicional

Se trata de un proceso que, aunque se lleva a cabo por internet, no es necesaria su integración en la pasarela de pago. Una vez la compra y el pago son realizados por parte del cliente, el vendedor verifica este a través del comprobante de pago que el cliente remite.

VENTAJAS	DESVENTAJAS
No coste para el vendedor	Medio Lento
Seguro para el vendedor	Proceso lento para el cliente
No manejo de datos bancarios	Gestión compleja e ineficiente
Universalidad	

Tabla IV. Ventajas y desventajas de las transferencias bancarias tradicionales

E. Contra reembolso

Esta opción de pago puede ser empleado por una tienda online sin la intervención de una pasarela de pago. El comprador paga en efectivo al repartidor al recibir el pedido.

VENTAJAS	DESVENTAJAS
Seguridad en ambos sentidos	Costes altos para el vendedor
Proceso de compra sencillo, prescinde de pago	Fácil cancelación post compra
Elimina desconfianza	Lentitud
Atracción a tienda física	Complejidad administrativa

Tabla V. Ventajas y desventajas del contra reembolso

F. Pago con criptomoneda

Este medio de pago esta incrementando lentamente su popularidad, no son muchas las tiendas que lo ofrecen por lo que puede ser un punto diferenciador entre los competidores. Para realizar transacciones es necesario disponer de una billetera electrónica (*wallet*).

VENTAJAS	DESVENTAJAS
Global	Poco popular
Exclusividad	Desconocimiento general
Sin comisión	Volatilidad
Cobro inmediato	
No rastreable	

Tabla VI. Ventajas y desventajas del pago con criptomonedas

Costes de uso e instalación

Los gastos asociados al uso de este tipo de servicios pueden ser divididos en tres grupos, costes de instalación, costes de utilización y costes bancarios derivados.
No siempre todos estos gastos están presentes, por lo que la correcta selección toma aún más importancia.

Al ser integrada la pasarela dentro del sitio web de la tienda, pueden aparecer varios escenarios. En el primero, la empresa encargada de la construcción de la tienda online se hace cargo, cobrando o no un suplemento. Otro de los casos, es cuando la plataforma de pago es la que realiza su propia instalación, incurriendo en un coste adicional en el comerciante. Por último, en el supuesto de que sea instalada por el propio comerciante, conocedor de este tipo de tecnología, el coste no será económico sino de oportunidad y tiempo.

Entre los costes asociados a la propia pasarela de pago, pueden aparecer principalmente costes de registro, cuota mensual, tasa por transacción, tasa por transferencia de fondos (en caso de estar almacenados en una cuenta mercantil de la propia plataforma) y cargos por cancelación de pedido.

Es importante comparar exhaustivamente los precios ofrecidos por las distintas plataformas ya que algunos, como las tasas por transacción, pueden suponer un gran decremento de los beneficios.

En último lugar, es común el uso de una cuenta mercantil como intermediaria en la transferencia del dinero entre la cuenta del cliente y la del vendedor. El dinero se almacena en esta hasta que el banco del comprador aprueba la transacción, una vez esto sucede, el dinero se transfiere de la cuenta mercantil a la cuenta bancaria del vendedor.

Existen pasarelas de pago que ofrecen la opción de crear una cuenta en la plataforma que actúa como cuenta mercantil y prescinde de las cuentas externas, por lo que este gasto se evitaría. En el caso de una cuanta externa sea requisito para el uso de la plataforma elegida, aparecen unos gastos adicionales al crearla con la entidad bancaria.

Compatibilidad entre la pasarela y el sitio web

Este factor es el más importante, ya que, si la viabilidad de instalación y trabajo conjunto entre la pasarela y el sitio web es baja, la opción debe ser rápidamente descartada. Una vez conseguida la complicada tarea de la venta, esta no puede interrumpirse debido a errores o dificultades técnicas, pues supondría una perdida de ingresos inaceptable.

Una vez comprobada la compatibilidad de tecnologías, el proceso de integración toma importancia. Algunos aspectos para valorar son, la necesidad de un programador externo, la sencillez en la instalación, uso de API (Application Programming Interface), el tiempo necesario para su puesta en funcionamiento o la posibilidad de personalización de la interfaz.

Seguridad proporcionada

El factor más importante tras la viabilidad técnica es la seguridad, tanto para el vendedor como para el comprador. Debido a la influencia que tiene la percepción de la seguridad en el desarrollo de una posible transacción, es necesario contar con una plataforma totalmente fiable.

Hay tres requisitos que una pasarela debe cumplir para garantizar su máxima protección:

1.Estándares PCI DSSS: estos estándares han sido establecidos por la industria de pago por tarjeta empleando métodos de encriptación y protección de datos.

2.Cuentas mercantiles: estas pueden ser externas (pertenecientes a una entidad bancaria) o internas (propias de la plataforma). Este tipo de cuentas ofrece una capa extra de protección contra el fraude.

3.Sistemas autentificación multifactorial: el más empleado es el 3D Secure, que garantiza la autentificación del comprador como legítimo.

Además del cumplimiento de estos requisitos, es aconsejable consultar información referente a las medidas de prevención, detección y lucha contra el fraude que aplica la plataforma. Es útil para comprobar su actuación en estos casos, obtener información sobre brechas de seguridad ocurridas recientemente y las medidas tomadas al respecto.

Experiencia de usuario

El objetivo de una tienda online es realizar una venta, el punto más crítico de este proceso es la introducción de información bancaria, por ello debe hacerse lo más sencillo y visualmente seguro posible.

Deben tenerse en cuenta en la selección aspectos como el número de pasos a completar o la cohesión entre la apariencia de la pasarela de pago y la tienda.
Cuando el proceso incluye un paso ajeno a la propia web, la probabilidad de que el cliente abandone el pago es mayor ya que, los entornos de la tienda y de la pasarela no siempre coinciden, incrementando la desconfianza y con ello las posibilidades de frustrar la transacción.

Para mantener la percepción de seguridad construida en la web es muy importante armonizar lo máximo posible la apariencia del sitio web y la pasarela, siendo la posibilidad de personalización de la interfaz de la segunda, un factor extremadamente importante en las pequeñas y medianas empresas online.

Calidad de servicio y atención

Aunque la importancia de este factor parezca inferior a la del resto, la respuesta ante un posible fallo es vital para minimizar el numero de ventas perdidas. Se debe tener en cuenta el tipo de atención al cliente que se ofrece, diferenciando entre una central telefónica o la atención personalizada. La mejor opción es consultar a algún usuario que trabaje con la plataforma acerca de su experiencia o buscar opiniones de clientes publicadas en foros online.

Posibilidad de expansión

Si el objetivo de la empresa es la venta internacional, es importante contar con una pasarela de pago que soporte diferentes divisas o que en futuras etapas del negocio pueda añadirse además de que permita transacciones y operaciones internacionales.

Almacenamiento de datos bancarios

La información bancaria debe ser almacenada siguiendo el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS). Existen dos opciones al diseñar el procedimiento de pago, diferenciados según donde introduce el cliente la información bancaria:

En el sitio web de la tienda

Mediante el uso de un formulario de pago integrado en esta, el cliente introduce la información en el sitio web del vendedor. Este formulario, mediante el uso de llamadas API, envía los datos a la pasarela de pago segura. Es importante remarcar que el uso de API puede requerir de programación para ponerlo en funcionamiento.

La principal ventaja de este flujo de información seleccionado es la experiencia del usuario ya que permanece en todo momento en la web de vendedor. Pero, por otro lado, este punto a favor puede verse opacado por la responsabilidad de seguridad adquirida por el vendedor al ser primer recolector de la información sensible.

Redirección para pagos

Una 3ª parte toma partido, generalmente al proceder al pago, el cliente es redireccionado a la propia pasarela de pago. En esta página, el cliente introduce la información y comienza el procesamiento de pago.

En este caso, la responsabilidad de seguridad del vendedor disminuye, otorgándole la responsabilidad total de recolección de datos bancarios a la pasarela. Al contrario que en el caso anterior, se perderá parte de la calidad de experiencia del usuario lo que puede reducirse si la pasarela permite la personalización de la interfaz.

Ambos flujos de pago tienen sus ventajas e inconvenientes, por lo que su elección en cuestión de preferencias y necesidades. Independientemente del flujo elegido, existe en algunas pasarelas la posibilidad de almacenaje de los datos bancarios en vez de guardarlas en el servidor de la propia empresa.

2.6.3 OPCIONES

Dentro del mercado se ofertan innumerables compañías dedicadas al procesamiento de pagos en línea, pero como se ha visto en el anterior apartado, el número elevado de variables hace que todas sean diferentes entre sí.

A continuación, han sido seleccionadas y analizadas algunas de las compañías más interesantes en cuanto a pasarelas de pago que operan al menos, en el mercado nacional español.

PayPal

Fundada en 1998, se trata de la pasarela de pagos más utilizada en todo el mundo. Con mas de 250 millones de clientes es la compañía de pago virtual para ecommerce más antigua.

Cada usuario en PayPal dispone de una cuenta a la que vincula sus tarjetas o cuentas bancarias, además puede enviar y recibir dinero que es sumado o restado a el saldo de la cuenta. A parte de estos métodos de pago, también dispone de tecnologías que permiten realizar compras a través de códigos QR, email o llamadas telefónicas de forma completamente segura.

La integración de la pasarela en el sitio web es muy sencilla de realizar y se hace mediante una API, siendo necesaria la creación de una cuenta de comerciante en la plataforma.
Ofrece la posibilidad a los vendedores de personalizar la pantalla del proceso de pago, haciendo posible que los clientes no tengan que abandonar la web de la tienda u abandonando esta hacia la interfaz mundialmente conocida de PayPal.

Gran parte del triunfo de esta compañía viene dado a la seguridad que ofrecen a sus clientes, tanto compradores como vendedores. Al vincular sus datos bancarios, los clientes evitan la sobreexposición de estos, contando por otro lado con el sistema de doble factor 3D Secure reduciendo el riesgo de fraude y utilizando un sistema encriptación de la información de alto nivel. Como añadido a la seguridad de todos los usuarios, tanto vendedores como compradores, cuenta con un sistema de devolución de dinero muy eficaz en caso de fraude.

Este servicio es gratuito para los compradores mientras que los vendedores deben pagar unas tarifas por transacción realizada, aunque no requiere de una cuota por apertura, mantenimiento o mensualidad. En el caso de España, la tarifa es de 2.9% de la compra más una tarifa fija de 0.35 €.

Figura 1. Logotipo de PayPal

Stripe

Este proveedor de pasarela de pagos es una de las más conocidos mundialmente y cuyo uso está muy extendido entre PYMES. Acepta más de 135 divisas diferentes, convirtiéndola en una gran opción para negocios internacionales.

¿Cómo funciona? Almacena datos de pago del cliente como PayPal, ofreciendo un panel de control en el que se visualizan todas las transacciones que se han iniciado, así como su estado final. Por último, ofrece muchas estadísticas acerca de las transacciones, lo que permite identificar las debilidades de este y actuar para mejorarlas.

En cuanto a los métodos de pago disponibles están AliPay, ApplePay, GooglePay, transferencias bancarias, tarjetas de crédito y débito además de muchos otros más empleados en otros países.

Una de las grandes ventajas que ofrece, es la sencillez en la integración de esta en la tienda online. Esto, se lleva a cabo mediante una API, que es personalizable y adaptable a la apariencia de la web, lo que resulta en una notable mejora de la experiencia del usuario. Su instalación y uso no precisa de altos conocimientos de programación y pueden ser puestas en marcha nada más instalarse.

La apertura y mantenimiento de una cuenta en Stripe es gratuita, y sus tarifas de procesamiento de pago son de 1.4% de la transacción más 0.25 € para tarjetas europeas.

En cuanto a la seguridad que ofrece, dispone de protección antifraude basada en la inteligencia artificial, un cifrado AES e infraestructura integrada, convirtiéndola en una plataforma realmente segura. El almacenamiento de datos bancarios se lleva a cabo mediante una *tokenización* de estos, manteniendo así la información totalmente segura.

Las opiniones en cuanto a la calidad de su servicio técnico son mejorables y existe un problema de inestabilidad recurrente en las cuentas. El pago tarda 7 días en llevarse a cabo.

Figura 2. Logotipo de Stripe

Redys

Esta empresa española es una de las pasarelas de pagos más utilizadas en las tiendas españolas, nació en 1981 de la unión de los sistemas de pago Sermepa y Redy. Esta compañía trabaja como TPV virtual para la mayor parte de los bancos que operan en España, ofrecen variedad de idiomas y divisas con las que trabajar además de que su reputación proporciona gran tranquilidad a los clientes.

Ofrece gran variedad de métodos de pago, entre los que se incluyen Bizum, PayPal, GooglePay, ApplePay, Masterpass, transferencias bancarias y tarjetas de crédito o débito.

En cuanto a su integración, dispone de una API de sencilla instalación mediante Plug&Play compatible con sitios web construidos con PrestaShop, OpenCartz, ZenCart y otros más. En el caso de que se hayan empleado softwares propios para la construcción de la tienda, ofrecen tres posibilidades de integración, redirección a su plataforma, conexión en el propio comercio electrónico y el envió de la información recogida en la tienda hasta la pasarela donde es procesada. Por último, existe también una opción específica para incluir en aplicaciones móviles.

La personalización en el caso del uso de Plug&Play se limita a el logotipo y banner de la compañía, pero cuando el módulo es integrado en la página, las características pasan a ser completamente modificables.

La información ofrecida respecto a los precios es privada, y no se encuentra publicada en su página web. Esto se debe a que se aplica una tarifa en función del perfil del negocio, y para conocer las condiciones es necesario hablar con el departamento de atención al cliente. Las tarifas por transacción suelen variar entre el 0.3% y el 1.5%.

Su reputación en cuanto a la seguridad que proporciona es muy buena, y viene respaldada con algunas de las herramientas que utilizan para ello. La información es encriptada desde que es introducida por el cliente independientemente del tipo de integración escogida y utilizan el sistema 3D Secure inteligente para reducir el riesgo de fraude. Todos los servicios que la entidad ofrece cumplen la directiva europea de seguridad PSD2 además de contar con el certificado PCI DSS y en relación con los datos bancarios, se les aplica una *tokenización* que permite almacenarlos de forma segura para disponer de ellos en caso de que un cliente vuelva a realizar una compra.

Figura 3. Logotipo de Redsys

PayComet

Entidad surgida en España en el año 2010 y adquirida por el banco Sabadell en 2018, opera con todos los bancos de la Unión Europea. Es una apuesta muy popular y sus herramientas están en continuo desarrollo.

Ofrece la posibilidad de pago con los medios tradicionales, tarjeta y transferencia bancaria además de los medios alternativos más usados como AmazonPay, GooglePay, ApplePay, Bizum y tecnologías como los enlaces de pago.

En cuanto a la integración de la pasarela, utiliza una API de fácil instalación y compatible con muchos CMS como PrestaShop, WooCommerce o Magento.

En el caso de las webs de desarrollo propio, existen varias opciones de integración que pueden realizarse empleando tecnología REST (la opción recomendada), XML y GET. Las tres opciones disponibles son:

-Fullscreen: integración rápida, métodos de pago alternativos y tarjeta. La pasarela se aloja en la web de PayComet y el cliente es redireccionado a ella al realizar el pago. Permite una ligera personalización.

-iFrame: se incrusta en la tienda online y el panel de control permite ser modificado. Se necesita algo más de conocimiento de programación en el caso de desear una personalización más profunda. Permite métodos de pago alternativos y con tarjeta.

-Embedido: sencilla integración con API, al comprar se abre una ventana en el sitio web y envía los datos de pago a la pasarela donde son procesados. Esta opción es completamente personalizable pero únicamente permite el pago con tarjeta

La tarifa que ofrece para pequeños volúmenes de ventas (hasta 2000€ al mes), es de 19€ de cuota mensuales más una tarifa por transacción de 0.5% más 0.09€ si se sobrepasa este límite.

Su gestión de la seguridad se basa en el uso de un módulo avanzado de gestión contra el fraude. Además, cabe destacar que se trata de la primera compañía española en obtener la certificación de seguridad PCI DSS del nivel de seguridad más alto en cifrado de datos. A esto hay que añadir, que trabaja con la *tokenización* de las tarjetas por lo que se almacena la información de forma segura para futuras compras.

Figura 4. Logotipo de Paycomet

UniversalPay

Es la filial de EVO Payments International en España y es regulada por el Banco de España. Acepta pagos en 49 divisas y países además de que no es necesario el cambio de cuenta bancaria ya que opera con todas.

La integración ofrece todas las posibilidades, redirección a una pagina de pago segura, un formulario instalado en la pagina web que no almacena los datos bancarios o la posibilidad de almacenar los datos en el propio servidor de la tienda. En las dos últimas opciones es posible la personalización completa del entorno, mientras que la primera, de más fácil instalación no se pueden alterar las características prefijadas2

Las tarifas dependen del volumen de facturación, comenzando en la franja de 9.99€ para facturaciones de menos de 1000€ al mes y llegando a los 19.99€ cuando la facturación es de menos de 2000€. El precio sigue incrementándose según lo hace la facturación del negocio. En el caso de superar la facturación asociada a la tarifa se aplica una tarifa por transacción de 0.5% más 0.1€.

La seguridad que esta entidad ofrece en su web cumple con los certificados PCI DSS por lo que, la protección de los datos bancarios facilitados está garantizada.

Figura 5. Logotipo de Universal pay

Braintree

Establecida en el año 2012, es un servicio ofrecido por PayPal y se especializa en el pago desde móviles (independientemente del SO). Al ser parte de PayPal, los métodos de pago permitidos son los mismos y este servicio esta presente en 50 países y permite el uso de 130 divisas.

Puede ser completamente integrada en el sitio web y es completamente personalizable, pero es necesaria la contratación de un desarrollador profesional para su implementación.

No existen cuotas de apertura y mantenimiento, sino que el pago viene a través de tarifas por transacción. El coste es de 2.9% más de 0.3€. por pago.

La tecnología de seguridad empleada cuenta con el sistema de doble factor 3D Secure y encriptación de la información con certificación PCI DSS nivel 1.

Gracias a los sistemas antifraude que emplea, en web presume de una reducción de las devoluciones de cargo del 50% en sus clientes y un incremento de los beneficios del 33%.

Figura 6. Logotipo de Braintree

Checkout.com

Se trata de la segunda empresa emergente más valiosa de Europa y comenzó a operar en el año 2012, actualmente trabaja con grandes multinacionales a nivel mundial ofreciendo pagos en 150 divisas.

Tiene disponibles como métodos de pagos las tarjetas de crédito y débito de las principales compañías, así como billeteras de pago, ApplePay, GooglePay ,etc.

La integración en plataformas como Shopify, BigCommerce o Chargebee es directa y se realiza mediante módulos. En el caso de no hacer uso de estas plataformas, se recomienda la contratación de un desarrollador ya que es complejo y dispone de una interfaz completamente personalizable.

No existen cuotas de apertura, pero a la hora de las cuotas mensuales y tarifas por transacción los precios se establecen teniendo en cuenta tanto el volumen de ventas como el perfil comercial y categoría de riesgo del comerciante. Para poder obtener una tarifa es necesario rellenar un formulario y ponerse en contacto con su servicio al cliente.

La seguridad de la pasarela está certificada con el PCI DSS y además emplea filtros antifraude de alto nivel. Utilizan también, una solución 3D Secure 2.0 cuya autentificación adicional reduce el riesgo de fraude.

Por otro lado, cuentan con una herramienta que crea de forma automática perfiles de riesgo permitiendo un mayor control en las potenciales ventas.

Ofrece adicionalmente con la pasarela de pago, una herramienta que permite la creación de informes acerca de todas las transacciones realizadas.

Figura 7. Logotipo de Checkout.com

2CheckOut

La plataforma esta disponible en 15 idiomas y trabajan con 87 divisas diferentes por lo que es posible trabajar en más de 200 países.

Acepta como métodos de pago tarjetas de crédito, débito y PayPal.

La integración es sencilla y se realiza mediante una API que está disponible en bibliotecas PHP, PYTHON, RUBY, .NET, JAVA y cURL. Además, está disponible su instalación en dos formas, como pago alojado y como pago en línea. Disponen de las siguientes opciones:

- Pago alojado, se trata de un motor de pedidos independiente que se aloja en la web del comercio, este es completamente personalizable y existen plantillas para su modificación.

- Pago en línea, se realiza mediante un iFrame cuya integración es más fácil de que la del pago alojado y también permite una personalización total.

- Gestores de contenido, WordPress, Magento, Shopify o BigCommerce entre ellos. La integración es aún más rápida que en las dos anteriores y la posibilidad de personalización sigue disponible.

2CheckOut no cobra cuotas mensuales ni de apertura de cuenta, sino que trabaja con tarifas planas por transacción. La tarifa más baja, prescinde de la opción de suscripciones, pero permite la venta global y tiene una tarifa de pago del 3.5% mas 0.35€ por venta exitosa. Por otro lado, existe un coste por devoluciones de cargo de 20€ aunque el número de casos es muy bajo.

La seguridad antifraude con la que cuenta es muy eficaz de ahí los altos costes de la devolución de cargos, además cuenta con una estrategia de 3 niveles para detectar el fraude en tiempo real. Todo el servicio ofrecido por 2Checkout dispone de la certificación PCI DSS de seguridad.

Figura 8. Logotipo de 2checkout

Monei

Ofrece multitud de medios de pago además de la tarjeta de crédito o débito, entre ellos destacan ApplePay, Bizum, PayPal, GooglePay, Bitcoin. Esta compañía permite la liquidación en cualquier entidad bancaria y esta se realiza en el plazo de 1 día.

Una de las principales ventajas que ofrece esta pasarela es la sencillez en su integración. Está disponible tanto como para multitud de plataformas como Shopify, WooCommerce, Wix, PrestaShop como para webs personalizas utilizando su API de pagos.

Dentro de su página web proporcionan toda la documentación e instrucciones necesarias para integrar la pasarela de pago en la web del comercio sin complicaciones. Debido a la interfaz tan sencilla que presenta y la sencillez de implementación, las opciones de personalización son escasas.

La tarifa con la que trabajan habitualmente está orientada a negocios basados en Europa y su coste es de 0.9% mas 0.24€ por transacción con un coste de 17€ por devolución de cargos. Monei también ofrece como opción una tarifa anual que podría ser interesante para algunos negocios, cuyo coste es de 990€ sin otras tarifas o cuotas adicionales.

En el ámbito de la seguridad cumple con la ce0dPrtificación PCI DSS nivel 1 además de con la nueva normativa europea PSD23 y la estructura 3D Secure 2.0[4] para la prevención del fraude.

Figura 9. Logotipo de Monei

AmazonPay

Desarrollada por el gigante global Amazon, permite el uso de la información ya ingresada en la cuenta de Amazon del usuario para realizar los pagos. Es necesario tener en cuenta que este servicio solo está disponible para vendedores con altos volúmenes de negocio y está desaconsejado para empresas que también dispongan de tienda física.

Da diversas opciones de pago como el pago pago inmediato o diferido, cargo recurrente.

Los precios que ofrece son del 3,4% más 0.35€ por transacción sin gastos de apertura instalación o mantenimiento.

Es integrable con soluciones ecommerce como Shopify, Magento, PrestaShop o WooCommerce y su personalización para hacerla coincidir con la estética de la tienda es sencillo.

La seguridad que ofrece esta pasarela coincide con la demostrada por empresa multinacional disponiendo del certificado PCI DSS, un sistema de encriptación segura y una doble verificación de datos.

Esta plataforma incluye en su servicio la garantía de la A a la Z característica de Amazon que garantiza el estado del producto y su entrega puntual.

Figura 10. Logotipo de AmazonPay

Addon Payments

Esta compañía española surgió de la unión de Caixa Bank con Global Payments, conocido previamente con el nombre de TPV de la Caixa. La interfaz de procesamiento se encuentra disponible en más de 15 idiomas y permite el pago con multitud de divisas.

Los clientes pueden realizar pagos con tarjeta de crédito o débito, PayPal, algunos otras conocidos métodos de pago europeo como GiroPay en Alemania y próximamente se incluirá ApplePay en su oferta.

Ofrece una tarifa para negocios pequeños en la que realizan la integración de la pasarela por 100€ y el coste de la cuota mensual es de 9€, a esto hay que sumarle la tasa de descuento correspondiente. La otra opción es para empresas, cuya cuota mensual es de 19€ y carece de cuota de apertura. En este caso la tarifa por transacción es de 0.09€ más la tasa de descuento que corresponda al banco del comerciante.

Uno de los puntos fuertes de Addon Payments es la sencilla integración en los sitios web. Como muchas otras pasarelas, es compatible con muchas de los sistemas de gestión de contenidos más empleados como Shopify, Magento, PrestaShop, WooCommerce, ...

Ofrece también la posibilidad de usar un iFrame para la instalación y también la redirección de la compra a su propia web, la integración en ambos casos puede realizarse en menos de 5 minutos y permite la personalización de la interfaz para mejorar la experiencia del usuario.

La compañía gracias a su compromiso con la seguridad ha implementado más de 30 reglas antifraude adaptables. Entre estas, se incluye el sistema 3D Secure para prevenir y evitar transacciones sospechosas. El cumplimiento de la certificación PCI DSS .3.2 permite que la entidad almacene los datos bancarios siguiendo las directrices internacionales.

Figura 11. Logotipo de AddonPayments

En el **Capitulo 6 "Caso de aplicación"** se ofrece una tabla comparativa entre las diferentes pasarelas de pago estudiadas para la justificación de la elección realizada para la tienda construida.

CAPÍTULO 3. SEGURIDAD

3. SEGURIDAD

El capitulo anterior finaliza con una reflexión acerca de los retos adicionales que el comercio electrónico tiene que afrontar respecto del tradicional. Estos retos tienen su origen en las nuevas herramientas que han sido incluidas en los procesos productivos de las empresas.

Como se ha comentado en el capítulo referente al comercio electrónico la información que posee una compañía se ha convertido en su activo de mayor valor y por ello su seguridad se ha convertido en una prioridad. ¿Pero qué se entiende por un concepto tan amplio como el de seguridad?

La seguridad, puede ser abordada desde diversas perspectivas dependiendo del área de aplicación, pero comencemos por su definición general: “La seguridad es una característica que realza la propiedad de algo donde no se registran peligros, daños o riesgos. Una cosa segura es algo firme, cierto e indubitable. La seguridad, por lo tanto, puede considerarse como una certeza. (Gardey, 2021)”.

El problema de está definición es que, si bien es clara, el concepto de seguridad es tan amplío que a pesar de permitir identificar cuando algo es seguro, no es tan sencillo identificar cómo llega a serlo. Para poder entender realmente que es lo que debe ser seguro y por qué, es preciso revisar el conjunto de elementos que rodean a la información y que también son susceptibles al peligro.

3.1 SISTEMA DE INFORMACIÓN

Dentro de una compañía, las cantidades de información y datos que se manejan actualmente son tan grandes que sería muy complicado gestionarlo sin ayuda de la tecnología. El conjunto de herramientas que ayudan a la empresa a tratar con toda esta información se conoce como sistema de información.

Los sistemas de información son los componentes que permiten la gestión, administración y el desarrollo de diversas operaciones y procesos dentro de una organización, utilizando para ello la información y las tecnologías necesarias.

Cuando estos sistemas trabajan, interaccionan con todo tipo de elementos, ya sea software, hardware, bases de datos e incluso con sistemas de gestión. Es decir, se componen de cualquier herramienta que proporcione acceso a los datos y permita

su tratamiento. Algunos de los sistemas de información de uso más común en la industria son los siguientes:

- ERP (Enterprise Resource Planning): se encarga del almacenamiento de todos los datos necesarios que permiten la gestión de la producción y una mejora de su eficiencia con un objetivo, como por ejemplo el de instaurar una metodología de Lean Manufacturing o JIT. Proporcionan una vista integral de cada área de la empresa.

- CRM (Costumer Realationship Management): es empleado para gestionar las relaciones entre clientes y la empresa, almacenando todos los datos proporcionados por estos, que posteriormente serán implementados en la creación de estrategias.

- SCM (Supply Chain Management): usado para gestionar toda la cadena de suministro de una empresa, desde el contacto con proveedores hasta la entrega del producto o la prestación del servicio al consumidor. El objetivo del uso de SCM es el aumento del valor añadido que se ofrece al cliente, permitiendo a su vez una mejor gestión del inventario, las ventas, la clasificación e incluso el aumento del beneficio neto.

- MIS (Management Information Systems): su uso está dirigido a la recopilación de información originada por diversas fuentes internas con objetivo de generar informes y estadísticas que ayuden en la toma de decisiones estratégicas en la organización.

Una vez comprendidas las diferentes partes que constituyen un sistema de información, es posible comenzar a hablar sobre la seguridad de estos sistemas.

3.2 SEGURIDAD DE LA INFORMACIÓN

La información es el activo manipulado por los sistemas de información en una empresa, en el caso de una tienda online saber utilizarla otorga una gran ventaja al empresario.

Beneficiarse del acceso a algunos de los datos que los clientes proporcionan, no es tan sencillo como parece. En primer lugar, es necesario saber identificar cual de estos datos son realmente útiles, pero además también es necesario asegurarse de que estos son siempre correctos y que estarán disponibles en el momento en el que sean necesarios. Como es lógico, esta ventaja de la que dispone el comerciante se

convierte a la vez en una responsabilidad ya que asume la tarea de proteger su carácter confidencial.

La seguridad de la información es el proceso cuyo objetivo es asegurar el cumplimiento de los principios recogidos en el modelo conocido como triángulo CIA. Los vértices de este polígono simbolizan las características que toda la información de la compañía debe poseer: confidencialidad, integridad y disponibilidad.

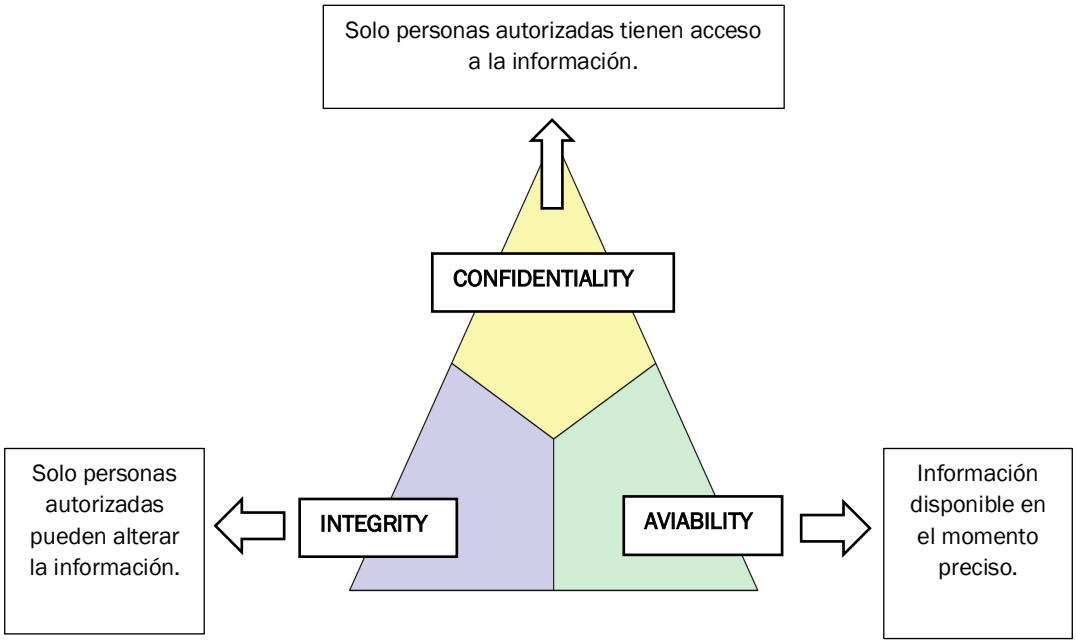


Figura 12. Diagrama descriptivo del triángulo CIA

Si bien es cierto que el triángulo CIA es un estándar dentro de la industria, se han llevado a cabo algunas reflexiones interesantes como la publicada por los autores Whitman, M. E., & Mattord, H. J. En esta, se expresa que el cumplimiento de las tres características de la información ilustradas por el modelo del triángulo CIA, es tan importante hoy en día como lo ha sido siempre. Pero el entorno en constante cambio de la industria informática hace surgir un debate acerca de si el cumplimiento de este triángulo, además de ser necesario es suficiente.

Para cerciorarse de si estos tres principios están realmente cumpliéndose, plantear las siguientes preguntas puede ser de ayuda:

1. ¿Están los datos protegidos de ser interceptados por personas no autorizadas?

2. ¿Están los datos protegidos de ser cambiados o eliminados por personas que no deberían poder hacerlo?
3. ¿Están los datos disponibles, para las personas que si deber tener acceso a ellos, cuando los necesiten?

En el caso de que estas tres cuestiones tengan una respuesta afirmativa, puede decirse que la organización cumple con este modelo de seguridad de la información denominado triángulo CIA.

3.3 SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Como ha sido mencionando en los apartados anteriores, existen unas herramientas que se emplean en las organizaciones para el tratamiento de la información. En una tienda online estas herramientas se conocen como Tecnologías de la información y la comunicación (TICs) o por sus siglas en inglés ICT.

El concepto de *ICT security* o seguridad de las TICs, surge para hacer referencia a la seguridad de los propios sistemas tecnológicos que recolectan, transmiten y almacenan la información. Los estándares internacionales vigentes de obligado cumplimiento referentes a la seguridad de las ICT se encuentran publicados en la ISO/IEC 13335-1 (2004).

La diferencia principal entre los conceptos de seguridad de la información y el de seguridad de las tecnologías de la información y la comunicación, es el activo que se pretende asegurar. En el caso de la seguridad de la información lo que se protegen son los propios datos y la integridad de estos. Por otro lado, para conseguir que las TICs sean seguras son las propias herramientas tecnológicas las que deben funcionar correctamente y estar protegidas de posibles alteraciones que puedan afectar a la información que manejan.

Para conseguir que la información esté realmente segura, además de la protección directa del propio activo, es necesario que todo el sistema de información cuente con esta protección. Es decir, el sistema no puede considerarse como seguro hasta que todos los procesos y fuentes que interactúen con la información lo sean también.

Al conformar las TICs la infraestructura que procesa la información en una tienda online es lógico concluir que, para que esta esté a salvo es indispensable que las TICs también lo estén.

3.4 CIBERSEGURIDAD

Una vez explicado qué es necesario para que el sistema de información que emplea la empresa sea seguro, es momento de poner el foco en la seguridad cibernética.

Habitualmente cuando se habla sobre la seguridad en internet se emplea el término ciberseguridad para referirse a cualquier incidente sucedido o a la protección de cualquier activo, pero la realidad es que su uso no siempre es correcto.

Las diferencias que aparecen entre conceptos como el de seguridad de la información, seguridad de las TICs y ciberseguridad, se basan en los objetivos, medios y herramientas con los que estos trabajan. Es importante esclarecer los limites de cada uno de estos términos, y puesto que los otros dos ya han sido tratados anteriormente, es el turno de la ciberseguridad.

El área de actividad de la ciberseguridad se extiende a cualquier activo que se encuentre en peligro o sea susceptible de ser atacado, siendo para ello utilizadas las tecnologías de la información y comunicación.

Para ejemplificar a que se refiere esto, a continuación, se describen algunos de los objetivos más comunes:

- Ciber-bullying: el objetivo del ataque es una persona, pero sus datos personales no tienen necesariamente porque ser puestos en peligro.

- Documentos digitales: dentro de industria del entretenimiento son comunes los casos de robo archivos digitales tales como películas, canciones, etc. Este tipo de ataques si son dirigidos a la información. Por el contrario, la piratería se encuentra dentro de los márgenes de la ciberseguridad y no de la seguridad de la información ya que, la información (la obra) ya ha visto la luz. En este caso los objetivos del ataque son los beneficios de la compañía y la propiedad intelectual.

- Ciber-terrorismo: estos ataques se dirigen a las infraestructuras que soportan el funcionamiento de un estado o región. La seguridad de la información de los habitantes no se ve comprometida, pero se pone en riesgo el funcionamiento normal de la sociedad. El ataque hacia la red de semáforos de una ciudad o la caída de la red que soporta el sistema en el servicio sanitario pueden ser ejemplos de este tipo de ciberataques.

- Casa inteligente: en los últimos años muchos sistemas en el hogar se han visto automatizados y su control se realiza desde sistemas tecnológicos. El acceso no

autorizado a algunos de estos sistemas puede llegar a suponer un peligro para el propietario, como desactivar la alarma de seguridad.

Como se ve gracias a los ejemplos, en la seguridad de una tienda online algunos de estos objetivos no tienen cabida, por ello en el siguiente apartado va a estudiarse la relación entre los tres conceptos de seguridad comentados para determinar cual se corresponde con el caso de estudio.

3.5 RELACIÓN ENTRE LOS TIPOS DE SEGURIDAD

La visión proporcionada sobre la seguridad de la información, la seguridad de las Tecnologías de la información y la ciberseguridad permite identificarlos como conceptos complementarios en el área de la seguridad. La *Figura 2* (Von Solms, 2013) permite apreciar la relación y límites que se establecen entre ellos.

Se puede observar como las principales diferencias que existen entre la seguridad de la información y la ciberseguridad como se ha comentado, son los activos objetivo y las herramientas o tecnologías empleadas para llevar a cabo los ataques.

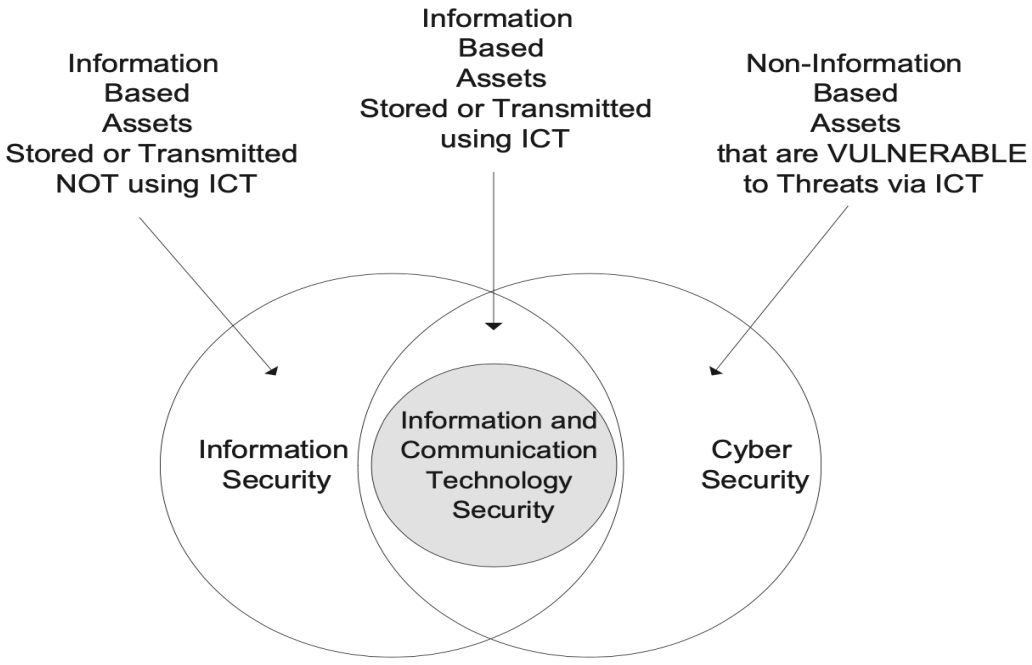


Figura 13. Relación entre seguridad de la información, seguridad de las Tics y ciberseguridad

En el caso de la primera, el objetivo siempre es la información, pero la vía de perpetración del ataque no debe necesariamente ser a través de las tecnologías de la información. Por otro lado, en la ciberseguridad, pasa exactamente lo contrario, la vía empleada para el ataque son siempre las TICs, pero el objetivo no tiene por que ser la información.

A pesar de estas diferencias, existe un área común en el que las tecnologías de la información y la comunicación son empleadas para realizar un ataque cuyo objetivo es la información. Esta área se conoce como seguridad de las TICs y es el objeto de estudio de este trabajo.

En una tienda online, se realizan transacciones utilizando diferentes elementos tecnológicos, en estas interviene información delicada como datos personales o bancarios. Es por esto, por lo que es de suma importancia para todos los agentes que esta información esté segura.

Es lógico comprender por qué un usuario, en este caso un comprador, está interesado en que su información no corra peligro, pero en el caso del vendedor existen incentivos que también incrementan su interés.

A parte del aspecto legal que obliga a la persona propietaria de un comercio electrónico a proteger la privacidad y la confidencialidad de los datos de sus clientes, desde el punto de vista empresarial también existen razones para tomar en serio esta responsabilidad.

La información es poder, y como tal, si se emplea estratégicamente puede usarse para competir con otras empresas y alcanzar un sector del mercado que de otra manera no sería posible. Este tipo de beneficio es relativamente evidente para un propietario hoy en día, pero es posible que las decisiones que se tomen en cuanto a la seguridad del negocio afecten de un modo más complejo a este. ¿Qué es realmente lo que lleva a un consumidor a elegir si comprar o no en una tienda online?

3.6 SEGURIDAD PERCIBIDA

Este concepto ha surgido de manera reciente en el entorno de los comercios en línea, el poder derivado de los datos implica el deseo de muchas personas de obtenerlos y no siempre de manera lícita. El caso de los pequeños comercios es especialmente preocupante debido a los recursos de protección limitados que poseen, ya que les convierte en objetivo más atractivo para los delincuentes. Esto no quiere decir que no sean seguros, sino que su tamaño no les exime de proteger correctamente sus activos.

Desde que apareció el comercio electrónico se han registrado ataques y estafas cuyo número aumenta cada año. Pese a la tendencia creciente que han seguido siempre, a partir del confinamiento en 2021, estas se han visto exponencialmente multiplicadas. Según las estadísticas proporcionadas por la Guardia Civil, durante este periodo, el aumento de las estafas realizadas a través de internet y webs falsas aumentó al menos en un 70% respecto a los ataques que venían sucediendo con anterioridad (Ortega Dolz, 2020).

Puede pensarse que este dato no es concluyente debido a que la situación vivida en ese periodo fue excepcional, pero los datos obtenidos posteriormente siguen preocupantemente la misma tendencia. España es "el país de la Unión Europea más afectado por el auge de *Ransomware*. Se estima que, durante la segunda mitad de 2020, se produjo un aumento del 160% en ataques de este tipo a empresas españolas" (Ciberpandemia, 2021).

Siendo los anteriores datos relativos a España, a nivel mundial, la tendencia no difiere de lo que viene observándose nacionalmente. Los costes derivados del secuestro de datos a nivel global se predijeron que alcanzarían los 20 billones USD en 2021 cuando la anterior estimación realizada por esta misma fuente fue de 11.5 billones USD para 2019, datos obtenidos de la reputada revista online de Cybercrime Magazine (Morgan, 2019). Es evidente un aumento de casi 9 billones USD en dos años implica un aumento sustancial en la actividad criminal cibernética. Estos continuos ataques afectan tanto a compradores como a vendedores y es, por tanto, común su interés en evitar que se produzcan con éxito, a pesar de que sus consecuencias son diferentes para ambos casos.

En los últimos años, se ha tratado el tema de la relación entre la seguridad de la información percibida por el usuario y su predisposición a la compra, obteniéndose como resultado una relación directa entre estos factores.

En los inicios del comercio electrónico aparecieron estudios, como el realizado en 1999 por la Comisión Federal de Comercio de Estados Unidos (FTC) que reflejaba cómo la desconfianza sería el obstáculo principal para el futuro desarrollo del comercio electrónico (Miyazaki, 2001). Más de 20 años después esta conclusión parece desfasada y comprobada como errónea ya que tan solo durante el tercer trimestre de 2021, el comercio electrónico en España movió más de 13.600 millones de euros.

A pesar de esto, si ha sido demostrado en estudios más recientes como el de Mekovec, R. & Hutinski, Ž. titulado "Rol de la privacidad y la seguridad percibida en el mercado online" como, aunque no es un impedimento para las compras a través de internet la percepción de la seguridad y la privacidad si siguen siendo factores que afectan notablemente a la confianza del comprador en relación con la

realización de esa compra. Es, por tanto, primordial además de proporcionar la seguridad, generar confianza en el tratamiento de los datos del cliente para lo cual es necesaria la construcción de un sitio web seguro que albergue nuestra tienda online.

Para conseguir este objetivo de seguridad percibida es necesario en primer lugar, conocer los problemas que principalmente preocupan a los consumidores a la hora de realizar compras online. Estos pueden dividirse en dos grupos, los relativos a la privacidad y los que tienen más que ver con la seguridad de su información, ya se ha explicado que es la seguridad, pero ¿qué es la privacidad?

3.7 PRIVACIDAD

A raíz de la creciente preocupación en la sociedad en torno a la privacidad de datos, esta se ha convertido en uno de los principales objetivos a contemplar dentro de la seguridad percibida. En realidad, se asocia este concepto al de seguridad cuando a pesar de tener relación, no tiene implicaciones dentro de la seguridad que un vendedor proporciona a sus clientes.

Para esclarecer esto, a continuación, se expone brevemente qué es y cómo funciona la privacidad.

La privacidad se refiere al derecho del consumidor a tener control sobre sus propios datos. Al realizar una compra a través de internet la tienda obtiene tres tipos de información:

- Información anónima: no se relaciona con la identidad del usuario, la IP del ordenador o el buscador utilizados pueden ser ejemplos de esta.

- Información personal no identificadora: como su propio nombre indica, esta información proporciona datos acerca de la persona, pero no compromete su anonimato. Algunas de estas son la edad, el género, los intereses o el nivel educativo.

- Información personal identificativa: información privada del usuario cuya filtración puede resultar muy perjudicial, nombre, dirección, teléfono, número de tarjeta de crédito, etc.

Esta clasificación se basa en la naturaleza de la información recogida sobre usuario, pero si se pone el foco en la forma de obtención de estos datos y el propósito de su uso, se obtiene la siguiente distribución:

- Recolección voluntaria para uso público: datos de registro online, datos de gestión administrativa, etc.

- Recolección voluntaria para uso privado: opiniones, reseñas, información personal del cliente, etc.

- Recolección involuntaria informada: este tipo de información se obtiene durante la navegación del cliente antes y durante la transacción como por ejemplo preferencias personales.

- Recolección involuntaria no informada: análisis del movimiento del cursor y los clics. Se suele emplear para la creación de estrategias de marketing y mejora del diseño web.

Como puede observarse, cuando un usuario navega a través de una tienda online la mayor parte de la información recogida es inofensiva y solo se emplea con fines comerciales. Un ejemplo de este uso es la herramienta de las cookies.

Las cookies son piezas de información que las páginas web recolectan de los consumidores y almacenan para poder identificar a los usuarios cuando vuelven acceder y utilizar sus preferencias para personalizar su experiencia.

Siguiendo las clasificaciones presentadas, las cookies entrarían dentro de la categoría de recolección involuntaria pero informada de datos, pero también dentro de la de recolección involuntaria pero no informada de datos. En cualquiera de estos casos, nunca se trata de información personal sensible por lo que su almacenamiento no constituye ningún peligro para el usuario.

Se debe tener en cuenta que toda la información personal identificativa recogida por una tienda online debe cumplir el Reglamento General de Protección de Datos (RGPD) por lo que la privacidad estaría a salvo en este entorno. Lo que si debe preocupar, es la fuga de esta información.

CAPÍTULO 4. AMENAZAS Y PROTECCIONES

4. AMENAZAS Y PROTECCIONES

Los ataques al comercio electrónico se producen cuando un ciberatacante intenta obtener acceso a alguno de los sistemas de red que conforman la empresa. Cuando esto sucede, sus objetivos pueden ir desde dañar a la empresa, realizar un chantaje o robar información hasta la curiosidad de saber hasta donde pueden infiltrarse.

Existen muchas herramientas y estrategias empleadas para realizar los ataques dirigidos y estos no se centran únicamente en las webs corporativas, sino que el consumidor de este tipo de servicios también se puede ver afectado.

Nunca hay que olvidar que el propietario de un comercio electrónico también es un usuario y que por ende las posibilidades de ataque se amplían. Es por esto por lo que a continuación van a tratarse las diferentes formas de ataque que son utilizadas tanto contra el comercio electrónico como contra el usuario, centrándose en ataques que pudieran afectar en el ámbito correspondiente.

4.1 ACTIVOS A PROTEGER

Para poder proporcionar seguridad a los activos, son necesarias las barreras físicas lógicas. Si bien, es en parte responsabilidad del vendedor realizar esta protección, no es el propio vendedor el que realiza un uso ilícito de la información sino algún otro usuario.

Para que una persona que almacena información de clientes sea capaz de proteger sus datos es necesario que sepa identificar que datos deben tenerse en cuenta y quien podría querer acceder a ellos, por ello, se pueden distinguir cuatro tipos de seguridad web según su intencionalidad:

- Proteger la integridad del sitio Web, impedir la modificación o eliminación de los contenidos que muestra
- Proteger la información y su propiedad que se publica en el sitio web para que nadie pueda hacer un uso ilegítimo de ella
- Proteger los datos que se transmiten utilizando como vía Internet
- Proteger la información que se proporciona y genera en la transacción

Teniendo en cuenta que estos son los cuatro principales objetivos en un ataque, es momento de identificar las posibles formas que existen de vulnerarlos, así como las precauciones que pueden tomarse y algunas defensas contra los ataques más comunes.

Dependiendo de la puerta de entrada que utilice el atacante para obtener acceso a las redes de una empresa, se pueden diferenciar cinco tipos diferentes de ataque. Estos son, ataques a contraseñas, ingeniería social, ataques al sistema, ataques web y ataques por programa maligno o *malware*.

4.2 ATAQUES A CONTRASEÑAS

Ya sea un usuario cualquiera, un empleado de una empresa o incluso el dueño de esta, todos disponemos de cuentas en webs o plataformas generalmente el acceso a estas se basa en una combinación de un nombre de usuario y una contraseña.

Dentro de estas cuentas se almacena información que puede variar desde datos personales propios a datos personales ajenos, por ello es primordial que una de las barreras de seguridad más básicas que tenemos esté bien construida.

El ataque para averiguar la contraseña en el ámbito del comercio electrónico no es tan común ya que resulta más sencillas otras técnicas como la infección por *malware* o la ingeniería social, pero nunca debe subestimarse y se ha de disponer de una contraseña robusta para no facilitar las cosas a las personas malintencionadas.

Dos tipos de ataques se centran en el robo de contraseñas, los ataques por fuerza bruta y los ataques por diccionario, la diferencia se encuentra en el proceso de obtención de esta y se explica a continuación.

4.2.1 FUERZA BRUTA

En este caso el atacante trata de adivinar la contraseña utilizada probando con información personal del objetivo o las estructuras de contraseñas más usadas, fallando y probando de nuevo hasta que consigue acertar. Generalmente se estudia a la persona antes de realizar el ataque para disponer de esta información personal.

4.2.2 POR DICCIONARIO

Este ataque tiene una mayor dificultad técnica ya que se emplea un software específico que probará diferentes opciones hasta conseguir acertar la contraseña. El programa va creando combinaciones de letras y números comenzando por estructuras simples y aumentando su complejidad a medida que avanza el ataque.

4.2.3 PROTECCIÓN

La defensa básica para este tipo de ataques es no cometer los errores básicos a la hora de establecer una contraseña. No se debe utilizar la misma contraseña para varios sistemas ya que si se obtiene acceso a uno, abre la puerta para el resto.

En cuanto a la construcción de la contraseña, como se menciona en el ataque por fuerza bruta, no deben utilizarse datos personales para ello. Mucho menos han de almacenarse las contraseñas en gestores no seguros, como los de los navegadores ya que el acceso a estas es bastante sencillo.

Además de estos sistemas basados en usuario y contraseña también es importante recordar que existen otros sistemas de identificación que pueden resultarnos más convenientes según la información que se quiera proteger. Los sistemas basados en tarjetas de identidad o coordenadas y los sistemas basados en características físicas no pueden únicamente sustituir, sino que pueden complementar a las contraseñas, conformando así una múltiple verificación que complica ampliamente este tipo de ataques. Este puede ser un buen recurso a la hora de construir una aplicación web o de un sistema informático empresarial.

Si bien es cierto que seguir todos estos consejos y recordar todas las contraseñas seguras puede ser complicado, puede hacerse uso de un recurso muy acertado para esto, los gestores de contraseñas seguros. Estos almacenan nuestras contraseñas impidiendo que las olvidemos, pero sin ponerlas en peligro.

4.3 INGENIERÍA SOCIAL

Como se ha comprobado con las contraseñas, los ataques no siempre requieren de un gran control técnico, sino que muchas veces el uso de otras técnicas más sencillas es más efectivo.

La técnica más extendida es la de la ingeniería social, esta se dirige a personas para utilizarlas como vía de entrada al sistema o a la información. Concretamente en el ámbito de la seguridad informática puede entenderse la Ingeniería social como una técnica de manipulación psicológica que es utilizada por los cibercriminales para conseguir información valiosa u obtener acceso a determinados recursos. La razón de su efectividad es clara, "en cualquier cadena de seguridad, los humanos son generalmente el eslabón mas débil". (Bodnar, 2020).

4.3.1 FASES DE ATAQUE

Todos los ataques que se valen de la ingeniería social emplean el mismo patrón de actuación para conseguir el éxito a pesar de emplear diferentes recursos para llevarse a cabo.

En primer lugar, se **recopila información del objetivo**, el ciberdelincuente investiga al objetivo para obtener información relevante sobre este, como la empresa para la que trabaja, el nombre de su superior, puesto, teléfono o cualquier información que pueda ser útil. Este paso se vuelve más concienzudo a medida que la víctima del ataque es más concreta.

Después de conocer al objetivo llega el momento de poner en marcha el plan y proceder a la **manipulación** de la persona. Para conseguir el objetivo se emplean técnicas psicológicas sobre la víctima, consiguiendo que esta otorgue acceso al sistema. Algunos de los métodos más eficaces son la suplantación de identidad de un superior, creando temor en la víctima, o realizar una solicitud alegando urgencia para que no pueda ser corroborada y limitar por tanto el tiempo de reacción, etc.

Por último, cuando el acceso está asegurado, se intenta de **abandonar** la treta sin ser descubierto o que en su defecto el tiempo de detección del engaño sea lo mayor posible. De esta manera, se reduce al máximo el tiempo de reacción disponible para los responsables de seguridad, y así el alcance del daño provocado aumenta.

Esta técnica es a veces utilizada como antesala al uso de otros ataques como los que usan *malware* o algún otro fraude, la ingeniería social proporciona la puerta de acceso para poder desarrollar un plan de infección mayor.

A continuación, se exponen algunas de las técnicas de ingeniería social más empleadas, cómo identificarlas y defenderse de ellas.

4.3.2 PHISHING

Este es el nombre que recibe un conjunto de técnicas cuyo propósito es el robo de datos o información a través del engaño a una persona, para obtener el acceso a su equipo. Estas técnicas son de las más utilizadas por los criminales ya que pueden hacer uso de varios medios tecnológicos para llevarlas a cabo como las llamadas telefónicas, los mensajes de texto o el más común, el correo electrónico.

La diversidad de medios usados permite realizar ataques a casi cualquier persona, en el caso de una tienda online el medio elegido sería el correo electrónico ya que, cualquier persona o entidad dispone de una dirección de correo y además cuenta con la ventaja de que el daño que se puede causar a través de él es muchas veces infravalorado.

En el pensamiento colectivo se ha instalado la idea de que un ataque que inicialmente se dirige hacia un lugar de la red en la que no guardamos información sensible no es peligroso, pero nada más alegado de la realidad. De esta manera, se abre una pequeña brecha a través del correo que puede convertirse en la vía de acceso a toda la información que almacena el servidor o la base de datos de la tienda. Las puertas de acceso al emplear este tipo de ataques son aquellos trabajadores con acceso a información importante, por ello es preciso una buena distribución de permisos y accesos a datos.

Para evitar que esto suceda y que empleados o usuarios no caigan en este tipo de estratagemas, la mejor estrategia es la educación. Por ello, a continuación, se ofrece una pequeña explicación de los tipos más comunes de *phishing* que ayudará a saber identificarlos si se presentan.

- *Spear Phishing*: en español conocido como fraude del CEO, la victima seleccionada es un trabajador de la empresa con cierto control en los recursos económicos de esta. El empleado es investigado acerca de su puesto y función dentro de la compañía.
  La estratagema tiene como objetivo que esta persona transfiera activos propiedad de la empresa a el creador del engaño. Para esto, este se hace pasar por un alto directivo de la compañía para la que trabaja, al cual la víctima no tiene acceso directo y le solicita con urgencia la realización de un movimiento bancario. Para evitar ser descubierto en el acto, apela a la confidencialidad de la transacción.

- *Whaling: whale phishing,* esto hace referencia a que el objetivo de esta actividad ilegítima son directivos o personas con alto poder dentro de las compañías, las *whales* (ballenas). Su objetivo es el robo de información y

credenciales, pero al acceder a través de altos mandos, la cantidad de información disponible es mucho mayor.

- Minnowing*:* las personas alto poder en una empresa son los objetivos más llamativos, pero también los más difíciles de alcanzar por eso, este ataque se centra en los hijos de estos. Al ser personas más descuidadas y generalmente más fáciles de engañar, se emplean las tácticas con los menores para conseguir las credenciales y la información confidencial de sus tutores.

- *Vishing:* surge de la unión de las palabras *voice* y *phishing*, en este caso la vía elegida para realizar el ataque es la llamada telefónica. La víctima recibe una llamada en la que se solicita información bancaria, credenciales o algún tipo de dato personal, para conseguir que la persona revele esta información se juega con tácticas típicas de la ingeniería social como la urgencia, la autoridad, etc.

- *Smishing:* como en el vishing, se utiliza el número de teléfono para contactar con el objetivo, pero en este caso, la vía elegida para realizar el ataque es el mensaje de texto. Generalmente los mensajes de texto son menos sospechosos que las llamadas y los correos, situación aprovechada por los criminales cuyo objetivo es acceso a tu dispositivo, para esto utilizan links o números de teléfono que se incluyen en el SMS.

- *Clone Phishing:* este caso es un poco diferente al resto, pare llevarse a cabo se utiliza un mensaje de correo real y legítimo que contiene archivos adjuntos o *links.* Se realiza una copia idéntica o muy similar de este, y se inyectan en los archivos o enlaces programas maliciosos. Este mensaje no solicita ninguna acción que pueda parecer sospechosa, simplemente indica que sea reenviado. Una vez el destinatario realiza la acción solicitada, el cibercriminal tiene acceso a todos los contactos de este y procede a realizar el ataque de nuevo, gracias a este efecto en cadena este tipo de ataque phishing es uno de los más dañinos.

Recursos empleados

En el *phishing* existen muchos recursos disponibles para engañar a la víctima, pero es posible identificarlos o simplemente reconocer características que nos hagan sospechar. La mayor parte de los ataques son realizados vía mail, por ello a continuación se muestran los más empleados en esta plataforma:

Falso remitente

Conocido también como *email spoofing*, consiste en la alteración de la dirección de correo que envía el mensaje haciéndola coincidir con una legítima, a la que suplanta y con esto hacer pensar al receptor que el email no es peligroso.

Falso enlace

La forma más sencilla de llevar a una posible víctima a confiar en una web es que el enlace desde el que accede sea como el real. Para esto, los criminales utilizan enlaces web falsificados que hacen coincidir con la dirección web verdadera, pero en realidad dirige a una web falsificada desde la que pueden acceder a los datos de la víctima.

Cybersquatting

Se asemeja a las dos anteriores ya que el objetivo sigue siendo hacerse pasar por una entidad segura, pero en este caso el atacante no falsifica la dirección de correo o web para que coincida con el real, sino que utiliza uno que sea extremadamente similar y casi imperceptible. Este recurso es útil pero muy sencillo técnicamente, bastaría por ejemplo con sustituir en el nombre la letra i en mayúsculas (I) con la letra L en minúsculas (l) ya que son prácticamente iguales.

Archivos adjuntos infectados

Otra de las técnicas típicas es el envío de documentos que contienen algún programa maligno. Para ello, valiéndose de la ingeniería social se utilizan nombres de archivo que simulan ser importantes o urgentes para que, cuando sean descargados este software se instale en el ordenador. El tipo de archivos elegidos suelen ser comprimidos o ejecutables pues son capaces de engañar a algunos programas de detección de malware.

Una vez reveladas las herramientas de las que se dispone en este tipo de ataques, cuando como propietario o empleado de un comercio electrónico se reciba algún mensaje de correo del que se desconozca el origen, debe hacerse uso de las diferentes estrategias de identificación y protección que se exponen a continuación.

Identificación y protección

En la mayoría de los clientes de correo existe una barrera externa que protege de forma general al servidor web y que consigue evitar que muchos de los mensajes *phishing* lleguen a sus destinatarios, estas protecciones se conocen como los filtros de correo.

Los filtros de mail son capaces de detectar en los correos propiedades de las campañas de phishing como un número de destinatarios masivo o un remitente falseado. Para construir dichos filtros se emplean los *feeds* de spam, que son listas con mensajes ya identificados como fraudulentos y que se usan para analizar características comunes en estos, e introducirlas en el filtro como indicadores. Cuando un mensaje cumple varios de los indicadores, este es detectado por los filtros, descartado y enviado a la carpeta de no deseado.

A pesar del uso de esta herramienta de prevención, es probable que algunos correos fraudulentos consigan escapar de la barrera ya que, no todos los filtros están siempre actualizados con las nuevas estafas que van apareciendo.
Siendo así, cuando un email que parezca sospechoso porque posea una de las característica o propiedades descritas en el apartado de recursos empleados, se dispone de algunas herramientas que permitirán comprobar si lo que parecía peligroso, efectivamente lo es.

Remites desconocidos

El remite es un claro elemento de sospecha, por ello si no se conoce la dirección que envía el mensaje o incluso si esta no coincide con la organización que se comunica con nosotros en el cuerpo del mensaje, puede que nos encontremos ante un correo *phishing.* En este caso es recomendable enviarle directamente a la carpeta de spam y no abrirle.

Remites falseados

Si el contenido del correo es sospechoso o realiza alguna petición de información importante, debe comprobarse si se esta siendo victima de la técnica conocida como email *spoofing*.

Cuando un correo es enviado, este guarda consigo toda la información sobre sí mismo, aunque haya sido modificada. Datos como de dónde ha salido y que lugares de la red o servidores ha atravesado hasta llegar a la bandeja de entrada son almacenados en las cabeceras del correo, que incluso

proporcionan información sobre el proveedor de correo usado o las fechas de envío.
El problema que hay, es que ser capaz de entender lo que dicen las cabeceras es complicado para un usuario normal y que además dependiendo del cliente de correo utilizado su acceso a ellas variará. La solución a estos dos problemas es sencillamente hacer uso de a la herramienta gratuita de Google, Messageheader.

El acceso a Messageheader se ofrece desde la *toolbox* de Google. En la primera página una vez se accede, aparece un recuadro amarillo (Figura 14) de ayuda que incluye un enlace útil en el caso de desconocer como obtener las cabeceras del correo.

Una vez obtenidas estas, regresando a la página principal, se puede realizar un análisis sencillo simplemente pegándolas en el cuadro de texto designado para ello (Figura 15).

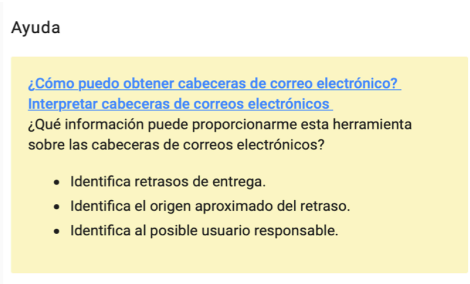


Figura 14. Ayuda para cabeceras correo

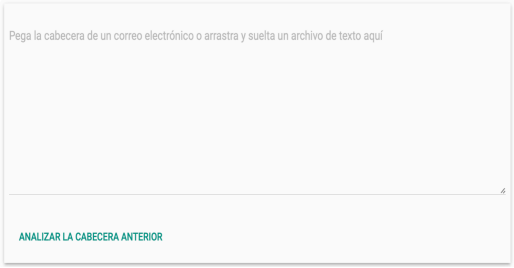


Figura 15. Recuadro inserción de cabeceras

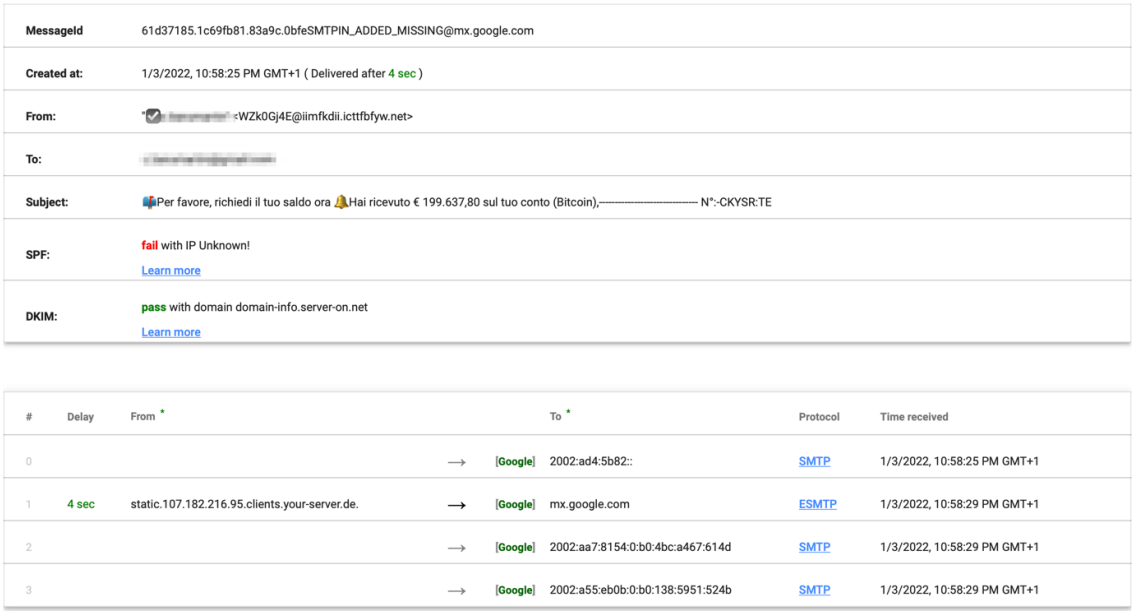
Una vez pegado el texto, solo será necesario hacer clic en analizar y el resultado mostrará el análisis, constando de tres puntos principales que observar:

- Dirección real del emisor del correo, esto permitirá comprobar si el remite había sido falseado o no.

- Registros SPF, DKIM y DEMARC, su función es verificar la legitimidad del mensaje. En el caso de que el correo falle en alguno de estos, será indicado con la palabra *fail* en letras rojas y significará que el correo tiene contenido peligroso.

- Número de servidores atravesados y tiempo de envío. Un tiempo alto de entrega combinado con el paso por un número elevado de servidores puede ser indicativo de peligro.

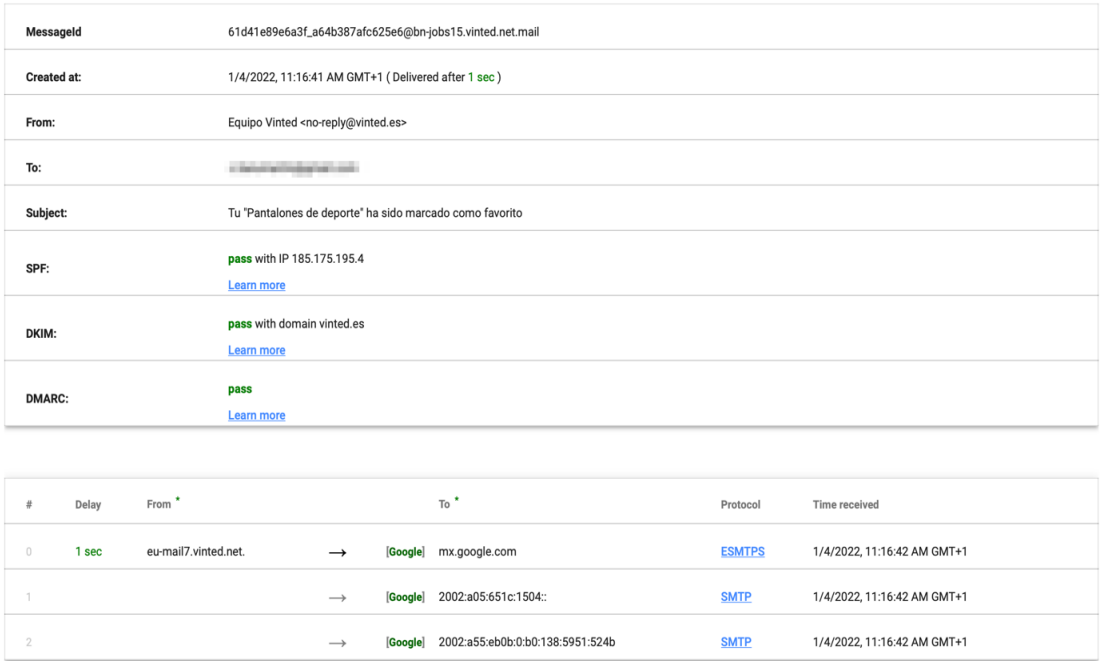
La siguiente imagen ofrece un ejemplo de los resultados obtenidos al analizar dos correos diferentes, siendo el primero fraudulento y el segundo legítimo.



MessageId	61d37185.1c69fb81.83a9c.0bfeSMTPIN_ADDED_MISSING@mx.google.com
Created at:	1/3/2022, 10:58:25 PM GMT+1 (Delivered after 4 sec)
From:	"[redacted]" <WZk0Gj4E@iimfkdii.icttfbfyw.net>
To:	[redacted]
Subject:	📬Per favore, richiedi il tuo saldo ora 🔔Hai ricevuto € 199.637,80 sul tuo conto (Bitcoin),---------- N°:-CKYSR:TE
SPF:	**fail** with IP Unknown! Learn more
DKIM:	**pass** with domain domain-info.server-on.net Learn more

#	Delay	From *		To *	Protocol	Time received
0			→	[Google] 2002:ad4:5b82::	SMTP	1/3/2022, 10:58:25 PM GMT+1
1	4 sec	static.107.182.216.95.clients.your-server.de.	→	[Google] mx.google.com	ESMTP	1/3/2022, 10:58:29 PM GMT+1
2			→	[Google] 2002:aa7:8154:0:b0:4bc:a467:614d	SMTP	1/3/2022, 10:58:29 PM GMT+1
3			→	[Google] 2002:a55:eb0b:0:b0:138:5951:524b	SMTP	1/3/2022, 10:58:29 PM GMT+1

Figura 16. Análisis de un correo fraudulento



MessageId	61d41e89e6a3f_a64b387afc625e6@bn-jobs15.vinted.net.mail
Created at:	1/4/2022, 11:16:41 AM GMT+1 (Delivered after 1 sec)
From:	Equipo Vinted <no-reply@vinted.es>
To:	[redacted]
Subject:	Tu "Pantalones de deporte" ha sido marcado como favorito
SPF:	**pass** with IP 185.175.195.4 Learn more
DKIM:	**pass** with domain vinted.es Learn more
DMARC:	**pass** Learn more

#	Delay	From *		To *	Protocol	Time received
0	1 sec	eu-mail7.vinted.net.	→	[Google] mx.google.com	ESMTPS	1/4/2022, 11:16:42 AM GMT+1
1			→	[Google] 2002:a05:651c:1504::	SMTP	1/4/2022, 11:16:42 AM GMT+1
2			→	[Google] 2002:a55:eb0b:0:b0:138:5951:524b	SMTP	1/4/2022, 11:16:42 AM GMT+1

Figura 17. Análisis de un correo legítimo

Si al analizar el mensaje se obtiene alguno de los resultados mencionados, debe eliminarse el mensaje y no se debe acceder a ninguno de los *links* o archivos que pueda contener.

Ficheros adjuntos

Cuando un correo de un remite que no identificado ajunta algún tipo de documento debe hacer saltar las alarmas inmediatamente. Como se ha dicho anteriormente, los archivos comprimidos o con extensiones ejecutables como son los .exe,.vbs, .docm, .xlsm o .pptm (INCIBE, INCIBE, 2015) han de ser tratados con precaución. En este caso se puede hacer uso de otra herramienta gratuita, alojada en la web Virustotal[3], esta permite subir y analizar el archivo para descartar que estén contaminados con algún tipo de software malicioso.

URL solicitando información

Aunque es común que los correos de algunas tiendas te redirijan a sus páginas webs a través de URL para agilizar el acceso, los enlaces son sencillos de falsificar. Si se va a introducir algún tipo de información personal en esta web es conveniente comprobar que el enlace es verídico o en su defecto escribir manualmente la dirección en el navegador.

El mismo recurso empleado para la comprobación de los ficheros adjuntos, Virustotal, permite también la comprobación de los URL. Basta con copiar la dirección y pegarla en el lugar correspondiente y tras una serie de comprobaciones se obtendrá como resultado la fiabilidad del enlace, puntuado en una escala del 0 al 93 siendo 0 la máxima seguridad alcanzable.

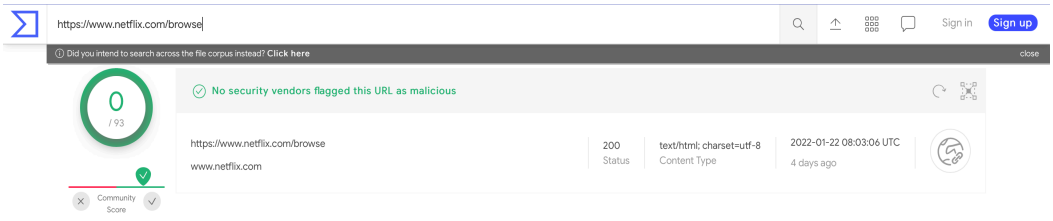


Figura 18. Análisis de veracidad de una URL

Tratamiento impersonal

Cuando se realizan ataques de forma masiva, el objetivo es atacar al mayor número de personas posible utilizando la misma herramienta, por ello se utiliza un lenguaje impersonal y general que pueda identificar a cualquier usuario. Se debe tener en cuenta que una entidad seria intenta siempre realizar comunicaciones un poco mas personales especificando a quien se dirige.

Modificaciones de plantillas

Existen compañías que emplean la misma plantilla siempre al comunicarse en sus emails por lo que, una ligera variación de lo que acostumbramos a ver como un logo o imagen que no aparece debe crear una sospecha. Pueden emplearse las herramientas mencionadas en este apartado para comprobar su veracidad.

Mala ortografía

Esta última forma de identificación era realmente útil hace unos años, pero actualmente los ciberdelincuentes son mucho más cuidadosos en la redacción de sus mensajes. Sin embargo, hay que mantener presente de que una mala redacción no es característica de una entidad seria ya que se realizan muchos esfuerzos para dirigirse correctamente al público. Si se recibe un correo mal escrito pueden las herramientas de identificación serán útiles para comprobar el remite, los archivos y enlaces adjuntos.

4.3.3 BAILING

Esta técnica es una de las más estratégicas, el plan se desarrolla situando un dispositivo de almacenamiento en un lugar clave que vaya a ser visitado por el objetivo. En el caso de que las potenciales víctimas sean empleados de una empresa, el dispositivo puede dejarse en la recepción de la oficina o si el objetivo no es concreto, puede situarse en un lugar público concurrido como un parque.

Apelando a la curiosidad de las personas o a la voluntad de querer devolver el dispositivo al propietario, el atacante que ha insertado en el dispositivo un software malicioso accederá al sistema al conectarse y se extenderá por él.

Protección

Este es uno de los ataques más fáciles de evitar, basta con no conectar ningún dispositivo desconocido al sistema y mantener los sistemas de protección en su última versión. Además, para evitar la filtración de información en caso de pérdida o robo, es aconsejable realizar encriptaciones en los dispositivos extraíbles e impedir que dispositivos sin autorización cifrada puedan ejecutarse en los equipos del sistema.

4.3.4 DUMPSTER DIVING

Puede parecer una técnica que solo se emplea en ficción, pero la realidad es que si se utiliza. En esta, los delincuentes rebuscan en la basura del objetivo para encontrar información valiosa como credenciales anotadas. Debido a esto, los propietarios o empleados con acceso a información o datos delicados deben ser muy precavidos con como son desechados.

Protección

Los documentos con información sensible o confidencial han de ser destruidos antes de ser desechados y se debe poner especial atención a las anotaciones de credenciales, números de teléfono y demás, que se realizan ya que deben ser también eliminadas. En el caso de los equipos electrónicos reemplazados, toda la información almacenada en estos debe ser destruida para que no pueda recuperarse.

4.4 ATAQUES AL SISTEMA

Cuando se tiene un negocio basado en un sitio web, es necesario un sistema informático que soporte su funcionamiento. En los ataques al sistema los objetivos de ataque son los componentes de este, principalmente el servidor.

4.4.1 ATAQUE DE DENEGACIÓN DE SERVICIO

Este este tipo de ataques se realiza con el objetivo de dejar inoperativo un servicio, en este caso la web de la tienda online. La operación consiste en enviar un número

tan alto de peticiones al servidor en la que se aloja la web, que no sea capaz de procesar las todas, sus recursos se saturen y no pueda operar.

Existen dos variantes de esta amenaza, que se diferencian por el número de dispositivos que involucran, el DOS DoS (*Denial of Service*) se perpetúa utilizando un único dispositivo mientras que el DDoS (*Distributed Denial of Service*) emplea toda una red de ordenadores.

Aunque es posible conseguir que un ataque de denegación de servicio sea exitoso con un único dispositivo en webs con recursos limitados, para las webs con grandes servidores suele emplearse una red de dispositivos. Los ordenadores empleados generalmente no pertenecen al usuario que esta llevando a cabo el ataque, sino que por medio de otros ataques se han infectado ordenadores de usuarios anónimos, de los que se ha tomado el control y actúan como *bots*.

Protección

Al no ser un ataque que implique que el atacante se relacione o comunique directamente con el objetivo, muchas veces es imposible detectar este antes de que suceda. Por ello, es imprescindible preparar el sistema para intentar reducir las consecuencias en caso de producirse.

En primer lugar, el sitio web debe alojarse en una zona diferenciada y protegida del resto del sistema, lo que se conoce como zona desmilitarizada, para que en el caso de que se tome el control del servidor web, el resto de la red interna se encuentre protegida. La empresa, además debe contar con un sistema de detección y prevención de intrusiones (IDS/IPS) que enviará una alerta en caso de que algún usuario no ha utilizado intente acceder al sistema. Y por último tanto para evitar este ataque como el resto debe instalarse un software de protección contra virus, malware, etc.

En el caso en el que la compañía no posea un servidor web propio, debe comprobarse que estas protecciones son ofrecidas por el hosting contratado.

4.4.2 COOKIES

Las cookies son piezas de información que se almacenan como texto y que un sitio web guarda en el ordenador de el usuario que las genera. Estos fragmentos, permiten al servidor identificar al usuario que accede y ejecutar información como

las preferencias del usuario, de forma mucho más veloz ya que las recuperan de su propio disco duro.

Aunque en los últimos años se ha extendido una preocupación sobre las cookies, la verdad es que no suponen un peligro si se protegen correctamente. Las cookies almacenadas solo deben ser accesibles para la propia web que las guardó, el problema viene cuando alguien sin autorización las obtiene o modifica.

La obtención de estas puede emplearse para recopilar información previa a otro tipo de ataque o las credenciales de acceso a esa web y su modificación implicaría incluso la posibilidad del cambio en el producto o el precio adquirido en la web.

Protección

Aunque este tipo de problemática suele deberse a falta de cifrados de protocolos de la web, es posible una gran filtración debido a una brecha en el diseño del sistema de protección. Por ello, es primordial que se mantenga actualizado el navegador que se utiliza ya que es posible, que se saquen nuevos parches para solventar algún déficit que haya sido descubierto.

Por otro lado, conviene eliminar la información almacenada en estos como el caché y cookies cada cierto tiempo, para minimizar así el daño en caso de ataque exitoso. En caso de querer evitar las cookies o que la información que se va a compartir no se desee que sea guardada, es recomendable utilizar el modo incógnito del navegador. En el caso de Google Chrome puedes consultar tus cookies almacenadas en la siguiente dirección chrome://settings/siteData.

4.5 ATAQUES WEB

Esta clasificación se refiere a cualquier ataque que al llevarse a cabo atraviese la web siendo o no esta el objetivo final.

4.5.1 DEFACEMENT

En estos asaltos, los autores consiguen acceso al gestor de contenidos de la web o en su caso al servidor web que la alberga consiguiendo así alterar el contenido del sitio web. Las razones que llevan a cabo este tipo de atentados van desde una

reivindicación o la intención de manchar la imagen de la tienda hasta el beneficio económico.

Para obtener acceso a estos recursos existen dos posibilidades, alguna brecha en la configuración del sitio web o como ya viene siendo habitual en todos los ataques, la mala práctica de una persona con privilegios de acceso. En el primer caso, una mala protección de las herramientas web o incluso un software obsoleto pueden permitir acceder al control de la web. En cambio, en el segundo caso solo es necesario valerse de alguna de las técnicas comentadas anteriormente para obtener las credenciales pertinentes.

Protección

Cuando la vía de acceso es el sistema informático, se deben mantener los gestores de contenidos y *plugins* de la web actualizados en su última versión, eliminando de esta forma una de las brechas de seguridad más comunes en la creación web.

En cuanto al personal la mejor opción siempre es la educación y aplicar las protecciones y métodos de identificación que se han venido comentando en este capítulo. Por otro lado, también deben realizarse una buena gestión de privilegios, otorgando a cada empleado únicamente los necesarios para permitir el desarrollo correcto de su labor.

4.5.2 INYECCIÓN DE SQL

Este caso no produce una modificación del contenido de la aplicación web, pero sí interfiere con uno de los activos de esta, las bases de datos.
La estrategia que se lleva a cabo es la inyección de código SQL, lenguaje de bases de datos, en los contenidos dinámicos de la web como barras de búsqueda o formularios ya que es la parte que se encuentra en contacto directo con la base de datos. Gracias a la introducción de estos comandos, se puede conseguir acceso a los datos, modificarlos e incluso eliminarlos.

Este tipo de ataques, pueden suponer una catástrofe para la empresa ya que dependiendo de la estructura elegida los datos bancarios de los clientes pueden quedar expuestos.

Protección

Para poder evitar este tipo de ataques es necesario la construcción de un código robusto coma el uso de determinadas funciones y consultas parametrizados impide que los comandos SQL se entiendan como consultas reales. Cuando se construye el sitio web, es importante evitar mostrar información innecesaria si se obtiene error en la ejecución de alguna función ya que puede facilitar el trabajo a los atacantes.

Otro de los aspectos que tener en cuenta, es la gestión de privilegios que se le da a las diferentes cuentas sobre la base de datos, los poderes deben ser limitados únicamente a la cuenta de administrador.

Uno de los recursos que la empresa puede plantearse, es construir una estructura en la que datos importantes como los números bancarios, no se almacenen en su propio servidor y hacer uso de compañías externas que asuman esa responsabilidad.

4.6 ATAQUES POR *MALWARE*

También conocido como software malicioso, es creado con el objetivo de producir daño en un sistema informático y acceder a los datos que este alberga.
Estos programas son utilizados para atacar a una empresa y robarle la información que posee, dañar sus dispositivos o realizar chantajes económicos a cambio de devolver el control del sistema.

En un comercio online el activo más importante es la información, la perdida o deterioro de esta supone en el peor de los casos, que los datos bancarios de todos sus clientes queden expuestos. Todos estos datos, son almacenados tanto en la red de ordenadores de la tienda como en los servidores en los que se aloja. La infección de parte de este sistema supondría una pérdida irreparable para la tienda online ya que, si bien pudiera continuar operando, perdería toda la confianza de los compradores.

La diversidad de programas maliciosos que existe es realmente amplia ya que se crean nuevos diariamente. Aunque existan cada vez más tipos de *malware* que emplean métodos de infección diferentes, la manera de hacerles frente es la misma, el uso de una herramienta eficaz antimalware en su última versión. A continuación, aparecen los softwares maliciosos que afectan de forma más común a el comercio electrónico.

4.6.1 VIRUS

Este software malicioso está construido para que se reproduzca continuamente y así pueda infectar a todos los dispositivos posibles. Las formas más habituales de transmisión del virus son a través del correo electrónico, en archivos adjuntos o en la descarga de archivos desde internet, pero también pueden propagarse empleando dispositivos extraíbles o al conectarse a redes desconocidas.

Los virus tienen la capacidad de editar archivos que están en el dispositivo infectado por lo que pueden tomar el completo control de este y proceder según los intereses del ciberdelincuente.

En el caso de que un virus tome el control del ordenador con el que se gestiona la tienda, esto supondrá que el atacante obtendrá control absoluto sobre esta y podrá realizar cambios e incluso infectar los dispositivos de los clientes.

Protección

Como se ha comentado antes, la forma de protegerse de estos programas es la instalación de un, en este caso, antivirus y mantener los últimos parches instalados. Además, si se tiene cuidado de no descargar archivos de origen desconocido de la red, las probabilidades de sufrir un ataque de estas características disminuyen notablemente. También pueden emplearse herramientas online de análisis de archivos en busca de virus, como la que se menciona en el capítulo anterior.

4.6.2 KEYLOGGERS

Es especialmente importante prestar atención a este tipo de programa, afecta tanto a usuarios compradores como gestores de tiendas online. Este *malware* tiene la capacidad de registrar todas las teclas pulsadas del teclado y aunque suele darse en formato software, puede insertarse en elementos como un dispositivo de almacenamiento.

Gracias a la infección con este programa, cuando se accede a una cuenta protegida mediante contraseña, al teclearla o al insertar los datos relativos a una tarjeta de crédito, estos son guardados por el ciberdelincuente.

En el caso del gestor de una tienda, si accede a esta, los datos de acceso serán revelados al atacante proporcionándole acceso al resto de datos.

Protección

Se recomienda el seguimiento de los consejos relativos a la instalación de softwares mencionados anteriormente y no conectar dispositivos extraíbles desconocidos a red.

Además, si aun así nuestro dispositivo es infectado, se puede hacer uso de aplicaciones que proporcionan teclados virtuales. En estos, el orden de letras varía aleatoriamente y se utiliza un método de clic para seleccionar la letra, evitando de esta manera que se conozcan los caracteres introducidos.

4.6.3 STEALERS

El objetivo es similar al de los *keyloggers,* obtener las contraseñas y datos de acceso a cuentas, pero en este caso el software realiza un análisis de las aplicaciones instaladas y roba de ahí el nombre o las credenciales guardadas. Al almacenar las contraseñas en gestores no seguros como los de los navegadores, al sufrir este tipo de ataques todos los datos de acceso quedan a merced del atacante.

Su distribución se lleva a cabo mediante archivos adjuntos infectados y descargas de aplicaciones de sitios fraudulentos. Tras conseguir su objetivo, el ciberdelincuente procederá a realizar otros fraudes con la información conseguida.

Protección

En primer lugar, con el objetivo de que el programa no acceda a el sistema, se recomienda una herramienta antimalware y ser cauto en la interacción con los elementos usados para perpetuar los ataques cibernéticos como enlaces o archivos adjuntos.

De todas formas, si por algún descuido este programa consigue colarse, no deben almacenarse contraseñas en lugares poco seguros como el navegador, las notas o un documento. Se puede hacer uso de programas gestores de contraseñas seguros, que facilitarán el trabajo de recordar todas estas diferentes contraseñas.

4.6.4 RANSOMWARE

Este malware se ha vuelto muy popular en los últimos años entre los criminales de internet ya que se utiliza para obtener un beneficio económico. El plan consiste en inutilizar todos los dispositivos y encriptar todos los datos que albergan extendiendo la infección todo lo que ese pueda en el sistema. Cuando los delincuentes han tomado el control, aparece un mensaje en las pantallas de los dispositivos que indica el precio del rescate para la recuperación de los datos, amenazando con la eliminación total de estos si no se colabora.

Aunque este ataque se puede detectar antes de que todo el sistema esté sentenciado, los atacantes los realizan estratégicamente durante los fines de semana o días no laborables para aumentar la capacidad de alcance de este.

Los adjuntos en emails son el medio preferido utilizado para la propagación ya que el ataque suele dirigirse a empleados de empresas haciendo uso de técnicas de ingeniería social. También es posible que el software venga oculto en enlaces, archivos y descargas ilegítimas de programas.

Protección

Para evitar que este tipo de ataques prosperen, es necesario que todos los dispositivos conectados a la red de la empresa dispongan de programas antimalware, así como que todos los empleados reciban información acerca de la ciberseguridad.

Con el fin de minimizar el impacto del ataque si éste sucediera, es recomendable realizar copias de seguridad recurrentes y almacenarlas en un lugar independiente de la red pudiendo así recuperar los datos en caso de ser necesario.

En el caso de sufrir un ataque de este tipo, el Instituto nacional de ciberseguridad ofrece una ayuda para guiar a las compañías y recomienda no pagar nunca el rescate.

En el caso de que los datos robados contengan información personal sensible, es necesario notificar el ataque en un plazo de 72 horas a la AEPD (Agencia Española de Protección de Datos).

4.6.5 SPYWARE

La instalación de este programa en un equipo supone la monitorización de toda la actividad de este remotamente, además de obtener el control de el. Este control remoto además del acceso al contenido y grabación de los datos de cualquier programa o de accesorios como la cámara y el micrófono constituyen un flagrante peligro para la integridad de la compañía. Toda acción que se realice con el dispositivo infectado, como consultar los movimientos bancarios de la tienda serán visibles para el creador del ataque.

El spyware puede llegar a un equipo realizando acciones cotidianas, un simple clic en un anuncio emergente de una página poco fiable puede comenzar la descarga de este.

Protección

Cuando se realicen instalaciones de programas en los ordenadores, es recomendable realizarlas de las webs oficiales ya que usualmente los spyware, son instalados en segundo plano de la instalación de otro software. Al aceptar la instalación del primero, el usuario acepta el segundo al no prestar atención a las condiciones aceptadas.

Por otro lado, se recomienda evitar clicar en enlaces, anuncios o cualquier otro tipo de banners en sitios web que no son confiables y como para cualquier otro tipo de *malware*, el uso de una herramienta de protección antimalware.

4.6.6 TROYANOS

Este programa maligno se oculta en el equipo haciéndose pasar como un software cualquiera mientras se dedica al robo de información. Cuando un troyano consigue alojarse en un dispositivo, este puede obtener el control total de este y por ende tiene acceso a todos los datos almacenados.

El acceso al sistema lo obtiene empleando los típicos medios de infección cómo son los correos electrónicos, archivos descargados, ...

Protección

Debe evitarse la descarga, instalación y ejecución de archivos de los cual no se conoce la procedencia, pudiendo hacer uso de los recursos web de análisis mencionados, pero siendo consciente de que no garantiza la seguridad.

Como siempre debe utilizarse un programa de detección de *malware* y mantenerlo en su última versión.

4.6.7 BACKDOORS

Su nombre "puertas traseras" explica su funcionamiento, se alojan en el sistema sin ser detectados intentando crear un orificio de entrada por el que van tomando el control del dispositivo, que su creador puede manejar a distancia.
La vulnerabilidad de las tiendas online ante este tipo de ataques consiste en que, además de obtener todos los datos almacenados y monitorear toda la actividad que se produce, puede modificar cualquier información u ordenar acciones al sistema.

La vía de transmisión sigue siendo la misma que los anteriores casos, archivos adjuntos, enlaces e instalaciones fraudulentas.

Protección

Si se realizan descargas desde tiendas autorizadas y se presta atención a los términos aceptados durante su descarga, se cierra una de las puertas de entrada más comunes de estos programas. Lo mismo sucede si se evita la descarga de archivos de origen desconocido y el acceso a webs desde enlaces peligrosos.

Si se hace uso de un programa de detección de *malware* y se actualiza este de forma continua, las probabilidades de sufrir este tipo de ataque son mínimas.

4.6.8 GUSANO

El objetivo de este programa maligno no es el robo directo de datos o credenciales, sino reproducirse e infectar todos los programas y dispositivos posibles. Mientras este programa trabaja utiliza los recursos propios del sistema en el que se esconde poniendo en peligro el correcto funcionamiento de este y de los usuarios que acceden a él.

El hueco que los gusanos utilizan para introducirse son los archivos, programas o dispositivos hardware. Si se conecta un dispositivo a un equipo infectado, el gusano accederá a el y cuando este sea conectado a un equipo libre de infección procederá a instalarse también en este.

Protección

Disponer de herramientas y programas de protección actualizados y activos para que en el caso de intentar acceder estos lo impidan, es vital para la seguridad del sistema. Por otro lado, deben evitarse las posibles vías de entrada de este software mediante una navegación segura.

4.6.9 BOTNETS

También conocida como red zombi, es un conjunto de dispositivos que han sido infectados y que son controlados remotamente por un ciberdelincuente.

Si los equipos de una empresa se ven infectados, el atacante puede realizar diversas acciones sobre ellos, por ejemplo, la captura de contraseñas, el envió de spam y virus, la realización de ataques DDoS o de fraudes bajo el nombre de la compañía.

Además, los dispositivos infectados utilizarán sus recursos para realizar las acciones ordenadas por el delincuente, disminuyendo la capacidad de estos y pudiendo también ralentizar o dejar sin servicio la página web.

Protección

INCIBE (Instituto Nacional de Ciberseguridad de España) ofrece un servicio gratuito llamado Antibotnet, este servicio permite al empresario comprobar si algún dispositivo de su empresa está infectado con botnet. Para ello, se comprueba si el IP público de la compañía se relaciona con alguna red botnet conocida y en caso afirmativo, a pesar de no identificar el dispositivo infectado, el instituto nacional ofrece información y herramientas para la desinfección.

4.6.10 CRIPTOJACKING

Actualmente el mercado de las criptomonedas está en auge, no como forma de pago online ya que su uso no está aún generalizado, sino como método especulativo. La

cantidad de transacciones que se llevan a cabo diariamente es inmensa y en la realización de cada una de esas transacciones se genera un beneficio económico, el intentar conseguir este beneficio, se le conoce como minar.

Para minar se necesita una gran cantidad de recursos al alcance de muy pocos, debido a la extrema competición que hay por conseguir el dinero, muchos cibercriminales están empezando a emplear este tipo de *malware* para poder utilizar los recursos de los sistemas infectados, en el minado de criptomonedas.

Este consumo de recursos puede llevar a que un sitio web no disponga de los necesarios para poder funcionar y por ende quede fuera de servicio.

Protección

La forma de protegerse de esto es el uso de herramientas de protección en los equipos como firewalls y sistemas de protección contra programas maliciosos. Además, como el funcionamiento de este tipo de ataques también implica el el sometimiento de los dispositivos de forma remota, es posible utilizar el servicio Antibotnet proporcionado por INCIBE para detectar y eliminar la infección.

NECESIDAD	RECURSO RECOEMNDADO
Almacenamiento de contraseñas	Keeper, Dashlane
Detección de virus en archivos	VirusTotal
Comprobación de enlaces	VirusTotal
Teclado virtual	Microsoft Swiftkey
Comprobación emails	Messageheader
Red zombi	Antibotnet

Tabla VII. Recursos recomendados para la protección contra amenazas

CAPÍTULO 5. CASO DE APLICACIÓN

5. CASO DE APLICACIÓN

Una vez expuestos los aspectos relativos al comercio electrónico y a la seguridad, y tras describir cómo puede una tienda electrónica ver vulnerada la seguridad de su información, en este capítulo va a explicarse cómo estos conceptos han servido para la creación de GymRat como caso de aplicación.

5.1 CARACTERÍSTICAS DE GYMRAT

Para poder construir una tienda online coherente cuyo objetivo es probar todas las cuestiones que han sido presentadas anteriormente de forma teórica, el primer paso ha sido decidir la actividad a desarrollar y las bases de la empresa simulada.

La primera idea que surgió fue acerca de una empresa dedicada a la activad física, después de elaborar ligeramente el concepto surgió GymRat. Este término hace referencia a una expresión muy empleada para denominar a las personas que son muy asiduas al entrenamiento de fuerza y que, por ello pasan muchas horas ejercitándose en el gimnasio.

La actividad de la pequeña empresa simulada se centrará en la venta y distribución de productos y materiales deportivos de alta calidad, seleccionando estos con criterio científico como elemento diferenciador con respecto al resto del mercado. Además, esta tienda solo realizará ventas de forma electrónica, prescindiendo del medio tradicional.

La misión, visión y valores de la empresa están reflejados en la página corporativa de esta, centrándose y resaltando siempre la importancia del uso de la ciencia y la biomecánica para conseguir la máxima eficiencia deportiva. El objetivo perseguido en la creación de la tienda es hacer que el consumidor sienta que forma parte de la familia GymRat.

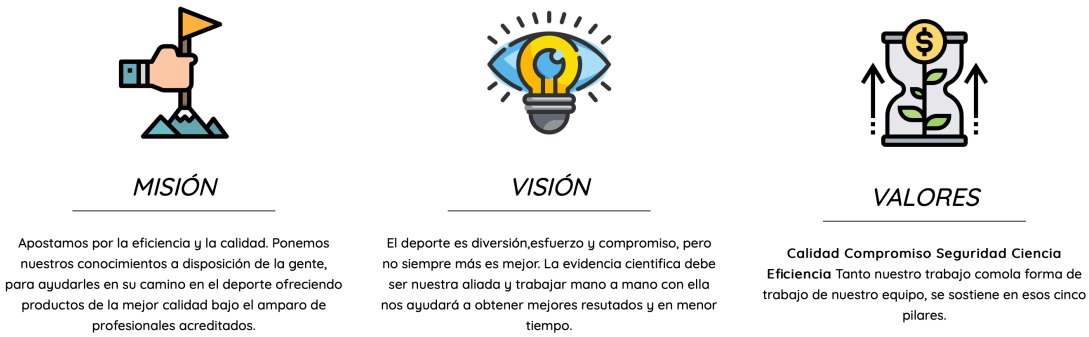


Figura 19. Misión, visión y valores de GymRat reflejados en su sitio web.

El siguiente paso en la construcción de la tienda electrónica ha sido crear la *website* de la empresa. Para ello, a partir de un servidor web y un servidor de bases de datos, se ha construido la web usando páginas HTML5 y CSS3. Las páginas web dinámicas han sido diseñadas mediante lenguaje PHP que además realiza las funciones de envío de consultas a la base de datos. El sistema gestor de bases de datos empleado es MariaDB.

Al tratarse de una empresa de nueva creación, tanto su tamaño como sus recursos son reducidos por lo que únicamente hay un empleado que además actuará con el rol de administrador.

5.2 CONSTRUCCIÓN DEL SITIO WEB

El sitio web de GymRat se ha dividido en dos partes, una corporativa que presenta a la compañía y su forma de trabajo conteniendo información relativa a la parte comercial de esta, y otra que constituye la propia tienda online.
Estas dos partes se encuentran relacionadas y es posible el acceso de una a otra durante la navegación por la web por lo que, a pesar de estar separadas en su estructura, trabajan y son percibidas por el usuario como un conjunto.

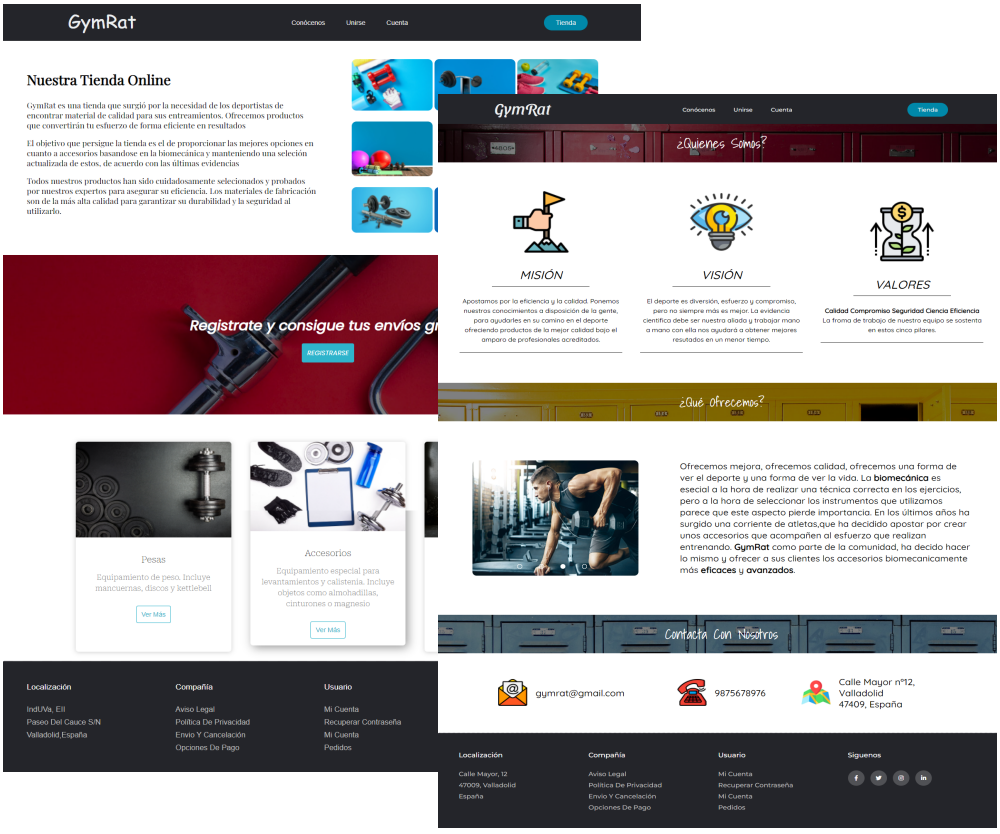


Figura 20. Captura de las páginas Index y Conócenos

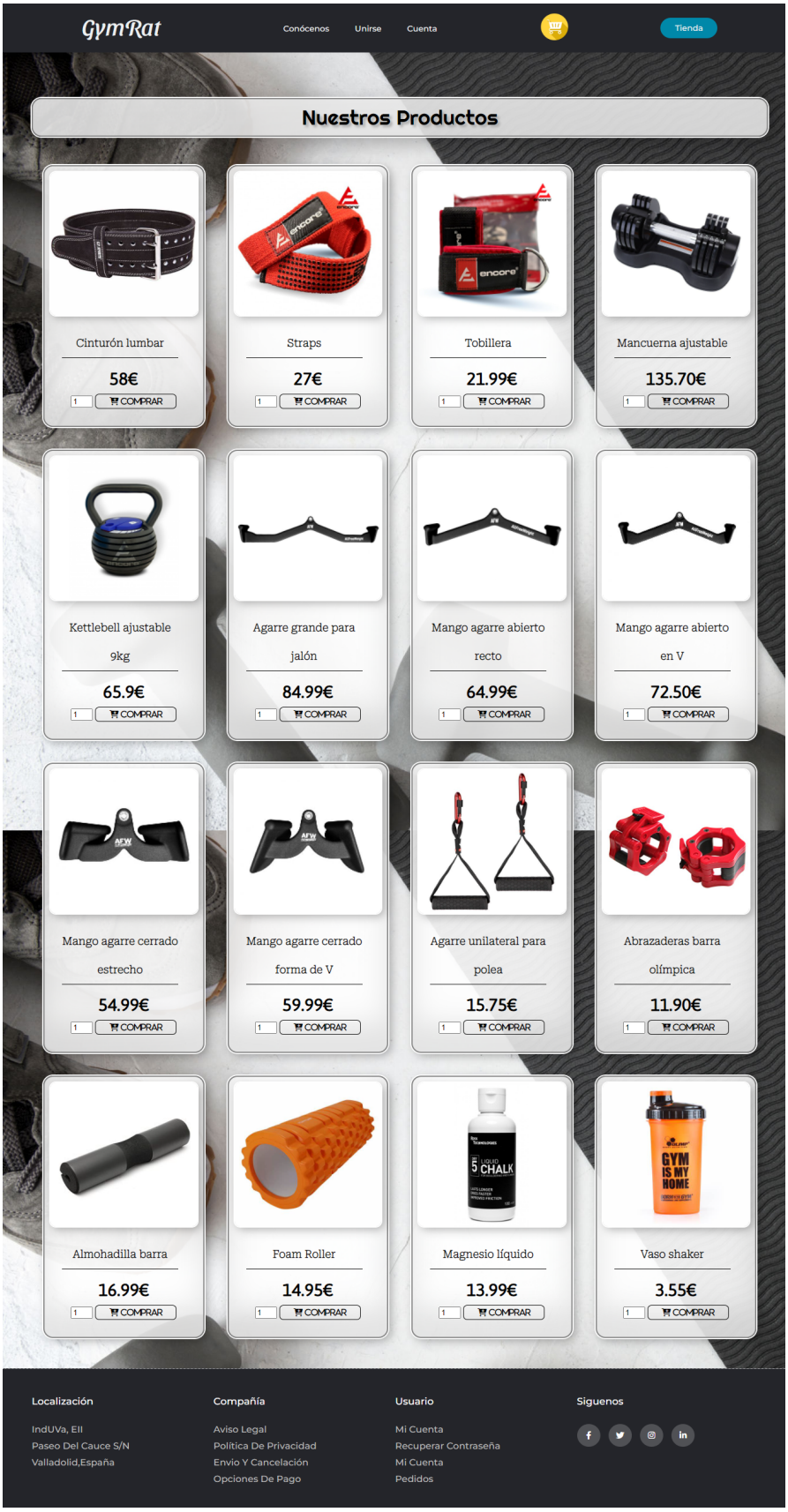


Figura 21. Captura de la página Tienda

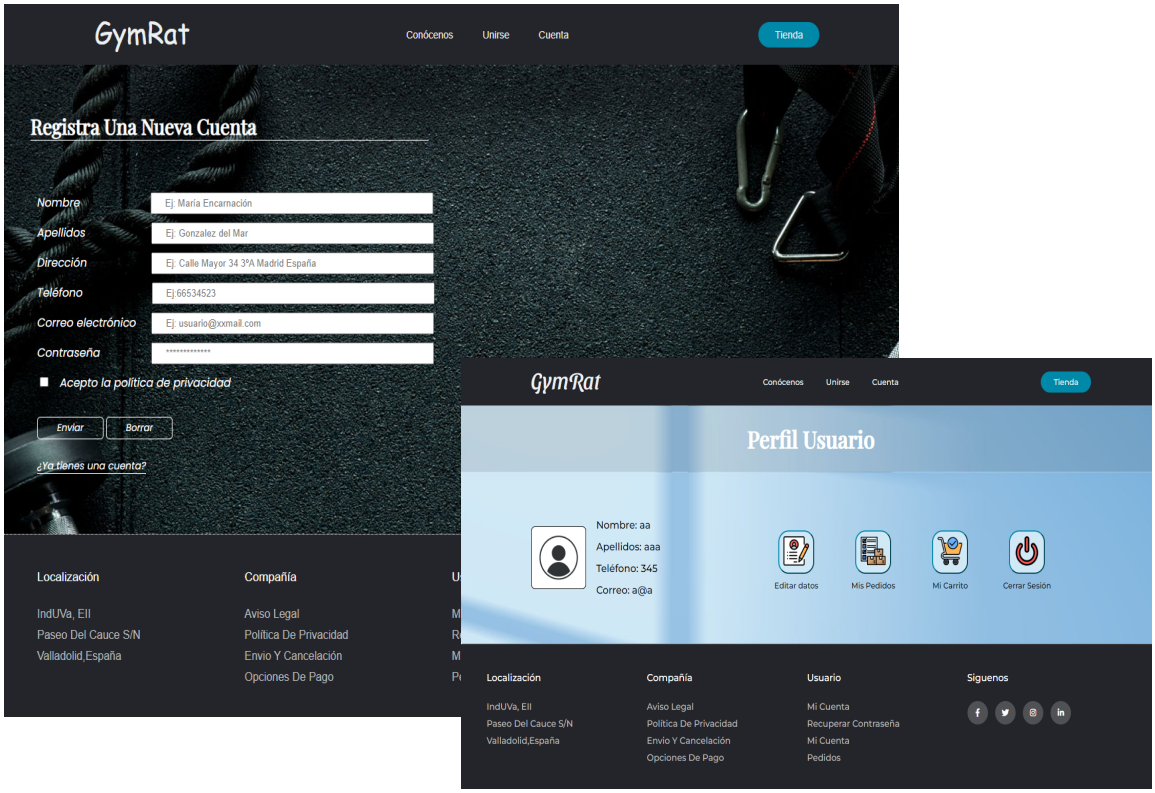


Figura 22. Captura de las páginas Unirse y Perfil

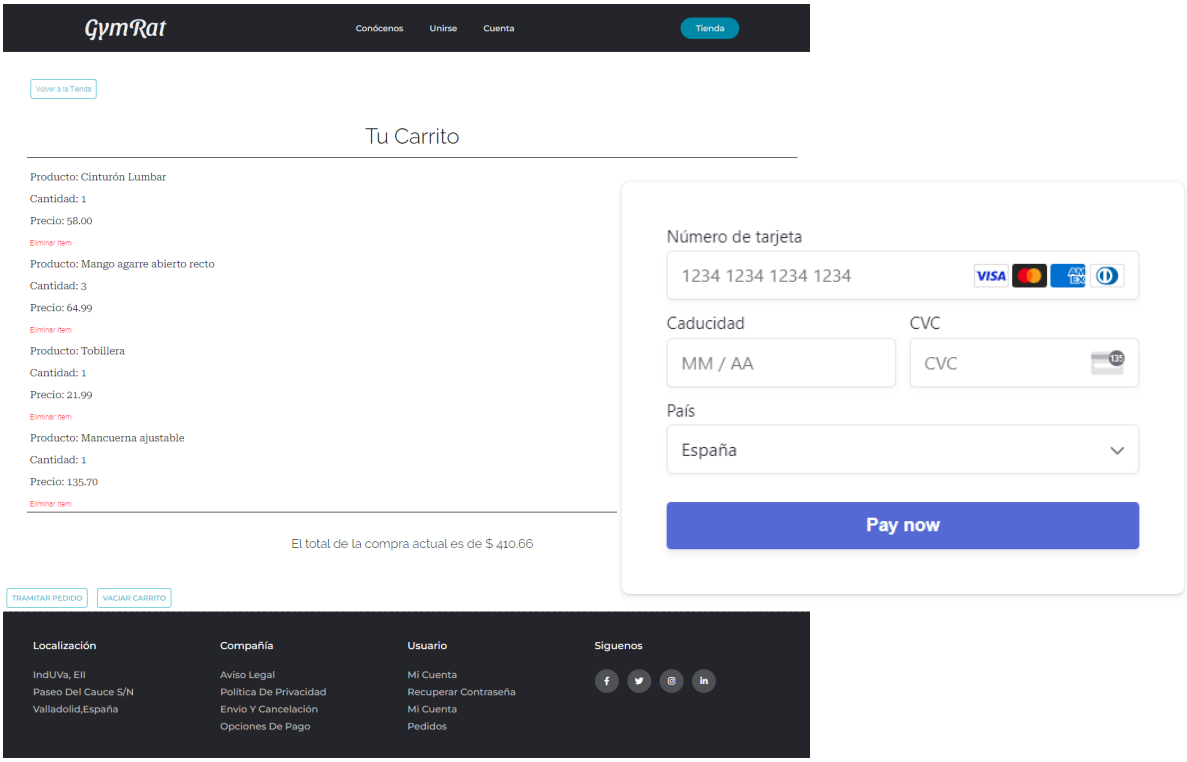


Figura 23. Captura de la página Carrito y de la Pasarela de pago

Desde el punto de vista técnico, cuando se construye una tienda online se necesitan diseñar tres aspectos: el *front-end*, el *back-end* y le base de datos (que podría incluirse dentro del back-end).

El front-end se refiere a la parte estática de la página, una interfaz gráfica que permite al usuario interaccionar con la información fijada en ella. Algunos ejemplos de esta son la página principal, la página conócenos o la página del aviso de privacidad.

El *back-end,* sin embargo, conforma la parte dinámica de la página, es el área lógica que modifica la información según las acciones o información introducida por el usuario. Dentro de esta categoría se encuentran el carro de la compra, el registro de usuarios o la tramitación del pedido.

La base de datos, por último, se encarga de almacenar y proporcionar todos los datos necesarios para el funcionamiento de la tienda online. En esta, se almacenan los datos de registro de los clientes, los productos y precios de la tienda, así como la información de todos los pedidos realizados.

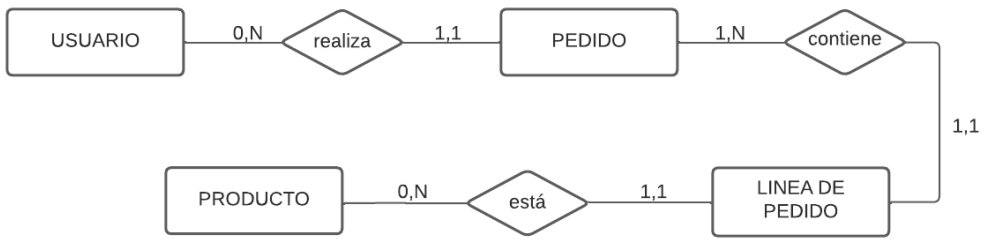


Figura 24. Modelo conceptual para la base de datos de GymRat

La Figura 24 representa el modelo conceptual de la base de datos utilizada, que proporciona una visión centrada en los datos sobre como funciona la organización. En este, se representan las principales entidades que participan en las operaciones de la empresa y las relaciones que surgen.

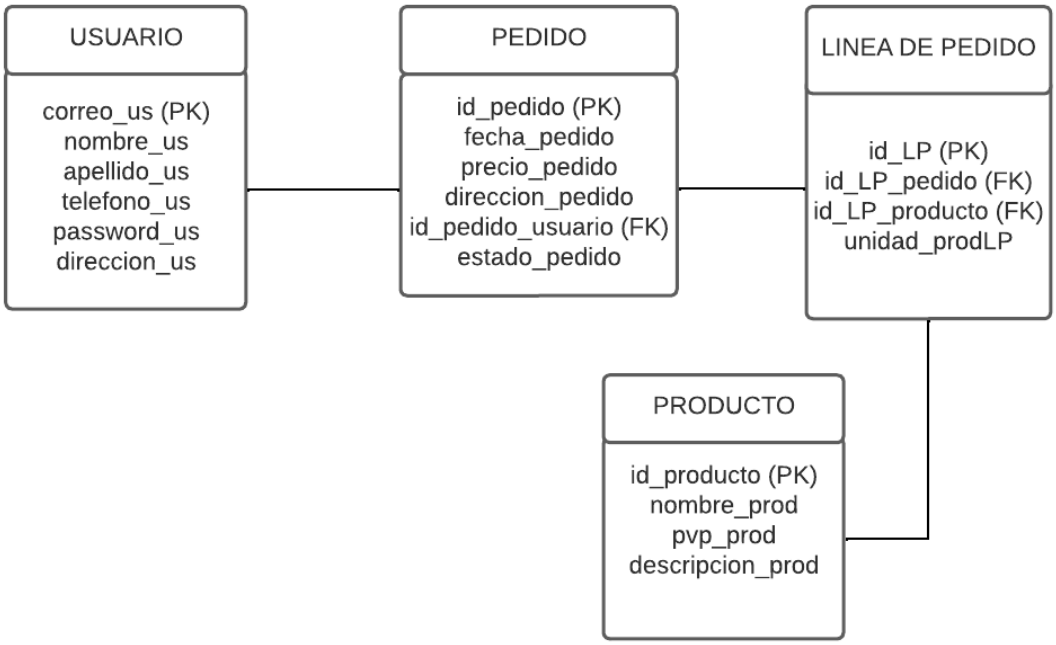


Figura 25. Modelo lógico para la base de datos GymRat

Tras la construcción del modelo conceptual para el que se utiliza un diseño de alto nivel, se debe traducir este a un esquema más detallado que tenga en cuenta los requisitos del sistema. Este modelo es conocido como modelo lógico y se puede ver representado en la Figura 25.

En el modelo lógico, se representan las entidades como tablas y las relaciones entre ellas como líneas, dentro de las tablas aparecen las diferentes columnas de datos que las conformarán estableciendo así las características propias de cada entidad.

Aunque existen más posibilidades, en la base de datos construida para GymRat los datos asociados a las columnas se clasifican en uno de estos tres supuestos:

- Clave primaria (PK *Primary key*): es obligatoria y sirve para identificar de forma única e inequívoca cada fila de una tabla.

- Clave foránea (FK Foreign key): proporciona un enlace entre datos almacenados en dos tablas.

- Atributos: definen las características de una entidad o tabla dando la información necesaria sobre esta.

Una vez el modelo lógico está completo es momento de normalizarlo y convertirlo en una base de datos real, para esto se emplea el lenguaje SQL. En este lenguaje es preciso especificar el tipo de dato que va a ser introducido y a pesar de existir muchas mas tipologías, en la creación de la base de datos de esta empresa su uso se ha restringido a los siguientes:

- int (tamaño): dato numérico que permite cifras del -2147483648 al 2147483648.

- tinyint (tamaño): dato numérico que permite cifras del 0 al 255.

- decimal (p,s): dato numérico decimal, p indica número máximo de dígitos total entre la izquierda y la derecha de la coma, y s indica el número de cifras decimales.

- varchar (tamaño): cadena de caracteres de longitud variable cuya longitud máxima es el tamaño indicado. Lo máximo que puede almacenar son 255 caracteres.

- text: permite insertar un texto con longitud máxima de 255 caracteres.

- datetime: indica la fecha y la hora en formato AAAA-MM-DD HH: MI: SS.

Una vez las tablas, relaciones y tipos de datos han sido definidos, la base de datos puede ser construida.

Las siguientes tablas recogen las columnas y los tipos de datos que almacenan estas, en el caso de la base de datos de GymRat.

Pedido

	NOMBRE	TIPO DE DATO
CLAVE PRIMARIA	id_pedido	int (11)
CLAVE FORÁNEA	id_pedido_usuario	varchar (50)
ATRIBUTO 1	fecha_pedido	datetime
ATRIBUTO 2	precio_pedido	decimal (10,2)

ATRIBUTO 3	direccion_pedido	varchar (80)
ATRIBUTO 4	estado_pedido	varchar (10)

Tabla VIII. Datos de la entidad Pedido

Usuario

	NOMBRE	TIPO DE DATO
CLAVE PRIMARIA	correo_us	varchar (50)
ATRIBUTO 1	nombre_us	varchar (20)
ATRIBUTO 2	apellido_us	varchar (40)
ATRIBUTO 3	telefono_us	varchar (12)
ATRIBUTO 4	password_us	varchar (15)

Tabla IX. Datos de la entidad Usuario

LP

	NOMBRE	TIPO DE DATO
CLAVE PRIMARIA	id_LP	int (11)
CLAVE FORÁNEA	id_LP_pedido	int (11)
CLAVE FORÁNEA	id_LP_producto	int (11)
ATRIBUTO 1	unidad_prodLP	tinyint (4)

Tabla X. Datos de la entidad LP

Producto

	NOMBRE	TIPO DE DATO
CLAVE PRIMARIA	id_producto	int (11)
CLAVE FORÁNEA	nombre_producto	varchar (40)
CLAVE FORÁNEA	pvp_prod	decimal (10,0)
ATRIBUTO 1	descripcion_prod	text

Tabla XI. Datos de la entidad Producto

Una vez diferenciados estos tres aspectos de la construcción de la website, se pueden detallar los lenguajes utilizados para su realización:

- Front-end: el contenido estático ha sido creado con HTML5 y el estilo de este se ha editado mediante CSS3.

- Back-end: construido mediante PHP7, que ha permitido dotar de lógica al sitio web y su comunicación con la base de datos.

- Base de datos: ha sido necesario el uso de SQL, lenguaje propio de estos programas cuya interfaz de gestión ha sido phpMyAdmin.

5.3 ELECCIÓN DE PASARELA DE PAGO

Una vez terminado el sitio web e implementada la tienda online con todas las operaciones en correcto funcionamiento, es momento de proceder a la integración de la pasarela de pago. Este último paso permitirá convertir todo el trabajo logístico y lógico realizado en ingresos monetarios reales para la tienda online por lo que, es importante seleccionar aquella pasarela que se adecue al caso de GymRat y cuya implementación sea posible.

En la Tabla XII se ofrece una comparativa de las opciones barajadas en la selección de la pasarela idónea.

	MÉTODOS DE PAGO	PRECIO	PERSONALIZACIÓN	INTEGRACIÓN	SEGURIDAD	ALMACENAMIENTO DE TARJETAS
PAYPAL	Tarjetas, cuentas bancarias, links y QR	2.9% + 0.35€	Alta	Sencilla mediante API	PCI DSS, 3D Secure, política reembolso fraude	SI
STRIPE	Tarjeta, transferencia, AliPay, Apple Pay, GooglePay…	1.4% + 0.5€	Depende del grado de integración pudiendo ser completo	Diferentes grados, sencilla mediante API o con gestores de contenido	PCI DSS, seguridad antifraude, encriptación AES, *tokenización*	SI
REDYS	Tarjeta, Bizum, PayPal, Apple Pay, GooglePay…	No es público	Limitada en gestores de contenidos, mayor en integración total.	Diferentes grados, sencilla mediante API o con gestores de contenido	PCI DSS, 3D Secure, *tokenización*	SI
PAYCOMET	Tarjeta, transferencia, Apple Pay, GooglePay, AmazonPay…	19€ al mes (hasta 2000€ sobrecoste de 0.5% + 0.09€)	Limitada en gestores de contenidos, mayor en integración total.	Muchas posibilidades, sencilla mediante API o con gestores de contenido	PCI DSS, módulo contra fraude, *tokenización*	SI
UNIVERSALPAY	Tarjeta, transferencia	9.99€-19.99€ al mes (sobrecoste de 0.5% + 0.1€)	Aumenta según lo hace el grado de integración	Diferentes grados, puede ser sencilla	PCI DSS	SI
BRAINTREE	Tarjeta, cuenta bancaria y PayPal	2.9% + 0.3€	Completamente personalizable	Es necesario un profesional	PCI DSS, 3D Secure y encriptación máximo nivel	SI
CHECKOUT.COM	Tarjeta, Apple Pay y GooglePay	No es público	Solo es personalizable fuera de los gestores de contenido	Sencilla en gestores de contenido. De otro modo es necesario un desarrollador	PCI DSS, 3D Secure y creación de perfiles de riesgo	NO
2CHECKOUT	Tarjetas y PayPal	3,5% + 0.25€ (Cuota por devolución 20€)	Alta en todos los tipos de integración	Muchas posibilidades, sencilla mediante API o con gestores de contenido	PCI DSS, buen sistema antifraude	NO
MONEI	Tarjeta, Apple Pay, GooglePay,	0.9% + 0.24€ o tarifas	Opciones escasas	Muchas posibilidades, sencilla mediante API	PCI DSS, PSD23 Y 3D Secure	NO

	Bizum, Bitcoin…	anual de 990€		o con gestores de contenido		
AMAZONPAY	Tarjeta, transferencia y pago diferido o recurrente	3.4% + 0.35€	Posibilidad media de personalización	Integrable con gestores de contenido	PCI DSS, encriptación y doble verificación	SI
ADDON PAYMENTS	Tarjeta, PayPal, GiroPay…	9€-19€ + tasa de descuento	Permite amplia personalización	Ofrece integración por 100€, integración sencilla con API y en gestores de contenido	PCI DSS, 3D Secure, reglas antifraude	NO

Tabla XII. Comparativa de pasarelas de pago

La mayor parte de las pasarelas de pago elegidas son compatibles con el caso de estudio de este trabajo, no obstante, hay algunas que pueden ser directamente descartadas por aspectos relacionados con su integración.

La pasarela de CheckOut.com requiere de la contratación de un desarrollador para realizar la integración en la tienda online por lo que esta opción no es viable. Además, los precios que ofrece no son claros y es preciso contactar con el servicio al cliente para obtenerlos. A pesar de la gran seguridad que ofrece la entidad esta queda descartada.

La complejidad en cuanto a la integración de Braintree convierte a esta en una opción poco apta, la especialización de esta pasarela en los pagos a través de dispositivos móviles tampoco resulta interesante para GymRat por lo que también es descartada.

AmazonPay tiene varios factores en contra, el principal es que trabaja únicamente con grandes volúmenes de venta. Además, al obligar a los clientes a crear una cuenta en Amazon, en el que se ofrecen todo tipo de productos de muchos vendedores, la competencia directa a la que se enfrenta la tienda se incrementa.

En el caso de UniversalPay y Paycomet no es la complejidad lo que las descarta, sino que las tarifas que ofrecen se basan en volúmenes de venta y cuando se sobrepasa el límite seleccionado, se cobran tarifas adicionales por transacción. Como GymRat es una empresa de nueva creación es complicado estimar el volumen de ventas que obtendrá en los primeros meses del ejercicio por ello, el riesgo de sobrecostes las convierte en una mala opción. Otra característica de UniversalPay que le resta

atractivo es la escasez de medidas y herramientas antifraude en su plataforma, lo que incrementa la probabilidad de devoluciones de cargo y por tanto de los costes.

Redys es aparentemente una buena opción en cuanto a seguridad, opciones de expansión, pago e integración, que gracias a la API que ofrece la compañía se realiza de manera sencilla. El problema que aparece es en cuanto a la falta de transparencia en los costes, según las informaciones proporcionadas por algunos clientes de la plataforma las tarifas son de un coste elevado. Estos factores económicos suponen que la plataforma pierda puntos y quede descartada.

PayPal a pesar de ser una reputada pasarela de pago, compatible y muy segura, ofrece unas tarifas superiores a la media del mercado. Por ello, al ser este un negocio con un previsible volumen de ventas bajo, el coste por transacción resultaría demasiado elevado. Además, otras pasarelas integran PayPal como forma de pago y ofrecen unas características y precios más acordes al caso.

Con 2Checkout sucede lo mismo que con PayPal al ser una subsidiaria de esta, los precios que se ofrecen son muy altos, pero, además no ofrece la opción de almacenar los datos bancarios de forma segura en su propia plataforma por lo que el descarte de esta es claro.

La dos últimas opciones desechadas, son Monei y Addon Payments que a pesar de las buenas tarifas ofrecidas y el alto grado de seguridad del que disponen, no son aptas para la tienda ya que no ofrecen la posibilidad de almacenar la información bancaria de los usuarios.

Finalmente, la opción elegida es:

STRIPE

Esta pasarela de pago ofrece multitud de métodos de pago por un precio asequible.

La seguridad de la plataforma es de una alta calidad, sigue los protocolos PCI DSS y dispone de un sistema antifraude además de una encriptación de alto nivel. Los datos bancarios se encuentran protegidos mediante cifrado desde el momento de su ingreso en el formulario hasta su almacenaje en el servidor de la pasarela, en este son almacenados en forma de *tokens* asegurando así su confidencialidad. Este tipo de sistema de almacenaje de datos permite que GymRat cumpla con la normativa PCI de almacenamiento de información de tarjetas de pago.

La integración de Stripe en la tienda online se realiza de manera sencilla mediante una API y se encuentra disponible en diferentes lenguajes de programación incluido PHP7 por lo que su integración es viable. La empresa dispone de manuales de integración para desarrolladores en los que se explica cómo añadirla a la web y personalizarla de forma sencilla. Además, proporciona unas claves y tarjetas bancarias de prueba para poder comprobar el correcto funcionamiento de la pasarela tras su integración.

5.4 SEGURIDAD DE LA TIENDA ONLINE

El sitio web se ubica en un servidor protegido mediante firewalls, su posicionamiento en una zona desmilitarizada provoca que en el caso de que un ataque se lleve a cabo exitosamente contra el servidor web, el resto de la red se mantenga protegida.

Todos los dispositivos de la empresa disponen de softwares de protección antimalware y de detección de intrusos. Además, los dispositivos extraíbles de almacenamiento que se emplean para guardar los datos se encuentran cifrados por lo que, en caso de pérdida o robo no podrá accederse a la información.

Respecto a uno de los peligros más comunes, el de los ataques por ingeniería social, todos los empleados han realizado o realizarán cuando entren a formar parte de la empresa, un curso de concienciación sobre ciberseguridad. De esta manera se evitará caer en las estratagemas utilizadas por los ciberdelincuentes.

La realización de copias de seguridad será periódica y se realizarán a las 20:00h todos los días en un dispositivo externo separado del resto de la red. De esta manera en caso de sufrir un ataque *ransomware* la pérdida será mínima y no será necesario el pago del rescate.

Desde el punto de vista de la base de datos además de la construcción de un código robusto, los poderes de administración y modificación de datos están limitados únicamente al administrador del sistema. De esta forma se impide que las inyecciones SQL, que son realizadas desde otras cuentas, se lleven a cabo.

Todos los datos introducidos en la página web son encriptados utilizando un algoritmo RSA del cual se han encontrado los métodos de codificación y descodificación en (Criptosistemas de clave pública. El cifrado RSA, s.f.)

Además de la protección que la encriptación proporciona a la información que se guarda en la base de datos, la pasarela de pago seleccionada permite el almacenamiento de la información bancaria en forma de *tokens*. Esto sumado al

certificado SSL que posee Stripe y su cumplimiento del PCI DSS, deja el almacenamiento de la información bancaria fuera de las responsabilidades de GymRat, pero completamente protegida.

Después de haber construido la tienda online y la base de datos desde cero, la realización de muchas pruebas y la estructura de seguridad con la que se ha dotado a GymRat, puede comprobarse si esta cumple el modelo de seguridad del triángulo CIA.

1. ¿Están los datos protegidos de ser interceptados por personas no autorizadas?

   Las medidas de protección tomadas en la creación y administración de GymRat hacen que toda información sensible con la que trabaja sea confidencial.

2. ¿Están los datos protegidos de ser cambiados o eliminados por personas que no deberían poder hacerlo?

   Los procesos de transmisión y modificación de la información han sido asegurados por lo que puede asegurarse la integridad de esta.

3. ¿Están los datos disponibles, para las personas que si deben tener acceso a ellos, cuando los necesitan?

   El funcionamiento tanto de los servicios del *website* como de las comunicaciones con la base de datos han sido comprobados en múltiples ocasiones. El funcionamiento es correcto y brinda la información correcta cuando es necesaria.

Se puede determinar en este caso, que la tienda cumple con el modelo del triángulo CIA, la integridad, confidencialidad y disponibilidad están asegurados.

5.5 MANUAL DE INSTALACIÓN

En este apartado se incluye una explicación de como disponiendo de todos los archivos que conforman el sitio web, puede replicarse GymRat.

5.5.1 SOFTWARE NECESARIO

Las herramientas utilizadas para construir el *website* han sido:

- HTML5
- CSS3
- PHP (versión superior a 5.3.3)
- Sistema gestor de Bases de datos MariaDB
- Servidor web HTTP Apache

Todo ello sobre una máquina virtual Linux del departamento de informática de la Universidad de Valladolid.

Además, se ha necesitado un editor de texto sencillo del estilo de Atom, Sublime Text o Notepad++. Para realizar la integración de la API de la pasarela de pago, ha sido necesaria la instalación de Composer, este programa es un sistema gratuito de gestión de paquetes para programar en PHP.

5.5.2 ARCHIVOS NECESARIOS

Para el funcionamiento correcto de la tienda ha sido necesario realizar:

6 ficheros .html	50 archivos .jpg
1 fichero .css	10 archivos .png
14 ficheros .php	1 carpeta “vendor”
1 script SQL	1 carpeta “public”
1 archivo .ico	

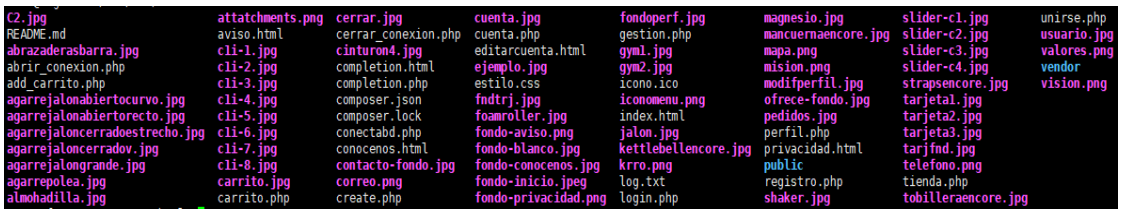


Figura 26. Archivos y ficheros para construcción de GymRat

La descarga de estos ficheros puede realizarse en el URL: http://virtual.lab.infor.uva.es:65072/tfg_tienda.tar.gz

5.5.3 INSTALACIÓN

En primer lugar, es necesaria la creación de la base de datos para lo que se debe acceder al gestor de bases de datos y pegar en la consola el contenido del script sql ("BasedeDatos.sql").

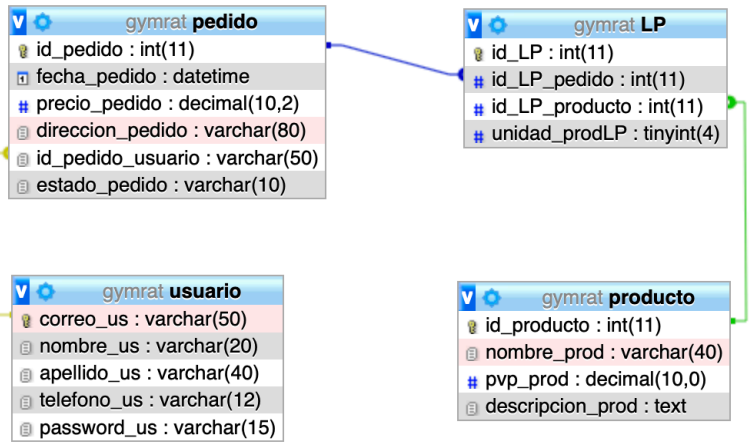


Figura 27. Modelo final de la base de datos GymRat obtenido en PhpMyAdmin

De esta forma se creará la base de datos que alimenta las páginas dinámicas del sitio web. Seguidamente, será necesario descargar el resto de los ficheros y archivos indicados en el anterior apartado y ubicarlos en un mismo directorio. (Preferiblemente /var/www/html para que puedan ser utilizados desde cualquier navegador).

Cuando todos los archivos estén ubicados, el sitio web estará operativo y puede procederse a la integración de la pasarela de pago.

Para poder utilizar Stripe como pasarela de pago es necesario crear una cuenta gratuita en su web. Una vez registrado, en el *dashboard* aparecerán las dos claves de la cuenta, una pública y otra privada, que permitirán trabajar con la pasarela de pago.

En este momento debe hacerse uso de las bibliotecas de Stripe disponibles en Composer para lo que, ubicándose en el mismo directorio en el que se han colocado

el resto de los archivos, debe introducirse el siguiente comando en la consola "composer require stripe/stripe-php".

El resto de los archivos necesarios para la pasarela se incluyen dentro de los ficheros enumerados en este trabajo ya que han sido modificados para trabajar con GymRat. (Carpeta "public" que incluye los ficheros "checkout.html", "checkout.css" y "checkout.js"; "composer .json" y create.php").

Al emplear una cuenta de Stripe diferente a la usada en primer lugar, es necesario modificar las claves que se incluyen en estos archivos ya que, se tratan de las claves propias de la cuenta de Gymrat. Para ello, debe accederse al fichero "checkout.js" y modificar la clave publica que aparece ya escrita por la nueva (Introducir donde indica "*This is your test publishable API key*").

```
// This is your test publishable API key.
const stripe = Stripe
("pk_test_51KzHyCHFTN53w39Uo9RJ7fHjgcCPNvD3WGlQH1btwteAu7Y");
```

Figura 28. Clave pública

En el caso de la clave privada, debe intercambiarse en el fichero "create.php" (Introducir donde indica "*This is your test secret API key*").

```
// This is your test secret API key.
\Stripe\Stripe::setApiKey('sk_test_51KzHyCHFTN53w39UNGfrM48U1YSqk
caSQQPAQngEzwYpLxGUiZLhxnpceVdOaG57B8Ups3CDnNTHaLE2itFxoLHg0089zL
HhKm');
```

Figura 29. Clave privada

Finalizados estos pasos, la construcción de la tienda online está completa y puede empezar a operar con normalidad.

CAPÍTULO 6. CONCLUSIÓN

6. CONCLUSIÓN

El objetivo de este trabajo ha sido adquirir conocimientos sobre las tiendas online y la seguridad en estas para obtener una visión global sobre cómo operan y poder construir una propia.

Para este cometido, ha sido necesario estudiar algunos conceptos sobre el comercio electrónico y su funcionamiento. Gracias a esto, se ha obtenido una perspectiva general sobre lo que una tienda online debe ofrecer a sus clientes para conseguir ser competitiva.

La infraestructura sobre la que se sustenta una tienda online es diferente a la conocida tradicionalmente, por ello las amenazas a las que enfrenta también son distintas y manifiestamente desconocidas por los usuarios.

Para poder crear una estructura segura para la tienda online, ha sido necesaria la identificación de los elementos que constituían una posible vía de entrada para estas amenazas. Tras identificar las más comunes en el ámbito del *ecommerce*, ha sido posible desarrollar una estructura de seguridad sólida para la tienda online construida.

El desarrollo de esta tienda online me ha permito aplicar todos los conocimientos adquiridos y desarrollar mi potencial en el ámbito del desarrollo *full-stack,* el cual formará parte de mi bagaje de conocimientos profesionales.

BIBLIOGRAFÍA

Ancarani, F., & Shankar, V. (2004). Price levels and price dispersion within and across multiple retailer types: Further evidence and extension. Journal of the academy of marketing Science, 32(2), 176-187.

Aranda, J. (2020, 10 diciembre). Métodos de pago online en España - Comparativa [2020]. Palbin.com. https://www.palbin.com/es/blog/p1338-metodos-de-pago-online-en-espana.html

Boar, B. (1997). Boar, B. H. (1997). Strategic thinking for information technology: How to build the IT organization for the information age. Inc. New York, NY, USA: John Wiley & Sons.

Clone Phishing, Spear Phishing & Whaling | Types of Phishing. (s. f.). Cofense. https://cofense.com/project/phishing-vs-spear-phishing/

Concepto de seguridad — Definicion.de. (2021). Definición.de. https://definicion.de/seguridad/

Criptosistemas de clave pública. El cifrado RSA. (s. f.). dma.fi.upm.

http://www.dma.fi.upm.es/recursos/aplicaciones/matematica_discreta/web/aritmetica_modular/rsa.html

Datos101. (2021a, marzo 16). El año de la Ciberpandemia: 5 claves para entender la nueva amenaza digital. Datos 101. https://www.datos101.com/blog/ciberpandemia-la-nueva-amenaza-digital-2/

Dolz, P. O. (2020, 20 abril). Las estafas por Internet aumentan un 70% durante la cuarentena. El PaÃs. https://elpais.com/espana/2020-04-19/las-estafas-por-internet-aumentan-un-70-durante-la-cuarentena.html

Fonseca, D. S., Pérez, W. R., & Faurés, M. L. M. (2013). Pasarela de pagos para la seguridad de transacciones bancarias en línea.

Freeze, D. (2019, 30 diciembre). Top 5 Network Security Risks And Threats. Cybercrime Magazine. https://cybersecurityventures.com/top-5-network-security-risks-and-threats/

Freeze, D. (2020b, enero 19). Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021. Cybercrime Magazine. https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/

Fundamento de las bases de datos: Modelo entidad-relación. (2013, 5 noviembre). Genbeta. https://www.genbeta.com/desarrollo/fundamento-de-las-bases-de-datos-modelo-entidad-relacion

González, R. (2021, 31 marzo). Los ciberataques en España crecen un 125%. La pyme la gran perjudicada. Cinco Días. https://cincodias.elpais.com/cincodias/2021/03/25/pyme/1616706362_846686.html

González, R. (2021, Marzo 21). Los ciberataques en España crecen un 125%. La pyme la gran perjudicada. CincoDías. Retrieved from CincoDías.

INCIBE. (2016, 18 febrero). Comercio electrónico. https://www.incibe.es/protege-tu-empresa/sellos-confianza/comercio-electronico

INCIBE. (2019, 6 marzo). La importancia de separar la información pública de la interna. https://www.incibe.es/protege-tu-empresa/blog/segmentacion-dmz

INCIBE. (2021a, abril 12). Medidas de prevención contra ataques de denegación de servicio. https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

INCIBE. (2021b, abril 12). Medidas de prevención contra ataques de denegación de servicio. https://www.incibe.es/protege-tu-empresa/blog/medidas-prevencion-ataques-denegacion-servicio

INCIBE. (2021c, abril 29). Ciberamenazas contra entornos empresariales: una guía de aproximación. https://www.incibe.es/protege-tu-empresa/guias/ciberamenazas-entornos-empresariales-guia-aproximacion-el-empresario

INCIBE. (2021d, septiembre 28). Políticas de seguridad para la pyme. https://www.incibe.es/protege-tu-empresa/herramientas/politicas

INCIBE. (2022a, enero 25). Servicio Antibotnet. https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antibotnet

INCIBE. (2022b, mayo 24). Ayuda ransomware. https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware

INCIBE. (2022c, mayo 25). Aspectos clave para proteger tu tienda online. https://www.incibe.es/protege-tu-empresa/blog/aspectos-clave-proteger-tu-tienda-online

INCIBE. (2022d, mayo 27). Herramientas de ciberseguridad. https://www.incibe.es/protege-tu-empresa/herramientas

INE - Instituto Nacional de Estadística. (2020). Productos y Servicios / Publicaciones / Colección Cifras INE. https://www.ine.es/ss/Satellite?L=es_ES&c=INECifrasINE_C&cid=1259952923622&p=1254735116567&pagename=ProductosYServicios%2FINECifrasINE_C%2FPYSDetalleCifrasINE

Jara Jimenes, K. G. (2020). Análisis sobre las seguridades en las transacciones electrónicas dentro del comercio electrónico.

Jiménez Castillo, W. (2017). Seguridad informática o de la información en pymes. Bogotá: Universidad Piloto de Colombia.

La diferencia entre el modelo de datos conceptual y lógico. (2021, 14 septiembre). Talent Garden. https://talentgarden.org/es/data/the-difference-between-conceptual-and-logical-data-model/

Liberos, E. d. (2010). El libro del comercio electrónico. Esic Editorial.

Linder, J. a. (2000). Changing Business Models: Surveying the Landscape. Accenture Institute for Strategic Change.

Linder, J. and S. Cantrell, 2000. Changing Business Models: Surveying the Landscape, Accenture Institute for Strategic Change.

Malca, Ó. (2001). Comercio electrónico. Universidad del Pacífico.

Mekovec, R. & Hutinski, Z. (2012). The role of perceived security in online market. Proceedings of the 35th international convention MIPRO, (pp. 1549-1554).

Mesquita, R. (2021, 12 febrero). ¿Qué es un Sistema de Información y cuáles son sus características? Rock Content - ES. https://rockcontent.com/es/blog/que-es-un-sistema-de-informacion/

Miyazaki, A. D. (2001). Consumer perceptions of privacy and security risks for online shopping. Journal of Consumer affairs, 35(1), 27-44.

Modelado de datos conceptual. (2021). Erwin. https://www.erwin.com/mx-es/solutions/data-modeling/conceptual.aspx

Morse, E. A., & Raval, V. (2008). PCI DSS: Payment card industry data security standards in context. Computer Law & Security Review, 24(6), 540-554.

Nemat, R. (2011). Taking a look at different types of e-commerce. World Applied Programming, 1(2), 100-104.

¿Que es el 3D Secure? (2020, 21 julio). Moeni.. https://monei.com/es/blog/what-is-3d-secure-and-its-advantages-for-e-commerce/

Qué es la ingeniería social y cómo evitarla. (2020, 29 octubre). Avast. https://www.avast.com/es-es/c-social-engineering#gref

Ramírez, H. (2021, 13 octubre). MageCart: La principal ciberamenaza para los ecommerce. Grupo Atico34. https://protecciondatos-lopd.com/empresas/magecart/

Redacción CepymeNews. (2021, 27 julio). La realidad del ransomware ataca, ¿cómo podemos contratacar?CepymeNews. https://cepymenews.es/ransomware-ataca-como-podemos-contratacar/

Salam, A. F., Rao, H. R., & Pegels, C. C. (2003). Consumer-perceived risk in e-commerce transactions. Communications of the ACM, 46(12), 325-331.

Sarosa, S. a. (2003). Strategy for adopting information technology for SMEs: Experience in adopting email within an Indonesian furniture company. Electronic Journal of Information Systems Evaluation, 6(2): 165-176.

Serrahima, R. (2014). Pasarelas de pago: nuevos sistemas que impulsarán el comercio electrónico. Harvard Deusto Márketing y Ventas, (123), 42-46.

Somalo Peciña, Abad Falla, P. J., Haro, G. de, & Velasco Gómez, M. (2017). El comercio electrónico : una guía completa para gestionar la venta “online” / Ignacio Somalo Peciña ; [Pedro Abad, Guillermo de Haro Rodríguez, María Velasco Gómez] (1a ed.). ESIC.

Tipos de datos SQL para MySQL. (s. f.). Tecnologías información. https://www.tecnologias-informacion.com/tipos-sql.html

Universidad Politécnica de Catalunya. (s. f.). Sistemas de Información. Facultad de Informática de Barcelona. https://www.fib.upc.edu/es/estudios/grados/grado-en-ingenieria-informatica/plan-de-estudios/especialidades/sistemas-de-informacion

Von Solms, R. &. (2013). From information security to cyber security. computers & security, 38, 97-102.

Whitman, M. E., & Mattord, H. J. (2014). Principles of Information Security (5th Revised ed.). Cengage Learning

GLOSARIO DE TÉRMINOS

CMS: sistema de gestión de contenidos.

iFrame: elemento de HTML que permite incrustar un documento HTML dentro de un documento HTML principal.

PCI DSS: Estándar de seguridad de datos para la industria de Tarjeta de Pago.

Plugins: son pequeños programas que se instalan en un sitio web y les añade una funcionalidad de forma mucho más simple ya que vienen pre-programados y no es necesario que alteres el propio código de la web.

PSD2: en 2018, la Unión Europea iteró la Directiva para proveedores de Servicios de Pago (PSD), yendo más allá de los objetivos originales. La directiva PSD2 pretende impulsar la innovación en el sector de los pagos electrónicos, reforzar la seguridad mejorando la protección de los compradores y facilitando el desarrollo de nuevos métodos de pago.

3-D Secure: (3 domain structure) ayuda a prevenir el fraude digital en las transacciones con tarjetas de crédito y débito. También conocido como "payer authentication", este protocolo ofrece un nivel de protección extra, tanto para el titular de la tarjeta como para el recipiente del pago. Durante la compra online, en el momento de proceder al pago, 3D Secure incluye un nivel de seguridad adicional para evitar el fraude. Esta información adicional del cliente es recogida a través de una acción por su parte. Esta validación consiste en pedir información al comprador directamente a través de su dispositivo o por ejemplo con un código mandado por SMS, datos biométricos, app del banco, etc. Este protocolo de seguridad protege de los chargebacks o retrocesos fraudulentos, ya que la responsabilidad de estos chargebacks recae sobre el banco emisor de la tarjeta.