Ciberseguridad en el comercio electrónico

Guía de recomendaciones para empresas

Financiado por la Unión Europea NextGenerationEU
Gobierno de España · Ministerio de Transformación Digital · Secretaría de Estado de Digitalización e Inteligencia Artificial
Plan de Recuperación, Transformación y Resiliencia
España | digital 2026
incibe_ Instituto Nacional de Ciberseguridad
protege tu empresa

Índice

1. Introducción

El objetivo de la «Ciberseguridad en el comercio electrónico: una guía de aproximación para el empresario» es describir los pasos a seguir para dotar a una tienda virtual de un nivel de ciberseguridad aceptable tanto para el propietario como para el cliente. El propietario de la tienda debe establecer unos requisitos de seguridad para que sus clientes tengan una experiencia digital segura.

El comercio electrónico está expuesto a múltiples amenazas, que llegan a través de Internet mediante distintas técnicas. En esta guía se describen las principales ciberamenazas y recomendaciones que hay que aplicar para reducir el riesgo de que se produzcan. Además, se describen una serie de puntos con los que se puede identificar una transacción como fraudulenta, así como la manera de actuar cuando se ha producido un fraude en la tienda virtual. Por último, se describe cómo se puede aumentar la confianza de los clientes en la tienda virtual.

Esta guía se dirige al empresario para que, independientemente de los conocimientos técnicos y de quién gestione la tienda virtual, conozca las pautas básicas a considerar en materia de ciberseguridad en su portal.

Para una mejor compresión de esta guía, se recomienda tener al menos conocimientos básicos en materia de ciberseguridad.

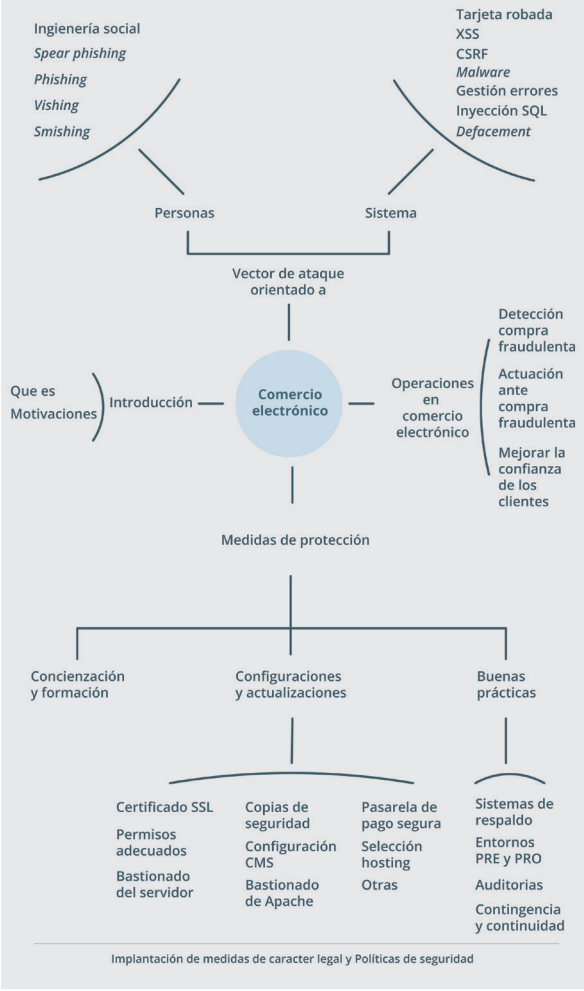


Ilustración 1. Diagrama completo

A continuación, se muestra un diagrama para identificar y visualizar los apartados dentro de la guía y situarlos en el contexto al que hacen referencia. El diagrama se encuentra dividido en cuatro zonas:

- En la zona izquierda se hace una pequeña descripción de qué es el comercio electrónico y de cuáles son las principales motivaciones de los ciberdelincuentes.
- En la zona superior se describen las principales formas de ataque contra una empresa de comercio electrónico.
- En la zona inferior se indican las principales medidas de protección contra las diferentes formas de ataque que tienen los ciberdelincuentes.
- En la zona derecha se hace referencia a la manera de actuar cuando las medidas de protección han fallado y cómo aumentar la confianza de los clientes en la tienda virtual.

2. Introducción sobre el comercio electrónico

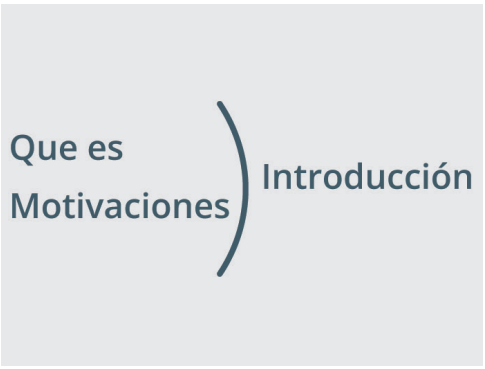


Ilustración 1. Introducción

La evolución de la tecnología y, en particular, la irrupción de Internet, provocaron un gran cambio de paradigma en la sociedad. Ahora, la información se procesa, almacena y transmite sin restricciones de distancia, tiempo o volumen.

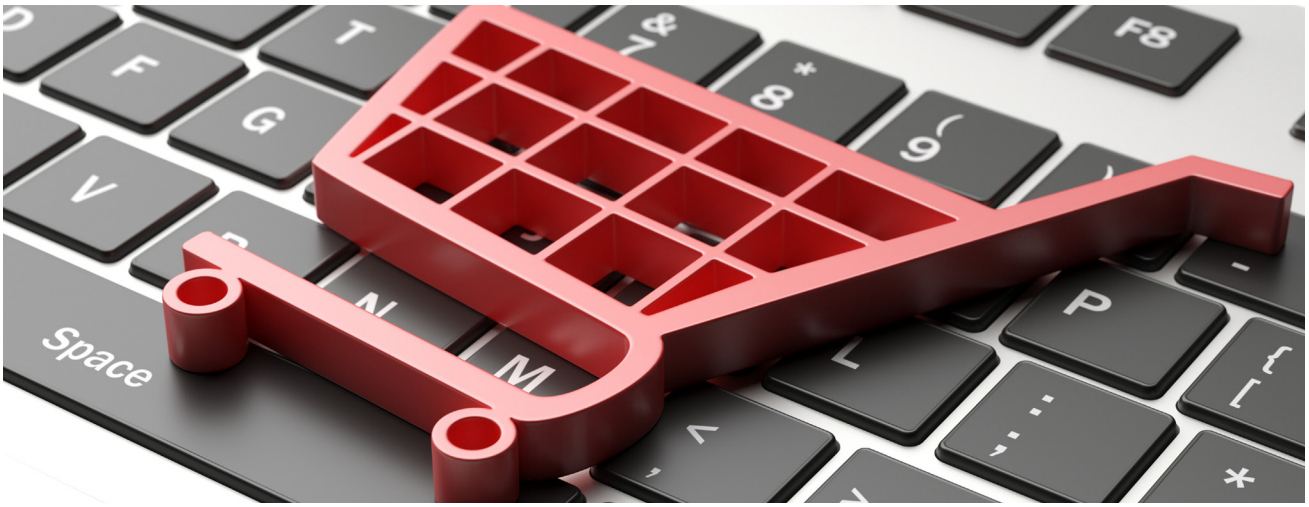
Este nuevo entorno tiene una gran trascendencia tanto para las empresas, como para la ciudadanía. Los mercados se han transformado en globales y digitales en poco tiempo.

La globalización, el aumento de capacidad y velocidad de las transacciones y la movilidad, provocados por la rápida evolución de la tecnología, han dejado obsoleta la forma de entender los negocios. Las antiguas reglas, las leyes y las normas se quedan escasas y es necesario reformularlas.

En este entorno la seguridad cobra un sentido especial. Todas las propiedades del mercado digital (velocidad, capacidad, movilidad...) son aprovechadas y explotadas por aquellos que pretenden obtener beneficio de manera fraudulenta, los denominados cibercriminales o ciberdelincuentes.

La pandemia del COVID-19 ha acelerado de manera sin precedentes la transformación digital y el comercio electrónico. Con el cierre de tiendas físicas y las restricciones de movimiento, consumidores y empresas se han volcado hacia las plataformas digitales para continuar con sus operaciones habituales.

Sin embargo, este cambio repentino y masivo hacia la digitalización ha traído consigo una ola de oportunidades para los actores malintencionados, intensificando la actividad de los cibercriminales que buscan explotar las vulnerabilidades que surgen en un entorno en constante evolución. El comercio en línea, fortalecido por la demanda de servicios a domicilio y la gestión remota de transacciones comerciales, ha expuesto a las empresas a un rango amplio de amenazas cibernéticas. En un contexto globalizado, la ciberseguridad es un elemento clave para el desarrollo económico. La protección frente a las amenazas (introducción de código dañino en sistemas, ataques a páginas web para robar información, cometer fraude electrónico y robo de identidad online...) y el fomento de la seguridad constituyen factores esenciales para el desarrollo de la economía de Internet. El gran pilar del desarrollo de la economía digital se apoya en el comercio electrónico, también conocido como e-commerce. La compraventa de productos utilizando medios telemáticos permite llegar a un número mayor de posibles clientes gracias a la disponibilidad 24/7. El comercio electrónico ha aumentado considerablemente en los últimos años y se espera que siga creciendo en los próximos. Por tanto, las empresas deben adaptarse y evolucionar hacia este mercado digital, teniendo como uno de sus principios rectores la ciberseguridad.



La protección de los datos, la privacidad y la integridad de la información se han convertido en prioridades tanto para las organizaciones como para los consumidores. Establecer medidas de seguridad robustas es fundamental para proteger los intereses de los propietarios de negocios y la confianza de sus clientes.

Para comprender mejor las formas de ataque usadas por los atacantes es necesario conocer cuáles son sus motivaciones.

Los ciberdelincuentes tienen como principal objetivo el beneficio económico. Para ello, utilizan diferentes vectores de ataque, como veremos en el siguiente apartado. Para conseguir su objetivo pueden robar distinta información confidencial, como es la cartera de clientes de una organización, o información bancaria, como el número de tarjeta, entre otros datos. Una vez que los ciberatacantes obtienen la información que quieren, pueden utilizarla para otros ataques o venderla en el mercado negro.

Pero también pueden existir otros dos objetivos:

- Dañar la imagen corporativa: para ello, pueden utilizar técnicas como la modificación de la página web de la organización cambiándola por otra degradante para la imagen de la empresa o una imagen reivindicativa. Este tipo de ataques contra la imagen corporativa causan, además del daño económico por pérdida de confianza de los clientes, el deterioro de su imagen de marca.

- Aprovechar los recursos tecnológicos de la empresa para atacar a terceros: se utilizan los recursos tecnológicos de la empresa para poder obtener un beneficio económico de un tercero. Si nuestra web no es segura, pueden utilizarla para poder distribuir malware, alojar un phishing o infectar nuestro servidor web para utilizar su capacidad de red, entre otros tipos de acciones maliciosas.

3. Ciberamenzas

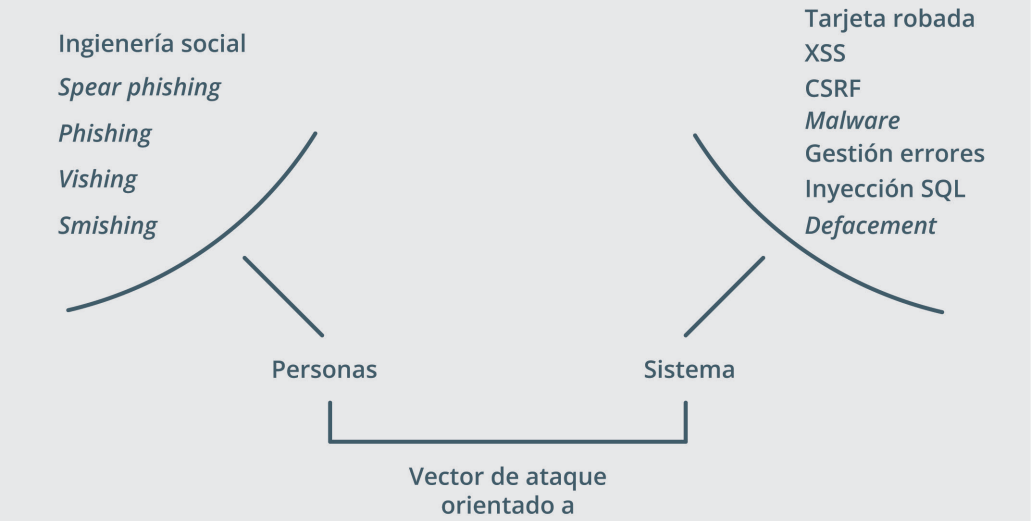


Ilustración 3. Ciberamenazas

Ninguna empresa puede pasar por alto las ciberamenazas, ya que provocan no solo pérdidas económicas o perjuicio directo en caso de un incidente, sino que pueden conllevar una degradación considerable de la imagen corporativa y, por tanto, de la confianza de los clientes.

Las amenazas cibernéticas a las que las tiendas virtuales están expuestas no difieren mucho de algunas amenazas «tradicionales» de un entorno offline. Existen muchas maneras en que los ciberdelincuentes pueden vulnerar un sistema. Por este motivo, es conveniente tener una visión global de los principales vectores de ataque a los que una tienda virtual está sometida.

Los ciberdelincuentes tienen principalmente dos formas de atacar a la tienda virtual y la información relacionada con ella, como, por ejemplo, la cartera de clientes y los proveedores. Podrán acceder por medio de las personas que trabajan en la empresa o por medio de vulnerabilidades propias de la tienda virtual, como es el gestor de contenidos o el servidor web.

A continuación, se describirán las principales ciberamenazas que utilizan los ciberdelincuentes, diferenciando si el vector de ataque son las personas o el sistema.

3.1 Ataques dirigidos contra las personas

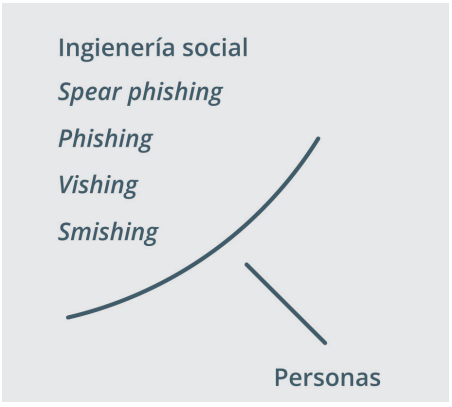


Ilustración 4. Ciberamenazas contra personas

Este tipo de ciberataque busca engañar a las personas y que los ciberdelincuentes obtengan cualquier clase de beneficio, principalmente información confidencial. La ingeniería social es una técnica que emplean los ciberdelincuentes para ganarse la confianza del usuario y conseguir así que haga algo bajo su manipulación y engaño, como puede ser ejecutar un programa malicioso, facilitar sus claves privadas o comprar en sitios web fraudulentos.

Con la evolución de la tecnología y de las medidas técnicas de seguridad ha quedado patente que el eslabón más débil dentro de la cadena de seguridad es la persona que tiene acceso de una u otra forma a la información. La seguridad de la información no se garantiza únicamente con la instalación de antivirus, el uso de contraseñas robustas o el cifrado de la información confidencial.

En el siguiente ejemplo la ingeniería social, en combinación con otras técnicas, juega un papel importante, apelando a la curiosidad de las personas y la falta de precaución:

El ser humano es curioso por naturaleza. Si aparece «olvidada» una llave USB junto a la cafetera de la sala de descanso de la empresa o en la entrada de la oficina, ¿cuánto tiempo pasará antes de que alguien la pinche en su puesto de trabajo? ¿Qué pasará si esa persona ve que el USB contiene un fichero con el nombre nominafeb2023.xls? Muchas personas caerían en la tentación de saber lo que cobra su compañero de departamento. Con esos aspectos propios del ser humano juega la ingeniería social. Los ciberdelincuentes saben que si dejan un USB, en cuestión de horas podrán utilizar el malware del mismo para conseguir un acceso directo a la organización.

Una consecuencia que puede tener la técnica anterior en una empresa de comercio electrónico es que el atacante acceda a información confidencial de la propia organización y de sus clientes. También puede obtener las credenciales de acceso al gestor de contenidos o CMS. Además, esta llave USB podría contener otros tipos de malware que podrían realizar cualquier otra acción maliciosa, como cifrar todo el contenido del ordenador y los demás dispositivos conectados a la red o dar el control remoto de la máquina al ciberdelincuente.

Este tipo de técnicas pueden ser realmente efectivas y peligrosas para una empresa. La información que manejan suele ser un bien muy preciado y, si esta información cae en manos de los cibercriminales, puede suponer graves perjuicios.

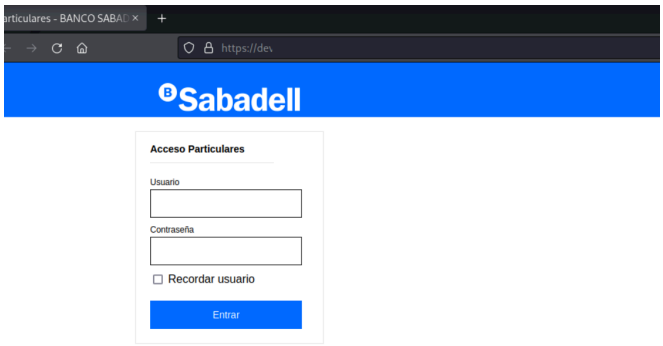
La ingeniería social es uno de los vectores de ataque más peligrosos y que más se está utilizando para acceder a las redes de las organizaciones, haciendo uso de los empleados de las propias organizaciones para vulnerar sus medidas de defensa. Las principales amenazas a las que los empleados de la empresa están expuestos son las siguientes:

3.1.1 *Phishing*

El phishing es un tipo de ataque cibernético que utiliza el engaño para extraer información confidencial, como datos de acceso o financieros de sus víctimas. Generalmente, se lleva a cabo a través de comunicaciones que aparentan ser de fuentes fiables, como empresas legítimas o contactos conocidos. Los atacantes emplean correos electrónicos donde incitan a los destinatarios a revelar información personal, hacer clic en enlaces maliciosos o descargar archivos que pueden contener malware.

Del mismo modo que pueden existir variantes de phishing altamente personalizadas, pueden darse campañas masivas sin un objetivo particular. Este tipo de ataques busca aprovecharse de la falta de conocimiento o la distracción de los usuarios para que actúen impulsivamente, a menudo creando un sentido de urgencia.

En una táctica común de phishing un atacante podría enviar un correo electrónico simulando ser un banco o un servicio de pago en línea, alertando al destinatario sobre un problema con su cuenta y solicitando que confirmen sus credenciales a través de un enlace proporcionado en el mensaje.



Este enlace dirige a una página web falsa, que parece legítima, pero está diseñada para recopilar las credenciales ingresadas por el usuario desprevenido.

El phishing representa una amenaza significativa para la seguridad en línea de individuos y organizaciones y requiere una vigilancia constante, así como medidas preventivas, tales como la verificación de la autenticidad de los mensajes recibidos o el uso de software de seguridad actualizado.

3.1.1.1 *Spear Phishing*

El spear phishing consiste en realizar ataques dirigidos, que se centran en una persona, grupo u organización en concreto. Generalmente, el ataque se realiza por medio de correos electrónicos, utilizando datos personales y conocidos de la víctima. Esto permite personalizar el mensaje y hacer que la víctima se sienta más confiada. Para realizar este tipo de ataque el atacante se basa en información obtenida en redes sociales, blogs personales y cualquier información personal que esté publicada en Internet.

El ciberdelincuente busca infectar a una víctima determinada. Esta víctima es el responsable de una tienda de comercio electrónico y se conecta al área de administración del gestor de contenidos desde su puesto de trabajo. El objetivo de los ciberdelincuentes es obtener las claves de acceso al área de administración de la tienda virtual. Para conseguir su objetivo el atacante ha recabado información personal de la víctima por medio de las redes sociales. Después de cierta indagación, descubre que la víctima y su familia son unos apasionados del esquí, además de que su hijo pertenece a una escuela de esquí. Con estos datos el ciberdelincuente prepara su engaño.

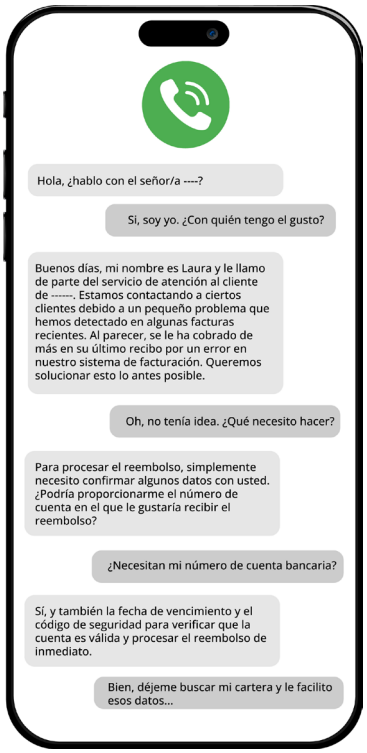
Ilustración 6. Spear Phishing

Una vez que la víctima descargue el documento PDF adjunto y lo ejecute -intentar abrirlo es el modo más habitual, aunque realmente ejecuta instrucciones introducidas en él-, instalará en su equipo un malware con el que el ciberdelincuente podrá ver las credenciales de acceso al gestor de contenido y desde allí modificar la tienda virtual para así afectar de manera negativa a su imagen corporativa.

3.1.1.2 *Vishing*

El vishing es una variante que utiliza el engaño a través de llamadas telefónicas para obtener información confidencial de las víctimas. En lugar de emplear correos electrónicos o mensajes de texto, los ciberdelincuentes realizan llamadas directas a sus objetivos, presentándose como representantes legítimos de instituciones reconocidas, como bancos o compañías de seguros. Durante estas llamadas, los atacantes manipulan a sus interlocutores para que divulguen información sensible, como números de la Seguridad Social, datos bancarios o contraseñas.

A diferencia del phishing general, que puede dirigirse a un amplio espectro de destinatarios a la vez, el vishing se basa en la interacción verbal, lo que a menudo puede dar una falsa sensación de legitimidad y urgencia. Se trata de crear un escenario alarmante que requiera una respuesta inmediata, aprovechando el factor humano y la tendencia a responder con inmediatez a lo que aparenta ser una llamada importante.



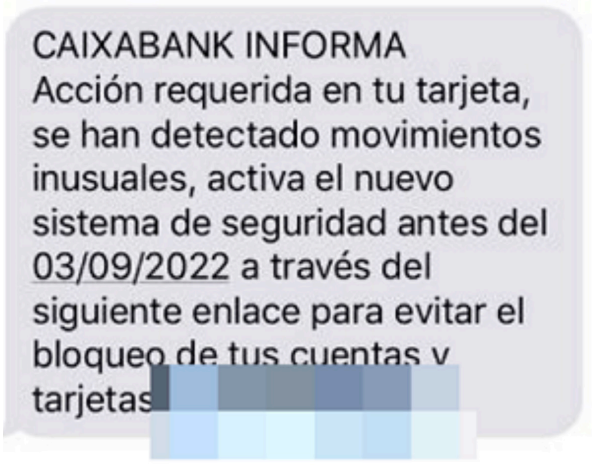
El vishing es una amenaza significativa que se aprovecha de la accesibilidad y la presencia constante de los teléfonos en la vida cotidiana. Para contrarrestar este riesgo, es recomendable usar métodos para verificar la identidad de quien nos llama y nunca proporcionar información personal o financiera, a menos que sea posible verificar completamente la identidad y la legitimidad de la solicitud.

3.1.1.3 *Smishing*

El smishing es una forma de actividad fraudulenta que se asemeja al phishing, pero se realiza a través de mensajes de texto SMS en dispositivos móviles. Este tipo de ataque busca engañar a los destinatarios para que proporcionen información personal, financiera o de seguridad, a través de mensajes que parecen ser de fuentes legítimas, como bancos, autoridades o incluso contactos personales.

Los atacantes utilizan mensajes de texto SMS que pueden contener enlaces a sitios web falsos o solicitudes para que las víctimas respondan con información privada. Al igual que en el spear phishing, el smishing puede emplear información específica sobre la víctima para aumentar la credibilidad del mensaje. Sin embargo, a diferencia del spear phishing, que se dirige a objetivos específicos con información personalizada, el smishing a menudo se realiza en una escala más amplia, buscando engañar a tantos destinatarios como sea posible, con la esperanza de que alguno caiga en la trampa.

Un ejemplo de este tipo de amenaza podría ser un mensaje de alerta a una víctima sobre una supuesta actividad sospechosa en su cuenta bancaria y pedirle que haga clic en un enlace para verificar su identidad, lo cual lleva a un sitio web falso diseñado para robar sus credenciales.



La efectividad del smishing se basa en la percepción de inmediatez y la tendencia de las personas a responder rápidamente a los mensajes de texto, especialmente cuando parecen urgentes. Además, resulta particularmente peligroso debido a la naturaleza personal de los dispositivos móviles; por tanto, requiere que los usuarios sean cautelosos con los mensajes no solicitados y verifiquen siempre la fuente antes de hacer clic en enlaces o compartir información.

3.2 Ataques dirigidos contra el sistema

En este tipo de amenazas el ciberdelincuente busca explotar vulnerabilidades relacionadas con el software que da soporte a la tienda virtual, como podría ser el gestor de contenidos o el servidor web donde está alojada la tienda.

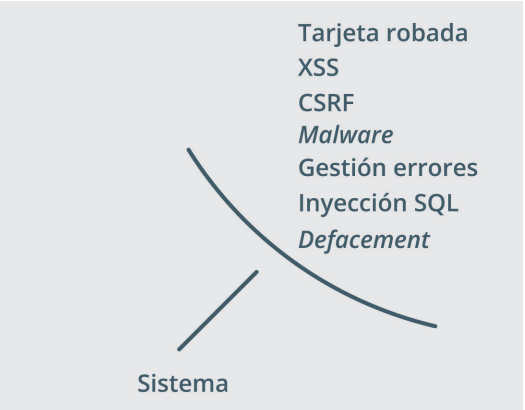


Ilustración 7. Ciberamenazas contra el sistema

Este tipo de vulnerabilidades se debe normalmente a malas configuraciones o falta de actualizaciones por parte del software que conforma la tienda virtual. A continuación, se describirán las principales vulnerabilidades que los cibercriminales explotan en su beneficio:

- **Pago con tarjeta robada:** este tipo de fraude consiste en que un ciberdelincuente utiliza el número de una tarjeta, bien obtenido de la tarjeta física o robando la misma, para realizar compras en la tienda virtual.
- ***Malware:*** Palabra que nace de la unión de los términos software malintencionado (malicious software). Dentro de esta definición tiene cabida un amplio elenco de programas maliciosos: virus, gusanos, troyanos, backdoors, spyware, etc. La nota común a todos estos programas es su carácter dañino o lesivo. Los ciberdelincuentes en ocasiones utilizan servidores o páginas web vulneradas para distribuir malware sin que el propietario tenga conocimiento de ello.
    - **Ransomware:** es un tipo de malware que restringe el acceso a los datos o archivos de un sistema, generalmente cifrando los archivos, y exige un rescate económico para que el atacante nos proporcione la clave de descifrado. Su nombre proviene de la palabra ransom (rescate, en inglés) y software, ya que el propósito del ransomware es monetizar el ataque cobrando por la recuperación del acceso a los recursos secuestrados. La eficacia del ransomware se debe a la dificultad de rastrear y procesar judicialmente a los atacantes, que suelen operar a través de redes internacionales.
- ***Cross-Site Scripting* (XSS)**: en un ataque por XSS una aplicación web envía un script que se activa cuando lo lee el navegador de un usuario o una aplicación vulnerable. Dado que los sitios dinámicos dependen de la interacción del usuario, es posible ingresar un script malicioso en la página, ocultándolo entre solicitudes legítimas. Los puntos de entrada comunes incluyen buscadores, foros, blogs y todo tipo de formularios en línea en general. Una vez iniciado el XSS, el atacante puede cambiar configuraciones de usuarios, secuestrar cuentas, envenenar cookies, exponer conexiones SSL, acceder a sitios restringidos e instalar publicidad en el sitio víctima.

- **Ataques de inyección SQL**: es un método de infiltración de código intruso que se sirve de una vulnerabilidad presente en una aplicación en el nivel de validación de entradas para la realización de consultas a una base de datos. El origen de la vulnerabilidad radica en la incorrecta validación de las variables utilizadas en un programa que contiene o genera código SQL.

- ***Cross-Site Request Forgery* (CSRF)**: este tipo de ataque obliga a un usuario legítimo a ejecutar acciones no deseadas en una aplicación web en la que actualmente está autenticado. Los ataques CSRF se dirigen específicamente a las peticiones de cambio de estado, no el robo de datos, ya que el atacante no tiene manera de ver la respuesta a la solicitud. Con la ayuda de ingeniería social, como el envío de un enlace por correo electrónico, un atacante puede engañar al usuario de una aplicación web para que realice ejecuciones a elección del atacante. Si la víctima es un usuario normal, un ataque exitoso CSRF puede obligar al usuario a realizar solicitudes fraudulentas, como la transferencia de fondos, el cambio de su dirección de correo electrónico y así sucesivamente. Si la víctima es un administrador, CSRF puede comprometer toda la aplicación web.

- **Ataque distribuido de denegación de servicio (DDoS)**: con este tipo de ataques los ciberdelincuentes intentan sobrecargar un sitio web con tráfico malintencionado, provocando una interrupción en el acceso o una bajada de rendimiento para los usuarios legítimos. Para ello, los ciberdelincuentes toman el control de una red de dispositivos comprometidos previamente, conocidos como botnets. A través de estas redes zombis, se dirige un gran volumen de tráfico falso hacia el servidor en línea de la tienda, saturándolo al no poder manejar todas las solicitudes, dando como resultado la inaccesibilidad de la web para los usuarios legítimos. Como consecuencia, durante la inactividad debida al ataque, el negocio sufrirá pérdidas de ingresos de aquellas compras que los clientes no puedan realizar. Además, esta situación puede suponer un daño reputacional y afectar a la imagen de la empresa.

- **Ataques de fuerza bruta**: son una táctica para obtener acceso no autorizado a cuentas de usuario mediante la repetición sistemática de diversas combinaciones de contraseñas o códigos de acceso hasta que se encuentra la correcta. Para aumentar la eficiencia de estos ataques, los atacantes suelen emplear colecciones de palabras de uso común, frases, patrones de teclado comunes y contraseñas previamente filtradas que se prueban contra las cuentas objetivo. Estos diccionarios se han enriquecido con la acumulación de bases de datos de contraseñas expuestas en brechas de seguridad anteriores. Además, los atacantes pueden utilizar programas automatizados que ejecutan rápidamente miles o millones de intentos de combinaciones de contraseñas en un corto período de tiempo. Estos ataques pueden ser particularmente exitosos contra sistemas que no implementan medidas de seguridad adecuadas, como el bloqueo de cuenta después de un número determinado de intentos fallidos, requerimientos de autenticación multifactorial o sistemas captcha.

- **Ataques de suplantación de identidad (pharming)**: supone la redirección del tráfico de un sitio web legítimo a un sitio web falso sin que lo sepa el usuario. Esto puede hacer que los usuarios introduzcan información confidencial en un sitio web fraudulento sin darse cuenta.

- **Ataques a la capa de transporte (TLS/SSL):** si la tienda virtual no utiliza cifrado SSL/TLS adecuado, un intruso podría interceptar las comunicaciones entre los usuarios y el servidor, consiguiendo este acceso a información confidencial de cualquier tipo.

Vulnerabilidades de aplicaciones web: las tiendas virtuales suelen depender de aplicaciones web complejas. Si estas aplicaciones tienen vulnerabilidades de seguridad, un usuario malintencionado podría explotarlas para acceder a la tienda o robar información.

Robo de sesiones: el robo de sesiones, también conocido como session hijacking, es una modalidad de ataque en la que un ciberdelincuente toma el control de una sesión web entre dos partes, normalmente entre un usuario legítimo y el servidor de una aplicación web. Este tipo de ataque se lleva a cabo después de que el usuario haya hecho login, lo que significa que el atacante evita tener que robar la contraseña del usuario; en su lugar, se apodera de la sesión ya autenticada para realizar acciones no autorizadas.

Ataques a bases de datos: el acceso no autorizado a bases de datos es un tipo de violación que compromete la información almacenada. Durante un ataque de este tipo, los ciberdelincuentes pueden extraer, modificar o destruir datos críticos, incluyendo información personal y financiera de los clientes, registros comerciales confidenciales y propiedad intelectual. La consecuencia de tal acceso indebido va más allá de la pérdida de datos y puede incluir daños reputacionales graves para la empresa afectada, pérdida de confianza por parte de los clientes y posibles sanciones legales y financieras, debido al incumplimiento de las leyes de protección de datos.

Gestión incorrecta de errores: controlar la información que facilitan las páginas de errores es importante, ya que pueden dar información sensible sobre cómo está construida la aplicación web y del software usado para su funcionamiento.

3.3 Ataques contra el sistema o las personas

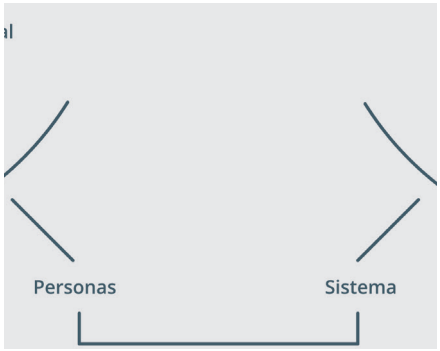


Ilustración 8. Ciberamenazas contra el sistema y personas

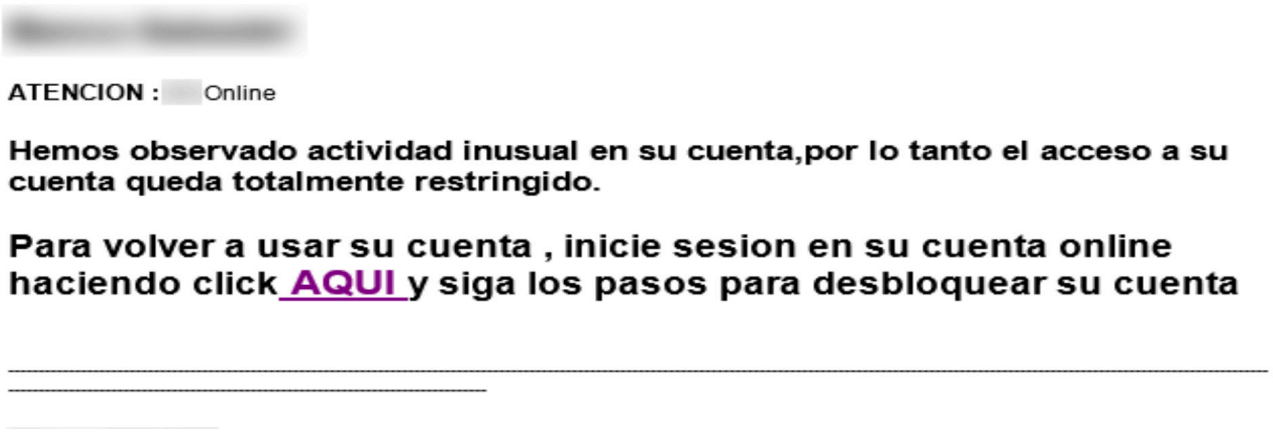
Este tipo de ciberamenazas combinan las dos vías de entrada descritas anteriormente. Los ciberdelincuentes ponen en riesgo los portales de comercio electrónico, valiéndose tanto de ataques contra el sistema como de ataques contra las personas. En función de la vía de entrada elegida, el ataque tendrá unas consecuencias u otras, como se explicará a continuación.

3.3.1 *Phishing*

Phishing es la denominación que recibe la estafa cometida a través de medios telemáticos mediante la cual el estafador intenta conseguir, de usuarios legítimos, información confidencial (contraseñas, datos bancarios, etc.) de forma fraudulenta. Una vez que los cibercriminales obtienen la información la usarán para cometer cualquier tipo de fraude. El phishing, como la mayoría de los ataques, se realiza utilizando técnicas de ingeniería social, persuadiendo al usuario para que realice una acción que será perjudicial para la víctima.

Phishing realizado contra los miembros de la organización

El phishing realizado contra los miembros de la organización es común que se realice por medio del envío masivo de correos electrónicos. Estos correos masivos suelen incluir enlaces a páginas web falsas, propiedad del estafador. Estas páginas webs falsas pedirán información confidencial a la víctima alegando que se está realizando cualquier tipo de mantenimiento o que se ha realizado un cargo en su cuenta, entre otros tipos de engaños. El phishing también puede realizarse utilizando otros medios, como una llamada telefónica (vishing), mensajes de texto o SMS (smishing), redes sociales, mensajería instantánea, etc.


ATENCION : Online

Hemos observado actividad inusual en su cuenta,por lo tanto el acceso a su cuenta queda totalmente restringido.

Para volver a usar su cuenta , inicie sesion en su cuenta online haciendo click AQUI y siga los pasos para desbloquear su cuenta

Ilustración 9. Phishing

este ejemplo de un phishing por correo electrónico realizado a un conocido banco se pide al usuario que haga clic en el enlace adjunto, alegando que se ha producido una actividad inusual en la cuenta y que la han bloqueado.

Una vez que la víctima cae en el engaño y hace clic en el enlace adjunto, esta será redirigida a una página web fraudulenta con la misma estética que la página web original. En esta web fraudulenta se le pedirá que se autentifique por medio de su DNI (documento nacional de identidad) y clave de acceso. Después, se le pedirá que introduzca los datos de su tarjeta de crédito. Cuando haya terminado de introducir los datos, la víctima será redirigida a la web oficial del banco, por lo que esta no será consciente de que le han robado información confidencial.

3.3.2 *Defacement*

El objetivo de este tipo de ataque, independientemente de la forma en que es llevado a cabo, es modificar una página web total o parcialmente. Para ello, deben acceder al gestor de contenidos o el servidor web de la organización por medio de alguna vía de entrada. Este tipo de ataque se realiza generalmente por dos métodos:

comprometiendo el gestor de contenidos o a través de una vulnerabilidad en el servidor web.

En la mayoría de las ocasiones suelen modificar textos o incluir imágenes llamativas en la página principal de la web víctima. Las motivaciones pueden ser varias, pero el principal denominador común es que tienen carácter reivindicativo (político, sociocultural, publicidad de un grupo de ciberdelincuentes...), además de dañar la imagen corporativa de la entidad. En algunos casos un cibercriminal realiza este tipo de ataque por motivos económicos.

El ***defacement*** también puede usarse como una distracción para ocultar actividades más maliciosas que ocurren en segundo plano, como la extracción de datos confidenciales, la creación de puertas traseras para acceso futuro o el despliegue de malware adicional.

4. Medidas de protección

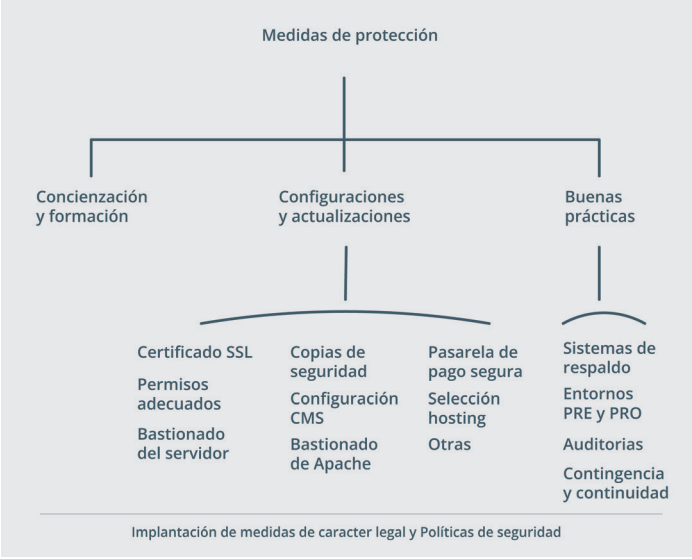


Ilustración 10. Medidas de protección

Cuando se crea una tienda virtual es necesario adoptar una serie de medidas de protección específicas contra el fraude. Como responsables del servicio, es necesario implementar todos los mecanismos de seguridad posibles que detecten y eviten el fraude y facilitar a los clientes herramientas que mantengan su seguridad en su trato con nosotros.

Para conseguir un nivel de ciberseguridad aceptable, es necesario tomar medidas en áreas distintas, como se describirá a continuación.

4.1 Concienciación y formación

El empleado es el gran protagonista de la seguridad en las empresas. La tecnología es importante, pero no siempre es suficiente para proteger nuestros sistemas de información. La implicación y participación de todos los empleados, incluidos los de más nivel en la jerarquía de la empresa, es esencial para llevar una gestión adecuada de la ciberseguridad en la empresa. Por este motivo, concienciar y formar a los miembros de la organización se convierte en una pieza clave del puzle de la seguridad en la empresa.

Ilustración 11. Personas

En algunas organizaciones todavía no existe un plan de concienciación, ya sea por falta de recursos o por desconocimiento. Para solucionar este problema, se hace imprescindible la puesta en marcha de un plan de concienciación y formación para los miembros de la organización. El plan de concienciación tiene como objetivo crear y catalizar una cultura de seguridad dentro de la organización. De este modo, se reducen los riesgos globales a los que se enfrenta una organización.

Desde INCIBE se ha diseñado y puesto a disposición de todas las organizaciones un **kit de concienciación** que permite mejorar de manera integral el nivel de ciberseguridad en las empresas. El programa de concienciación incorpora múltiples recursos gráficos, elementos interactivos y una programación detallada. Todo ello para mejorar la ciberseguridad desde el propio corazón de la organización: las personas.

El kit de concienciación tiene como propósito facilitar al empresario el diseño y puesta en marcha de un plan de formación integral en materia de seguridad de la información para todos los empleados, proporcionando a los empresarios un mecanismo útil para formar y concienciar a sus empleados en ciberseguridad. El kit ha sido elaborado para que el empresario pueda descargárselo y entregarlo a sus empleados de una manera secuencial, de acuerdo con un programa o planificación, que también se le facilita. Para ello, el programa incorpora materiales de seguimiento y despliegue, compuesto por materiales gráficos, documentación, cuestionarios, etc.

4.2 Configuraciones y actualizaciones

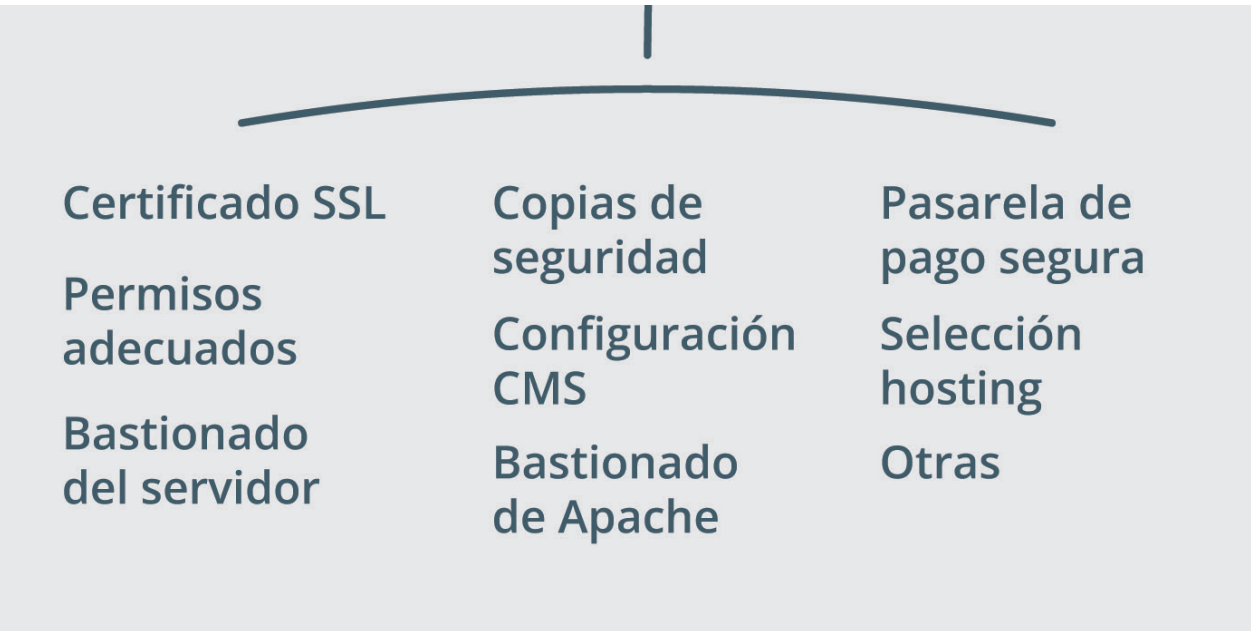


Ilustración 12. Configuraciones y actualizaciones

Una tienda virtual está formada por varios elementos, tanto software como hardware, que trabajando en conjunto hacen que la tienda cumpla sus funciones como mecanismo de comercio.

Para que la tienda virtual realice sus funciones de manera correcta es necesario adoptar una serie de medidas de seguridad. Las medidas de seguridad dotarán a la tienda de un nivel de seguridad aceptable tanto para el empresario como para sus clientes. A continuación, se explican algunas de las medidas de seguridad para tiendas virtuales.

4.2.1 Certificado SSL/TLS

Un certificado SSL (Secure Socket Layer) es un protocolo de seguridad que garantiza la privacidad y la integridad de la información transmitida entre un sitio web y el navegador del usuario. De esta forma, se consigue una navegación segura y encriptada que protege los datos confidenciales, como tarjetas de crédito, contraseñas y datos personales.

TLS (Transport Layer Security) consiste en un certificado más seguro basado en SSL, siendo totalmente compatibles. Disponer de un certificado SSL/TLS instalado proporciona una serie de ventajas:

- Permite identificar del sitio web de forma inequívoca.
- La información transmitida entre el navegador del cliente y el servidor donde está alojada la tienda virtual viaja cifrada, por lo que es ilegible si es interceptada.
- La información se transmite de forma íntegra y, si se produce una modificación o pérdida de información, esta se podrá identificar y descartar.

Para que el navegador que usa el cliente reconozca el certificado es necesario que lo proporcione una autoridad de certificación reconocida. Estas autoridades garantizan la legitimidad del certificado por medio de controles de seguridad y verificaciones. Si el certificado no está emitido por una autoridad de certificación, el navegador web del cliente le avisará de que está intentando acceder a un sitio web, cuya legitimidad no se ha podido verificar. Existen principalmente tres tipos de certificados:

- **Certificados autofirmados**: este tipo de certificados no han sido emitidos por una autoridad certificadora de confianza, por lo que, aunque la dirección comience por "https", el navegador web del cliente no podrá reconocer la legitimidad del sitio web, avisando al usuario de que está entrando en un sitio web no confiable. Instalar este tipo de certificados no es recomendable para tiendas virtuales en producción.

- **Certificados sin validación extendida**: este tipo de certificados son emitidos por una autoridad de certificación reconocida, por lo que el navegador web del cliente no lanzará ninguna alerta. Cuando se conecta un cliente a una web con este tipo de certificado la dirección comienza con "https" y a su lado se encuentra un candado.

- **Certificados con validación extendida**: este tipo de certificados, como el anterior, son emitidos por una autoridad certificadora reconocida y, al igual que el anterior, el navegador web del cliente no lanzará ninguna alerta al usuario. Los certificados con validación extendida otorgan las máximas garantías de conexión, lo que aumenta la confianza de los usuarios. Cuando un cliente se conecta a una página web con un certificado SSL de validación extendida, además de ver que la dirección comienza por "https" y que hay un candado a su lado, también verá una barra verde que identifica a la organización a la que pertenece.

El uso de certificados SSL se ha convertido en un estándar de seguridad esencial para todas las páginas web, no solo para aquellas que manejan información sensible, como contraseñas o datos de tarjetas de crédito. Desde hace años, los navegadores líderes en el mercado han empezado a adoptar políticas más estrictas respecto a la seguridad en línea. En este contexto, los navegadores modernos están diseñados para proporcionar a los usuarios información clara sobre la seguridad de los sitios web que visitan. Por ejemplo, cuando un sitio web no tiene un certificado SSL/TLS, los navegadores pueden marcarlo como "No seguro" o mostrar un candado abierto, lo que indica que la conexión no es privada y que la información enviada o recibida a través de ese sitio podría ser interceptada por terceros.

4.2.2 Copias de seguridad

También conocido como backup, es una copia de los datos originales que se realiza con el fin de disponer de un sistema de respaldo en caso de pérdida, deterioro o robo de información. Dependiendo del tamaño de la empresa, los soportes en los que se realizará la copia, la frecuencia y los procedimientos para realizarla serán distintos. Realizar copias de seguridad es importante para cualquier empresa y las tiendas de comercio electrónico no son una excepción. Un sistema de copias de seguridad puede hacer que una tienda que se ha visto afectada por un fallo de seguridad pueda recuperar su actividad diaria.

Por ejemplo, una empresa ha sido atacada por un cibercriminal y ha conseguido ejecutar un malware de tipo ransomware. Este malware cifrará una gran cantidad de información perteneciente a la empresa, pero, al disponer de copias de seguridad, se puede restaurar la información cifrada. Gracias al sistema de copias de seguridad, la empresa no tuvo grandes pérdidas económicas y de información, lo que permitió continuar con la actividad comercial.

Los soportes en los que se pueden realizar copias de seguridad son variados. El soporte escogido dependerá del sistema de copias que se elija, de la fiabilidad que se necesita y de la inversión económica que se quiera realizar. Los más utilizados son:

- Unidades USB y discos duros portátiles.
- Discos duros de equipos específicos.
- Cintas de seguridad.
- Soportes ópticos, como Blu-ray, DVD o CD.
- Almacenamiento de copias en la nube.
- Servidores de almacenamiento en red (NAS).

A la hora de implantar un sistema de copias de seguridad, es necesario tener en cuenta estas características:

- Analizar la información de la que se realizara la copia, descartando toda la información que carezca de relevancia. Es necesario incluir todos los equipos de la organización.
- Definir el número de versiones que se almacenarán de cada elemento y su periodo de conservación. Esta forma de actuar se conoce como política de copias de seguridad. Esta política dependerá del tamaño de la organización y del volumen de información que maneje.

- Otro punto importante es la realización de pruebas de restauración, ya que, si las copias realizadas son inaccesibles o se encuentran dañadas, un sistema de pruebas resolvería este problema.

- Control de los soportes donde se realiza la copia, etiquetando y registrando la ubicación de los soportes. También hay que llevar un control de la vida útil del soporte. Si la información almacenada en la copia es confidencial, es necesario valorar la posibilidad de cifrar las copias.

Documentar el proceso de realización y restauración de las copias. En caso de utilizar almacenamiento en la nube, hay que contar con la posibilidad de no tener conexión a Internet, además de estar informado en cuanto a las políticas de privacidad y seguridad, en caso de almacenar datos sensibles.

En INCIBE ponemos a tu disposición una guía con información detallada sobre los aspectos más relevantes de las **copias de seguridad.**

4.2.3 Medios de pago seguros

Sistema que tienen las tiendas virtuales para aceptar los pagos por medio de tarjetas de crédito o débito. Es común que las proporcionen las entidades bancarias, recibiendo el nombre de "TPV virtual" o simplemente "TPV". La pasarela de pago que se implemente en la tienda debe tener un certificado SSL/TLS de validación extendida. De esta manera, el cliente identificará la entidad bancaria a la que pertenece de manera inequívoca y sus datos bancarios viajarán cifrados.

Antes de implantar la pasarela de pago en la tienda virtual que se encuentra en producción, es necesario realizar una serie de pruebas y configuraciones en preproducción para comprobar su correcto funcionamiento y, si no es así, corregir los errores. Una vez que la pasarela de pago funciona correctamente, es el momento de implementarla en la tienda con acceso a Internet, es decir, en preproducción. La pasarela de pago que se implemente en la tienda debe tener un área de administración propia o back-office, desde donde poder consultar todos los accesos al TPV por parte de los clientes.

La pasarela de pago elegida debe tener unas medidas de seguridad antifraude. Implementarlas es de gran importancia, ya que, de esta manera, se reducen las posibles pérdidas económicas de la tienda virtual.

Las medidas necesarias de seguridad son:

- **CVV**: código de tres dígitos visibles en la parte posterior de la tarjeta junto a la banda magnética. Si solo se implementa esta medida de seguridad, no se conseguirá la seguridad necesaria, ya que el CVV está impreso en la tarjeta y cualquier persona que tenga acceso a ella tendrá acceso a la única medida de seguridad.
- **3DSecure**: este sistema de seguridad está promovido por Visa y MasterCard. Al implementar el sistema 3DSecure en la pasarela de pago, los negocios ya no son los responsables de las devoluciones a causa de las reclamaciones de fraude por parte de los propietarios de la tarjeta. Este sistema de verificación transfiere la responsabilidad de una reclamación por fraude a la entidad que emitió la tarjeta. Es necesario confirmar los términos exactos en el desplazamiento de la responsabilidad con la entidad bancaria de la tienda virtual.

  El sistema 3DSecure verifica que el cliente que está realizando la compra es el verdadero titular de la tarjeta. Antes de terminar el proceso de compra, el cliente debe autenticarse, no pudiendo terminar el proceso de compra alguien que no sea su propietario.

  El método de autenticación de sistema 3DSecure puede ser de diferentes tipos, dependiendo del protocolo de seguridad que tenga la entidad bancaria propietaria de la tarjeta, pudiendo tratarse de un código recibido a través de SMS o desde la misma aplicación de la entidad bancaria.

La implantación de este sistema de seguridad en la pasarela de pago reduce drásticamente el número de transacciones fraudulentas. Esto supone otra ventaja, y es que los administradores de la tienda tendrán que invertir menos tiempo en analizar las ventas producidas en busca de fraude, ya que no habrá tanto riesgo.

Aunque el método de pago más usual es la tarjeta de crédito, en los últimos años, han aparecido nuevas posibilidades para ofrecer a nuestros clientes diferentes posibilidades a la hora de realizar la compra.

Estándares de seguridad para pasarelas de pago

Las pasarelas de pago son servicios críticos que manejan la autorización y el procesamiento de pagos con tarjeta para comerciantes en línea y físicos. Como tal, están directamente afectadas por los estándares del PCI DSS (Payment Card Industry Data Security Standard), que es el estándar de seguridad diseñado para proteger los datos de las tarjetas de crédito y débito y las transacciones de pago contra el fraude y las violaciones de datos.

Las pasarelas de pago deben realizar una transición de la versión 3.2 a la versión 4.0 del PCI DSS antes de la fecha límite del 31 de marzo de 2025. Esto implica actualizar sus sistemas y procesos para cumplir con los nuevos requisitos y recomendaciones más estrictas, tales como la importancia del MFA.

Las pasarelas de pago ahora están obligadas a realizar pruebas de seguridad con más frecuencia para verificar la efectividad de los controles de seguridad y la infraestructura existente. Además, respecto al cifrado de datos, las pasarelas de pago deben asegurar que toda la información sensible, tanto en tránsito como en reposo, esté encriptada, lo cual es ahora un requisito y no solo una recomendación.

Bajo el PCI DSS v4.0, las pasarelas de pago necesitarán llevar a cabo evaluaciones de riesgo específicas y análisis para identificar posibles vulnerabilidades y asegurar la aplicación de controles adecuados para mitigar esos riesgos. La nueva versión también exige reforzar los procedimientos de validación y reporte, lo que requiere que las pasarelas de pago sean más transparentes y detalladas en su reporting sobre la seguridad de los datos de tarjeta.

Pasarelas de pago seguras (PayPal, Stripe, Square...)

Este tipo de plataformas se han popularizado en los últimos años. El usuario crea una cuenta, la cual tiene asociada una tarjeta de crédito o débito, saldo o cuenta bancaria. A través de esta cuenta, el cliente nunca tiene que compartir directamente la información con el sitio web y, por ende, hace más seguro el pago.

Además, cada plataforma cuenta con su propia protección en caso de fraude, tanto para compradores como para vendedores, aunque las políticas y el alcance de esta protección pueden variar, según la plataforma y las circunstancias específicas del fraude. La efectividad de la protección contra el fraude en estas plataformas depende de varios factores, como la rapidez con la que se informa el incidente, la naturaleza del fraude y la capacidad del usuario para proporcionar pruebas que respalden su reclamación

Bizum

Este servicio, por el momento disponible solo en España, está siendo cada vez más usado en los últimos años gracias a la facilidad del mismo. Simplemente se necesita conocer el número de teléfono asociado para realizar el pago. No se proporciona ningún dato financiero y, además, es inmediato.

Se considera un método seguro, ya que funciona directamente con las aplicaciones de banca móvil, lo que hace que herede los protocolos de seguridad e infraestructuras de protección de datos de los grupos financieros. Además, tiene sistemas de límites de transacción y cumple con la Directiva de Servicios de Pago Revisada (PSD2) de la Unión Europea.

e-Wallets (Apple Pay, Google Pay, Samsung Pay...)

Estas carteras electrónicas almacenan información de las tarjetas de crédito y débito de forma segura. Los datos sensibles no se comparten directamente con el comercio durante la transacción, haciéndolas más seguras.

Se consideran seguras, ya que encriptan los datos, requieren una fuerte autenticación, emplean tokenización para realizar transacciones, monitorizan la actividad... Además, deben cumplir con las regulaciones financieras estipuladas por los organismos reguladores, como el cumplimiento de PCI DSS, al manejar los datos de las tarjetas de crédito.

Transferencia bancaria

Se trata de una transacción de dinero del cliente al beneficiario. La urgencia de la misma puede ser configurada por el usuario. Es un método muy seguro, ya que, los bancos están sujetos a regulaciones financieras muy rigurosas, incluido el cumplimiento de estándares internacionales, como el anteriormente mencionado PCI DSS, para cualquier transacción con tarjeta de crédito, así como leyes nacionales e internacionales que exigen altos niveles de protección de datos y privacidad.

Contra reembolso

El consumidor solamente realiza las gestiones previas a la compra y, en caso de devolución, las posteriores, pero el pago se hace en el momento de la recepción del pedido. De esta forma, no se comparte ningún tipo de información bancaria.

4.2.4 Permisos adecuados

Una práctica muy recomendable es dar los permisos apropiados a los archivos y directorios que componen la tienda, ya que se encuentra en un directorio con acceso público, como es el directorio public_html, raíz o similar.

La asignación de permisos es la manera que tiene un sistema operativo de gestionar qué puede o no puede hacer un usuario con los documentos y directorios.

Aplicar de manera correcta los permisos a una tienda virtual es importante, ya que una mala gestión de los mismos puede provocar vulnerabilidades. La mayoría de tiendas virtuales están creadas con un CMS, por lo que aplicar los permisos adecuados a archivos y directorios es importante para la seguridad de la tienda.

La modificación de permisos dentro del CMS es conveniente que sea realizada por un administrador con experiencia en gestores de contenido, ya que una mala aplicación de permisos puede hacer que el CMS no funcione de manera correcta.

4.2.5 Configuración correcta del CMS

La gran mayoría de tiendas virtuales están creadas utilizando un CMS e-commerce o sistema de gestión de contenidos. Se trata de una aplicación o software que facilita la creación, administración y modificación del contenido de las páginas web de forma sencilla, sin necesidad de conocimientos de programación. Pero, como todo software, los CMS pueden tener vulnerabilidades que pueden ser aprovechadas por los cibercriminales. Una gran cantidad de estas vulnerabilidades se deben a malas configuraciones del CMS. Para garantizar la seguridad de un CMS, es necesario implementar una serie de buenas prácticas y medidas de seguridad.

Contraseña de la base de datos: los CMS requieren para su funcionamiento una base de datos, donde se almacenan los artículos, categorías, usuarios y contraseñas, etc. Para acceder a la base de datos es necesario identificarse con un usuario y contraseña. Es de gran importancia que la contraseña que da acceso a la base de datos sea robusta. Para conseguir una contraseña robusta hay que cumplir estas recomendaciones:

- Longitud igual o superior a doce caracteres.
- Incluir mayúsculas, minúsculas, números y símbolo especiales (¡, $, %, &, ?, #).
- Debe ser única y no contener el nombre de usuario, fechas de nacimiento, combinaciones de palabras comunes...
- Debe cambiarse periódicamente y establecer políticas de contraseñas para los usuarios.

- **Prefijo de las tablas de la base de datos**: el prefijo de las tablas de la base de datos es una medida de seguridad importante en la gestión de sistemas de gestión de contenido (CMS). Los prefijos son esenciales porque los nombres de las tablas predeterminados utilizados por los CMS son comúnmente conocidos y pueden ser fácilmente adivinados por ciberdelincuentes en un intento de ataque de inyección SQL u otros tipos de explotaciones de bases de datos. Es recomendable que el prefijo tenga una longitud de cinco caracteres alfanuméricos como mínimo. La gran mayoría de CMS generan prefijos en las tablas de forma automática, pero es recomendable cambiar este prefijo por defecto por uno nuevo con las características anteriores. Esto se hace con la función de mejorar la seguridad de la base de datos del CMS, ya que previene de multitud de tipos de ataques a la misma. Aun así, la base de datos no es la única vía mediante la cual un usuario malintencionado puede acceder a una instalación legítima.

- **Actualización del CMS**: la mayoría de las tiendas están creadas con gestores de contenido orientados a la venta online. Casi todas las vulnerabilidades descubiertas de los CMS se solucionan realizando una actualización del software. Por eso, mantener el CMS actualizado es fundamental para evitar posibles fallos de seguridad.

  En los CMS es muy común usar complementos o plugins que dotarán a la tienda de nuevas funcionalidades. Es importante utilizar plugins confiables y oficiales También, como en el caso de los CMS, es importante mantener actualizados los plugins, ya que, si están desactualizados, estos pueden contener vulnerabilidades que comprometan la tienda.

- **Usuario y contraseña de la zona de administración (backend):** es recomendable que el nombre de usuario no haga ninguna referencia al nombre de la tienda o que tenga alguna relación con la palabra administrador. En el caso de la contraseña, es importante que sea robusta, siguiendo los consejos dados en el apartado anterior: "Contraseña de la base de datos".

- **Borrado del directorio de instalación**: los CMS cuentan con una serie de archivos, cuya única finalidad es la de la instalación de la aplicación. Una práctica recomendable es borrar el directorio y todos los archivos de instalación del CMS, ya que han terminado su función y puede ser una vulnerabilidad que no se eliminen del directorio donde está la tienda virtual. Cabe destacar que algunos CMS no dejan terminar la instalación si el directorio donde se encuentran todos los archivos de instalación no es borrado.

- **Acceso seguro**: para acceder al panel de configuración, es necesario hacerlo de forma segura, utilizando "https" para encriptar la conexión entre el navegador y el servidor. También es posible restringir el acceso al panel solo a direcciones IP autorizadas o configurar los permisos adecuadamente para limitar los accesos no autorizados, asignando los roles y permisos necesarios para cada usuario.

- **Monitorización y registro de actividad**: implementar herramientas para monitorear la actividad y revisarla regularmente permite detectar comportamientos sospechosos, inusuales e intentos de intrusión.

4.2.6 Selección de *hosting*

Cuando la elección tomada para alojar la tienda virtual es contratar un servicio de hosting externo, es necesario seguir una serie de pasos para contratar la mejor opción. Antes de contratar el servicio de almacenamiento en una de las muchas empresas especializadas en estos servicios que hay en el mercado, es necesario informarse sobre los puntos descritos a continuación para hacer la mejor elección.

- **Evaluar las necesidades**: en función del tipo de web que se desee crear, del volumen de la empresa, el tráfico estimado, etc.
- **Tipo de hosting**:
  - **Compartido**: aloja varios sitios web en un mismo servidor, pudiendo considerarse para pequeños negocios. Es más económico, pero puede tener limitaciones en cuanto a recursos y personalización. Además, puede suponer un riesgo en caso de que uno de los sitios web se vea vulnerado.
  - **VPS (servidor privado virtual)**: esta opción ofrece más control y recursos que el hosting compartido, pero su coste puede ser más elevado.
  - **Dedicado**: consiste en un servidor completo para el sitio web. Es más adecuado para alojar negocios con un alto tráfico y necesidades de personalización.
  - **Cloud**: utiliza varios servidores virtuales interconectados. Es escalable en caso de que el sitio web crezca y ofrece una alta disponibilidad.
- **Reputación del proveedor**: este es un aspecto clave, preferiblemente hay que elegir una empresa con bastante experiencia en este tipo de servicios.
- **Soporte**: es necesario saber qué política tiene el proveedor de alojamiento en cuanto a posibles fallos o problemas y decantarse por uno que ofrezca un soporte técnico eficiente y rápido (preferiblemente 24/7) para obtener una solución en caso de que el servidor deje de funcionar.
- **Elementos técnicos**: los proveedores de alojamiento suelen tener una serie de herramientas que ayudan a la gestión de la tienda. Estas herramientas, que los proveedores ponen a disposición de los clientes, realizan diferentes tareas, como el acceso a la base de datos de la tienda, copias de seguridad o la subida de archivos al servidor de manera segura.
- **Políticas de seguridad**: asegurarse de que el proveedor cuanta con medidas de seguridad robustas para proteger el sitio web contra posibles amenazas.
- **Política de uso y condiciones del servicio**: es necesario informarse sobre cuáles son las condiciones de contratación y tener en cuenta aspectos como la situación del centro de procesamiento de datos, o CPD, y las leyes que se aplican en el país donde está alojado, entre otros.

- **Rendimiento y velocidad**: elegir un hosting que proporcione un buen rendimiento y alta velocidad es fundamental para la experiencia del usuario.
- **Facilidad de uso**: verificar que la interfaz y las herramientas proporcionadas son intuitivas y permiten instalar aplicaciones y gestionar archivos fácilmente.
- **Costes**: comprender y asegurarse del precio y de que el servicio no acarree costes ocultos.

4.2.7 Bastionado del servidor

Cuando se opta por la opción de contratar un servidor dedicado o de adquirir un servidor propio para el alojamiento de la tienda online, es muy importante bastionarlo correctamente. El término bastionar se refiere a la práctica de fortalecer la seguridad de un servidor para protegerlo ante amenazas y ciberataques, minimizando las vulnerabilidades.

Bastionar un servidor dedicado y hacerlo seguro para los distintos dispositivos que están conectados a la red es una tarea que debe realizar un profesional. Para conseguir un servidor dedicado seguro es necesario contar con varios elementos de seguridad, como:

- **Ubicación de la página web**: cuando el almacenamiento de la tienda virtual es interno es conveniente ubicar el servidor web en una zona aislada al resto de servidores internos de la organización. Para conseguirlo, es necesario segmentar y ubicar el servidor web en una zona desmilitarizada, también llamada DMZ. Desde la DMZ no debe haber visibilidad a la red interna y, desde la red interna hacia la DMZ, será necesario filtrar todo el tráfico con un cortafuegos o firewall. Implementando estas medidas se evita que, si el servidor que aloja la tienda virtual es vulnerado, el atacante pueda acceder a la red interna de la organización.
- **Monitorización del tráfico de la red**: es conveniente monitorizar todo el tráfico generado desde y hacia la tienda virtual. De esta manera, se podrán detectar posibles ataques y situaciones en las que la tienda virtual haya sido comprometida.
- **Controlar las conexiones hacia el exterior**: la tienda virtual en algunas ocasiones establece conexiones con el exterior, como es el caso de actualización del gestor de contenidos. Este tipo de conexiones deben estar siempre administradas y controladas por una política de conexiones y su correspondiente cortafuegos.
- **Guardado de registros**: esta metodología es importante, ya que por medio de estos registros o logs, se podrán investigar incidentes producidos en la tienda virtual y, si es el caso, poder ponerlos a disposición judicial.

4.2.8 Otras medidas de protección

Una aplicación web, para funcionar correctamente, necesita de distintos softwars que necesitan ser ejecutados por un usuario. Es importante que el usuario que inicia estos servicios tenga solo los privilegios necesarios para el correcto funcionamiento del programa, ya que, si un usuario con privilegios totales del sistema inicia uno de estos servicios y este es vulnerado, el ciberdelincuente tendrá privilegios totales sobre el sistema.

Eliminar metadatos

Cuando se pretende publicar documentos descargables, como PDF, es conveniente borrar los metadatos, ya que estos pueden contener información importante de la organización, como nombres de usuario, directorios, etc.

Validar y filtrar los formularios

La validación y filtrado de los datos debe producirse tanto en el navegador del cliente como en el servidor donde está alojada la tienda online. La validación y filtrado los datos de entrada es importante para evitar fallos en el funcionamiento de la tienda virtual, así como que un ciberdelincuente introduzca información con propósitos maliciosos.

Utilizar sistemas captcha

Cuando la tienda tenga un área donde los clientes introduzcan datos por medio de un formulario es conveniente incorporar sistemas captcha. Este tipo de sistemas es usado para diferenciar personas de máquinas y que estas no puedan crear contenidos o cuentas de usuario de manera automática. Además, puede proteger contra intentos de acceso automáticos que pueden intentar adivinar contraseñas a través de métodos de fuerza bruta.

4.3 Buenas prácticas

4.3.1 Sistemas de respaldo

Este sistema debe ofrecer al usuario unas funcionalidades mínimas en caso de que la tienda virtual no funcione. Los sistemas de respaldo pueden encontrarse en una empresa externa a la organización o dentro de la misma. Si se encuentra dentro de la organización, es conveniente que el sistema de respaldo no comparta ningún tipo de infraestructura con el servidor principal, ya que un problema que afecte al servidor principal podría afectar al servidor de respaldo.

4.3.2 Entornos de PRE y PRO

Es importante diferenciar estos dos tipos de entorno. De esta manera, se podrán aplicar las actualizaciones en un entorno seguro antes de implementarlas en la tienda puesta en Internet.

- El entorno de preproducción tiene como objetico asegurar el correcto funcionamiento de una aplicación en un ambiente controlado. Para ello, se realizan las pruebas exhaustivas antes de su despliegue en producción.
- El entorno de producción es el real, aquel al que los usuarios tienen acceso y en el que pueden utilizar la aplicación. En caso de necesitar implementar cambios o actualizaciones, se probarán primero en preproducción.

4.3.3 Auditorías

Realizar una auditoría técnica de seguridad de la tienda online y del servidor antes de publicar la tienda en Internet es una práctica muy recomendable para evaluar la robustez y protección de los sistemas, descubrir vulnerabilidades y encontrar las soluciones necesarias para corregirlas. Además, mediante la auditoría se asegura que la empresa cumpla con las regulaciones y leyes aplicables, como:

- Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD);
- Reglamento General de Protección de Datos (RGPD);
- Ley de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI-CE);
- Ley General para la Defensa de los Consumidores y Usuarios;
- Real Decreto Legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual;
- Ley de Competencia Desleal y Ley General de Publicidad;
- Ley de Marcas;
- Normativa específica del sector (sector financiero, sector salud...).

analizar la auditoría, se deberán documentar todos los hallazgos identificados durante el proceso de auditoría. Ello incluirá una evaluación de los riesgos asociados, destacando aquellos que presenten mayores amenazas para la seguridad. Con base a los hallazgos y la evaluación del riesgo, se deberán desarrollar planes de acción para mitigar las vulnerabilidades o riesgos detectados. Es esencial realizar auditorías de forma periódica, con el fin de garantizar la seguridad y continuidad del negocio, en cumplimiento con la legislación vigente.

4.3.4 Planes de contingencia

Estrategias destinadas a la realización de acciones y gestiones encaminadas a la recuperación de la actividad total o parcial del negocio, en el caso de que se produzcan incidentes de seguridad que afecten a su continuidad en el tiempo. Gracias a la elaboración de estos servicios, se puede dar una respuesta planificada cuando sucede un fallo de seguridad, haciendo que la organización se recupere antes. Además, se consigue que la imagen corporativa se vea menos dañada de cara al público, con lo que se reducen las posibles pérdidas financieras.

Un plan de contingencia y continuidad debe estar presente en todas las organizaciones, independientemente del tamaño de estas. El plan de contingencia y continuidad debe estar adaptado a cada empresa en función de sus necesidades. Por ejemplo, una gran organización, ante un fallo de seguridad en sus sistemas de telecomunicación, podría hacer uso de un centro de respaldo alternativo. Sin embargo, en una empresa más pequeña dedicada a la venta online podría ser suficiente con que se realizaran copias de seguridad periódicas, almacenándolas en una ubicación distinta al servidor principal o en la nube, y se dispusiese de un servidor de respaldo con el que la página web siga funcionando.

Fases de un plan de continuidad de negocio:

- **Fase 0**: determinación del alcance. Un paso fundamental en un plan de continuidad empresarial es definir su alcance, que incluye los aspectos clave de la organización a enfocar para garantizar su futura operatividad. Esto involucra a todo el personal y abarca activos de información, sistemas y procesos. El enfoque elegido (activo o proceso) determina el alcance del proyecto, adaptándose a distintos tamaños de empresa.

- **Fase 1**: análisis de la organización. En esta fase se recopilará toda la información necesaria para determinar los procesos de negocio críticos a través de reuniones con los usuarios. A continuación, se realizará el análisis de impacto sobre el negocio (BIA), que identificará y evaluará el impacto potencial que tendría la interrupción de las funciones críticas de la organización. Por último, a partir de la información obtenida, se realizará el análisis de riesgos y se generará un plan de tratamiento de riesgos.

- **Fase 2**: determinación de la estrategia de continuidad. El siguiente paso será determinar las estrategias de recuperación más adecuadas. Se deberán valorar aspectos como el coste, la viabilidad de implantación, el mantenimiento, etc.

- **Fase 3**: respuesta a la contingencia. En esta fase se comienzan a implantar las iniciativas recogidas en las fases anteriores, además de la documentación donde se recogerá el proceso, como el plan de crisis.

- **Fase 4**: prueba, mantenimiento y revisión. Para mantener el plan de continuidad actualizado en todo momento será necesario someterlo a una serie de pruebas de diferentes grados de complejidad. Después de cada prueba, se realizará un informe que recoja los resultados obtenidos, se analizarán las incidencias que hayan podido surgir y se aplicarán las medidas correctoras necesarias.

- **Fase 5**: concienciación. Por último, se debe plantar un proceso de concienciación en relación con la continuidad para todos los empleados.

4.4 Políticas de seguridad

Ilustración 13. Políticas de seguridad

Cada vez son más frecuentes los incidentes de seguridad que afectan a las empresas. Las noticias se hacen eco de robos de información y otros ciberataques constantemente. En algunas ocasiones estos incidentes de seguridad son ocasionados de manera involuntaria por el propio personal de la organización, aunque en otras ocasiones son realizados por empleados malintencionados o por ciberdelincuentes ajenos a la organización. Estas situaciones serían en la mayoría de los casos evitables con la implantación de políticas de seguridad de la información.

El primer paso debe ser analizar cuál es la información más importante y crítica para la organización, como puede ser la lista de proveedores o información confidencial de los clientes.

Para conocer la criticidad de la información que trata la organización, puede ser de utilidad abordar las primeras fases del **plan director de seguridad** que INCIBE tiene en su página web.

Una organización de comercio electrónico es recomendable que siga las siguientes políticas de seguridad:

- **Política y normativa de seguridad de la información**: es importante definir, documentar y difundir la política de seguridad dentro de la organización para que todos los usuarios conozcan cuáles son sus obligaciones en materia de seguridad de la información.
- **Controles de acceso lógico**: instaurar una política de contraseñas robustas para el acceso al sistema operativo y a las aplicaciones corporativas, como es el gestor de contenido.
- **Protección frente al malware**: una de las principales amenazas a las que la organización está expuesta es el malware. Para paliar esta amenaza la mejor medida es instalar antivirus en todos los equipos y servidores de la organización. Será necesario actualizarlo periódicamente y configurarlo de manera correcta.
- **Actualizaciones**: establecer una política de actualizaciones, tanto si es automática como manual, solucionará las vulnerabilidades descubiertas de los sistemas operativos y las aplicaciones que gestiona la organización.
- **Medidas de seguridad para la transmisión de información**: proteger de forma correcta todos los canales por los que se transmite información sensible mediante el cifrado de la misma, como puede ser el correo electrónico o la página web.
- **Gestión de soportes**: los soportes extraíbles constituyen una de las principales amenazas de fuga de información e infección por malware, por lo que es necesario controlar el acceso a los puertos en los equipos de la organización.

- **Política de buenas prácticas en las redes sociales**: las redes sociales se han convertido en una herramienta fundamental para las empresas, sobre todo para las tiendas online. Pueden ser un escaparate a nuevos clientes de todas partes si se gestionan de forma adecuada, pero también tienen sus riesgos.

- **Teletrabajo seguro**: poder trabajar desde cualquier ubicación tiene claras ventajas para los empleados, pero con la llegada del teletrabajo han aparecido nuevas amenazas. Es importante seguir una serie de buenas prácticas si se va a trabajar fuera de la infraestructura de la empresa.

- **Uso de dispositivos móviles**: tanto si se va a trabajar con dispositivos móviles corporativos como con personales (BYOD), es necesario hacerlo de forma segura. Los empleados deben seguir unas pautas trabajar con sus dispositivos móviles de forma segura.

4.5 Implantación de medidas de carácter legal

Implantación de medidas de caracter legal

Además de las medidas de seguridad indicadas, es necesario que la tienda cumpla con la siguiente legislación:

Ilustración 14. Medidas legales

- La LSSICE (Ley de Servicios de la Sociedad de Información y Comercio Electrónico) regula los aspectos relacionados con los servicios de la sociedad de la información y del comercio electrónico. Esto incluye las obligaciones de los prestadores de servicios, las comunicaciones comerciales vía electrónica y su prohibición en ciertos contextos, así como la información que debe proporcionarse de manera previa y posterior a la celebración de los contratos electrónicos, junto con las condiciones relativas a su validez y eficacia. Asimismo, la LSSI establece un régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información. En lo relativo a las exigencias de información, la web deberá disponer de las siguientes cláusulas:

    - **Aviso legal**: se deberá incluir la información contenida en el artículo 10 de la LSSI: denominación social de la entidad, NIF, domicilio social, dirección de correo electrónico de contacto, datos de inscripción registral, información sobre el precio del producto o servicio y códigos de conducta a los que se encuentre adherido, en su caso. La AEPD ha elaborado un Informe sobre políticas de privacidad en internet, en el que se proporciona la información necesaria para la correcta implementación de dichas cláusulas en la web.

- **Política de cookies**: información necesaria para cumplir con el requisito de consentimiento informado relacionado con las cookies. En este sentido, la AEDP ha elaborado una Guía sobre el uso de las cookies, que proporciona orientaciones prácticas para cumplir con las obligaciones previstas en la LSSI relativas al uso de las cookies. Las cookies son pequeños dispositivos de almacenamiento y recuperación de datos que se utilizan en el equipo de un usuario, con la finalidad de almacenar información y recuperar la información ya almacenada. Entre otras finalidades, se utilizan para mejorar nuestra navegación o mostrar publicidad personalizada, según nuestros hábitos de navegación. Las empresas tienen la obligación de informar a los usuarios sobre el uso de cookies y obtener su consentimiento antes de utilizarlas, especialmente aquellas que no son estrictamente necesarias para el funcionamiento del sitio web.

- El RGPD (Reglamento General de Protección de Datos establece las normas que rigen la protección de los derechos y libertades fundamentales de las personas físicas, en relación con la protección de sus datos personales. Este reglamento, con carácter europeo, busca garantizar un correcto tratamiento de los datos personales de la ciudadanía en la era digital. Algunas de las exigencias que contempla la normativa es la de notificar a las autoridades competentes (en nuestro caso, la Agencia Española de Protección de Datos (AEPD)) en aquellos supuestos en los que se produzca una brecha de seguridad que afecte a datos personales, así como obtener el consentimiento explícito, informado, unívoco y específico de los usuarios para el tratamiento de sus datos cuando no haya otra base de legitimación que ampare dicho tratamiento.

- Por su parte, la Ley Orgánica de Protección de Datos Personales y Garantía de Derechos Digitales (LOPDGDD) adapta el ordenamiento jurídico español al RGPD, estableciendo garantías específicas relativas a los derechos de los usuarios en el entorno digital. Además, establece la edad mínima de 14 años para aceptar el tratamiento y uso de datos personales.

- Normativas sectoriales: dependiendo del tipo de productos o servicios que se trabajen en la tienda electrónica, se pueden dar unas normativas específicas que se apliquen a su sector. Por ejemplo, las tiendas en línea que venden productos alimentarios deben cumplir con regulaciones de seguridad alimentaria.

- Ley General para la Defensa de los Consumidores y usuarios: las tiendas online tienen la obligación de cumplir con las leyes de devoluciones y garantías que se aplican a la venta de productos. Entre estas obligaciones se incluye proporcionar información clara sobre las políticas de devolución y garantía, así como respetar los derechos de los consumidores, en caso de productos defectuosos o no deseados, y facilitar un formulario en aquellos supuestos que el consumidor o usuario desee desistir de la compra en el plazo legalmente establecido.

- **Ley de Propiedad Intelectual**: si en la tienda virtual comercializa productos digitales, como por ejemplo software o música, o incluso si simplemente se contienen en la propia web creaciones artísticas de terceros, es esencial cumplir con las leyes de propiedad intelectual y derechos de autor correspondiente. Ello implica respetar los derechos de los creadores y asegurarse de contar con las licencias necesarias para la venta, comercialización o publicación de dichos contenidos. Además, se deberá informar de manera clara a los usuarios acerca de las restricciones de uso y derechos de propiedad intelectual con relación a los propios productos ofertados en la web, así como con las creaciones incluidas en la misma.

- **Ley de Competencia Desleal** y **Ley General de Publicidad**: la empresa deberá proteger la competencia, resultando prohibidos los actos de competencia desleal, incluida la publicidad ilícita en los términos establecidos en la Ley General de Publicidad.

- **Ley de Marcas**: La empresa deberá cumplir con la legislación en materia de propiedad industrial, asegurando la protección de sus marcas registradas y sus diseños y evitando el uso no autorizado de marcas de terceros, fortaleciendo así la confianza de sus clientes.

- **Facturación electrónica y fiscalidad**: Se debe cumplir con las regulaciones fiscales vinculadas a la facturación electrónica, la declaración de impuestos y otros aspectos financieros, tales como el IVA.

5. Seguridad de las operaciones en el comercio electrónico

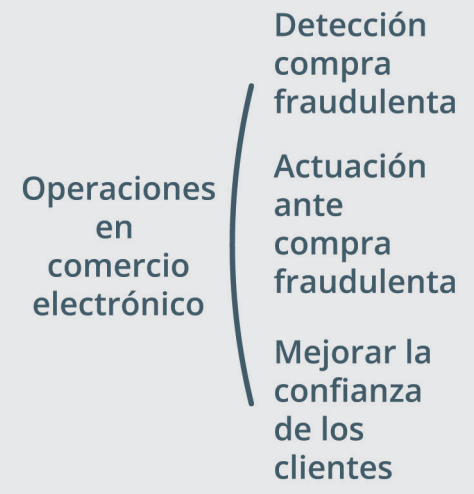


Ilustración 15. Operaciones

En el capítulo anterior se han mostrado los mecanismos para dotar a la tienda virtual de un nivel de ciberseguridad aceptable, pero, como ningún sistema es infalible, es necesario saber de qué manera actuar cuando los mecanismos de seguridad han fallado.

En este capítulo se explicará cómo detectar una compra fraudulenta que se ha producido en la tienda, qué hacer cuando se tiene constancia de que se ha producido una compra fraudulenta y cómo aumentar la confianza de los clientes en nuestra tienda virtual.

5.1 Detección de compras fraudulentas

Implementar mecanismos de seguridad en la tienda es una tarea importante, ya que ayudan a proteger el negocio. Este tipo de mecanismos reducen enormemente la cantidad de fraudes que se cometen en la tienda, pero no son infalibles, por lo que se hace necesario alguna herramienta o metodología de trabajo que ayude a detectar a estos compradores fraudulentos.

Para detectar las compras fraudulentas, es necesario que la persona encargada de administrar la tienda conozca los indicadores que hacen que una compra sea posiblemente fraudulenta. El hecho de que en alguna compra exista un indicador de los descritos a continuación no la hace obligatoriamente una compra fraudulenta, pero es una alerta y se debe prestar especial atención a la compra:

- Varios intentos de compra erróneos en el TPV antes de que la operación sea aceptada. En algunas ocasiones los ciberdelincuentes prueban con varias tarjetas robadas hasta que alguna de ellas pasa los controles, por lo que hay que prestar atención cuando un cliente tiene varios intentos de compra erróneos con distintas tarjetas.

- Verificar que la dirección de email sea verdadera y los datos del cliente coherentes. Una buena práctica comúnmente implementada es enviar un correo de confirmación de pedido. De esta forma, si el correo enviado es devuelto, debido a que la dirección de correo electrónico es inexistente, podemos encontrarnos ante un comprador fraudulento. También hay que desconfiar cuando los datos personales del receptor son incoherentes, incompletos o parecen falsos. Un cliente lícito no suele falsear los datos de envió ni el correo electrónico, ya que, si existe algún problema con el producto, no podrá reclamar si los datos no son correctos.

- Envío urgente del pedido. Si la tienda virtual tiene la opción de "envío urgente" y pedir este tipo de envío encarece considerablemente el importe del producto, puede ser un indicador de que el cliente está cometiendo fraude en la tienda.

- Varios clientes diferentes con la misma dirección de destino. Esto podría ser un indicador de que a la persona a quien se realiza la entrega es una "mula" y no el comprador. Esta "mula" suele ser un intermediario que se encarga de recoger todos los envíos y, posteriormente, entregarlos a los compradores fraudulentos.

- Otra práctica muy recomendable es la creación de listas blancas y listas negras. Las listas blancas contendrán los clientes de la tienda con los que no se ha tenido ningún tipo de problema y la lista negra aquellos clientes que con los que se han tenido problemas, así como cuál fue el problema. Esta forma de trabajar ayuda a tener una visión global de las formas que los ciberdelincuentes usan a la hora de llevar a cabo las estafas.

- Contratar los servicios de empresas especializadas en pagos online y gestión del riesgo, denominadas IPSP (Internet Payment Service Providers). Este tipo de empresas sirven como intermediario entre el cliente y la entidad bancaria de la tienda virtual. Estas empresas incluyen dentro sus productos herramientas antifraude, pasarelas de pago seguras y un panel de administración (back-office), donde se puede realizar el seguimiento de todas las operaciones.

5.2 Actuación ante compras fraudulentas

Cuando el administrador de la tienda sospecha que ha sido víctima de una transacción fraudulenta, lo principal es no enviar la mercancía bajo ningún concepto. Esta forma de actuar puede ir en contra de la política de la empresa, pero es mejor ser cauteloso a perder los artículos enviados al estafador y el dinero de la venta, ya que será reclamado por el banco. Los pasos a seguir en estos casos son los siguientes:

- Ponerse en contacto con el banco para que comprueben si tienen indicios de que esa transacción es fraudulenta. Si es por vía telefónica, solicitarles también la respuesta a través de un email. Así estará todo el proceso bien documentado.

- Contactar con el cliente y pedir que verifique los datos tanto personales como de entrega y tener un registro con todos estos datos. Si el contacto con el cliente se produce vía telefónica, es conveniente que se realice también por correo electrónico. Esta forma de actuar, por lo general, suele disuadir a los cibercriminales, ya que saben que los han descubierto y les requiere más trabajo intentar engañar al comerciante que probar suerte en otra tienda online.

- Es importante documentar toda la información posible del pedido sospechoso, como puede ser el número del pedido, datos del cliente y datos donde se realizaría la entrega. Con toda esta información, acudir a las Fuerzas y Cuerpos de Seguridad del Estado e interponer una denuncia.

Una vez que se realiza una venta y se es consciente de que ha sido una operación fraudulenta, es conveniente no hacer nunca uso del dinero generado por esa transacción, independientemente de que la mercancía se haya enviado o no. El dinero que ha generado esa transacción fraudulenta puede ser reclamado por el banco emisor de la tarjeta. Si se usa de manera reiterada el dinero generado por transacciones fraudulentas, se podría estar incurriendo en un acto delictivo penado por la ley.

5.3 Mejorar la confianza de los clientes

Los clientes son un pilar fundamental para cualquier negocio y, por tanto, es importante brindarles cierto nivel de seguridad y calidad en las compras que realizan a través de Internet. Para que una tienda online sea exitosa, no basta con tener unos precios que compitan con los de las demás tiendas de su sector, sino que tiene que inspirar confianza a la hora de realizar una compra. Es aquí donde entran en juego los sellos de calidad. Estos distintivos garantizan que la tienda posee unas garantías de calidad para con sus clientes.

Estos distintivos de calidad y seguridad pueden ser proporcionados por empresas privadas, entidades públicas u organizaciones sin ánimo de lucro. Estas organizaciones realizan una serie de auditorías para comprobar si el negocio sigue las pautas necesarias para obtener el sello de confianza.

6. Glosario

Centro de procesamiento de datos (CPD): también conocido como centro de procesamiento de datos. Es la ubicación física que contiene los servidores.

CMS: siglas del término en inglés Content Management System o gestor de contenidos. Programa que permite la creación y administración de contenidos principalmente para páginas web.

Linux: sistema operativo de software libre.

PIN: número de identificación personal.

Plugin: complemento que sirve para otorgar una nueva funcionalidad a otro software.

Servidor: máquina capaz de atender peticiones de un cliente y responderlas en concordancia.

Software: soporte lógico de un sistema informático.

VPN: siglas del término inglés Virtual Private Network, que significa red privada virtual. Permite conectarse de forma segura a una red local desde una red no segura, como una red wifi pública.

7. Referencias

[1] Protégete frente al defacement y que no le cambien la cara a tu web

https://www.incibe.es/empresas/blog/protegete-frente-al-defacement-y-no-le-cambien-cara-tu-web

s

[2] Kit de concienciación

https://www.incibe.es/empresas/formacion/kit-concienciacion

[3] Copias de seguridad: una guía de aproximación para el empresario

https://www.incibe.es/sites/default/files/contenidos/guias/guia-copias-de-seguridad.pdf

[4] PCI Security Standards Council

https://www.pcisecuritystandards.org/document_library/

[5] Pagos en línea más seguros: PCI DSS versión 4.0

https://www.incibe.es/empresas/blog/pagos-en-linea-mas-seguros-pci-dss-version-40

[6] Plan Director de Seguridad

https://www.incibe.es/empresas/que-te-interesa/plan-director-seguridad

[7] Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico

https://www.boe.es/buscar/act.php?id=BOE-A-2002-13758

[8] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales

https://boe.es/buscar/act.php?id=BOE-A-2018-16673

[9] AEPD - Agencia Española de Protección de Datos

https://www.aepd.es/

[10] Guía sobre el uso de las cookies

https://www.aepd.es/documento/guia-cookies.pdf

[11] Reglamento (UE) 2016/679 Del Parlamento Europeo y del Consejo de 27 de abril de 2016

https://www.boe.es/doue/2016/119/L00001-00088.pdf

[12] Glosario de términos de ciberseguridad

https://www.incibe.es/sites/default/files/contenidos/guias/doc/guia_glosario_ciberseguridad_2021.pdf

[13] Plan de Contingencia y Continuidad de Negocio

https://www.incibe.es/empresas/que-te-interesa/plan-contingencia-continuidad-negocio

[14] Protege tu web

https://www.incibe.es/protege-tu-empresa/que-te-interesa/protege-tu-web

[15] Protección de la información

https://www.incibe.es/protege-tu-empresa/que-te-interesa/proteccion-informacion

[16] Buenas prácticas en el área de informática

https://www.incibe.es/protege-tu-empresa/que-te-interesa/buenas-practicas-area-informatica

[17] Fraude y gestión de la identidad online

https://www.incibe.es/protege-tu-empresa/que-te-interesa/fraude-gestion-identidad-online

[18] Archivo robots.txt

https://www.robotstxt.org/

[19] Qué son las cookies y cómo mostrarlas en un sitio web

https://www.incibe.es/empresas/blog/son-las-cookies-y-mostrarlas-sitio-web

[20] Si tu web cuenta con certificado de seguridad, comprueba que utilizas una versión segura del protocolo TLS

https://www.incibe.es/empresas/blog/si-tu-web-cuenta-certificado-seguridad-comprueba-utilizas-version-segura-del

[21] Principales formas de estafa a través del email: phishing más comunes

https://www.incibe.es/empresas/blog/principales-formas-de-estafa-traves-del-email-phishing-mas-comunes

[22] Cazando los mitos del comercio electrónico

https://www.incibe.es/empresas/blog/cazando-los-mitos-del-comercio-electronico

[23] Aspectos clave para proteger tu tienda online

https://www.incibe.es/empresas/blog/aspectos-clave-proteger-tu-tienda-online

[24] Tu web es tu tarjeta de presentación. ¡Protégela!

https://www.incibe.es/empresas/blog/tu-web-tu-tarjeta-presentacion-protegela

[25] Aviso legal, una parte importante de tu web

https://www.incibe.es/empresas/blog/aviso-legal-parte-importante-tu-web

[26] ¿Cómo defender la reputación de mi negocio frente a las reseñas falsas?

https://www.incibe.es/empresas/blog/como-defender-la-reputacion-de-mi-negocio-frente-las-resenas-falsas

[27] Blacklist: qué es una lista negra y cómo salir de ella

https://www.incibe.es/empresas/blog/blacklist-que-es-una-lista-negra-y-como-salir-de-ella

8. Ilustraciones