Ciberseguridad en comercio electrónico

Una guía de aproximación para el empresario

incibe_

INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

Autor: Darío Beneitez Juan

Esta guía ha sido elaborada con la colaboración de Jorge Chinea López, Miguel Herrero Collantes y Juan Delfín Peláez Álvarez.

1 SOBRE LA GUÍA

El objetivo de la «guía de ciberseguridad para comercio electrónico, una 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 como 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 quien 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.

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 que es el comercio electrónico y de cuáles son las principales motivaciones de los ciberdelincuentes.
- En la **zona superior** se describe 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 como aumentar la confianza de los clientes en la tienda virtual.

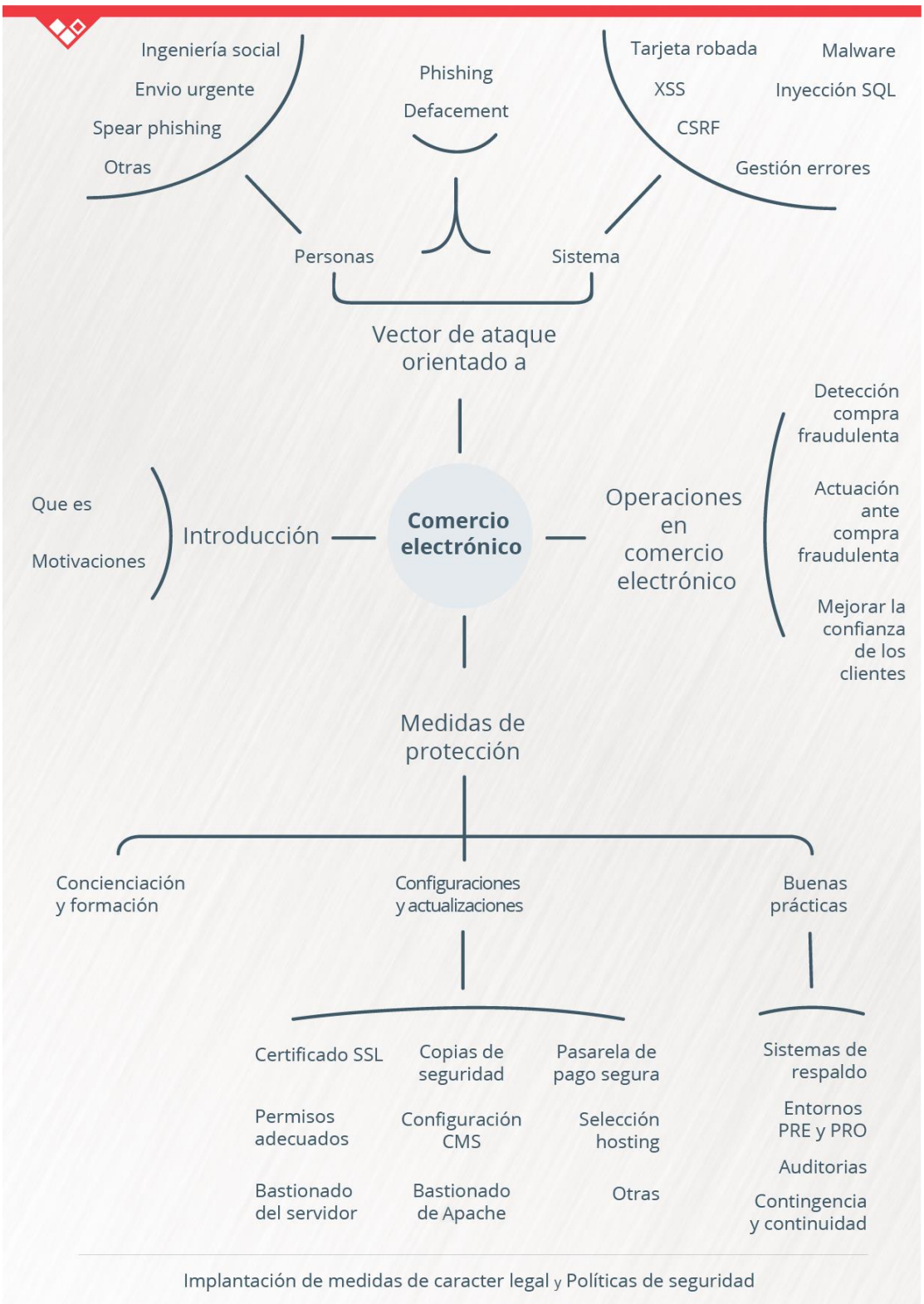

Ilustración 1 Diagrama completo

2 INTRODUCCIÓN SOBRE EL COMERCIO ELECTRÓNICO

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

Ilustración 2 Introducción

Este nuevo entorno tiene una gran trascendencia tanto para las empresas, como para los ciudadanos. 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*.

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 on-line,...) 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 compra-venta de productos utilizando medios telemáticos permite llegar a un número mayor de posibles clientes 24 horas al día, 365 días al año. El comercio electrónico ha aumentado considerablemente en los últimos años y se espera que siga creciendo en los próximos. Por tanto, las empresas deben de adaptarse y evolucionar hacía este mercado digital, teniendo como uno de sus principios rectores la ciberseguridad.

Para comprender mejor las formas de ataque usadas por los ciberdelincuentes 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. Una vez que los ciberdelincuentes 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 beneficio económico de un tercero. Si nuestra web no es segura, pueden utilizarla para poder distribuir *malware*, alojar un *phishing*, infectar nuestro servidor web para utilizar su capacidad de red entre otros tipos de acciones maliciosas.

3 CIBERAMENAZAS

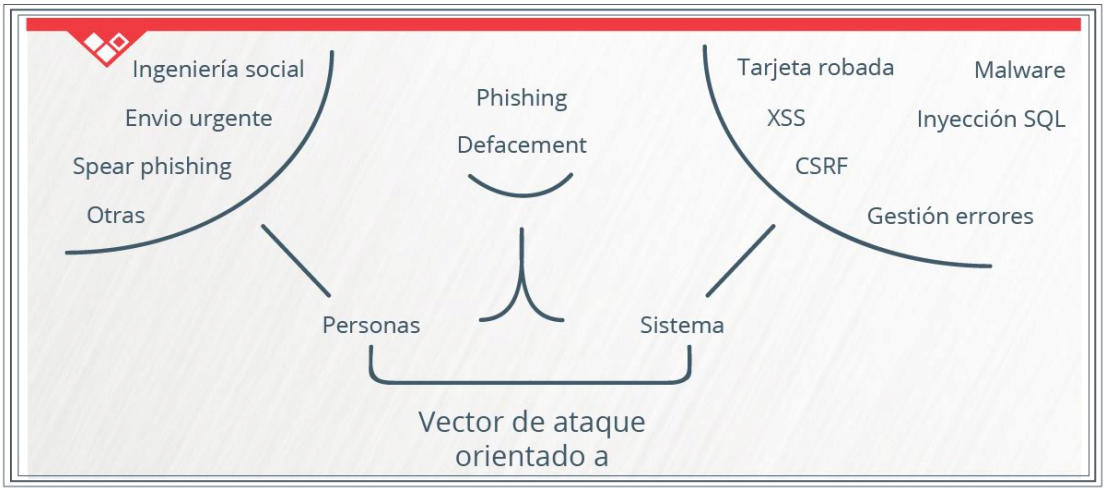

Ilustración 3 Ciberamenazas

Ninguna empresa puede pasar por alto las ciberamenazas, ya que provocan no sólo 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 ciberamenazas 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 las principales ciberamenazas a las 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 delincuentes, diferenciando si el vector de ataque son las personas o el sistema.

3.1 Ataques dirigidos contra las personas

Este tipo de ciberamenazas buscan engañar a las personas y que los ciberdelincuentes obtengan cualquier clase de beneficio, principalmente información confidencial. Las principales amenazas a las que los empleados de la empresa están expuestos son las siguientes:

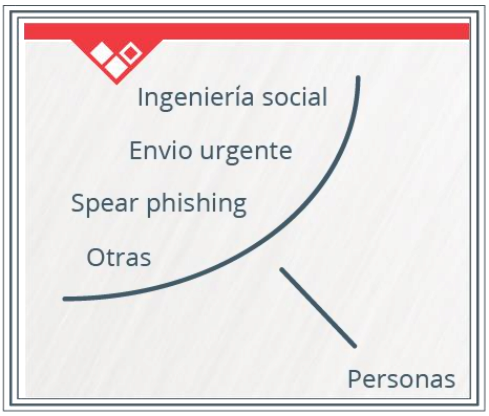

Ilustración 4 Ciberamenazas contra personas

3.1.1 Ingeniería social

La ingeniería social consiste en persuadir y engañar a una persona para influenciarla en sus acciones.

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, por poner algunas medidas.

En el siguiente ejemplo, la ingeniería social en combinación con otras técnicas juega un papel importante alegando 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 nominafeb2015.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.*

Un ejemplo del efecto Una consecuencia que puede tener la técnica anterior en una empresa de comercio electrónico es que el ciberdelincuente 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.

3.1.2 Envío urgente

Otra técnica usada por los ciberdelincuentes muy particularmente en las tiendas virtuales para obtener de manera fraudulenta un artículo es la denominada "Envío urgente". En este tipo de fraude el cliente tiene mucha prisa por conseguir un artículo ya que es para un cumpleaños o cualquier otra fiesta y que pagará el artículo mediante transferencia bancaria. El responsable de la tienda recibe un comprobante escaneado de la transferencia bancaria que está falsificado. El comerciante al haber recibido el comprobante bancario por correo electrónico envía el artículo lo antes posible sin antes ponerse en contacto con la entidad bancaria para comprobar que se ha ingresado el dinero.

El siguiente ejemplo muestra a un ciberdelincuente utilizando esta técnica:

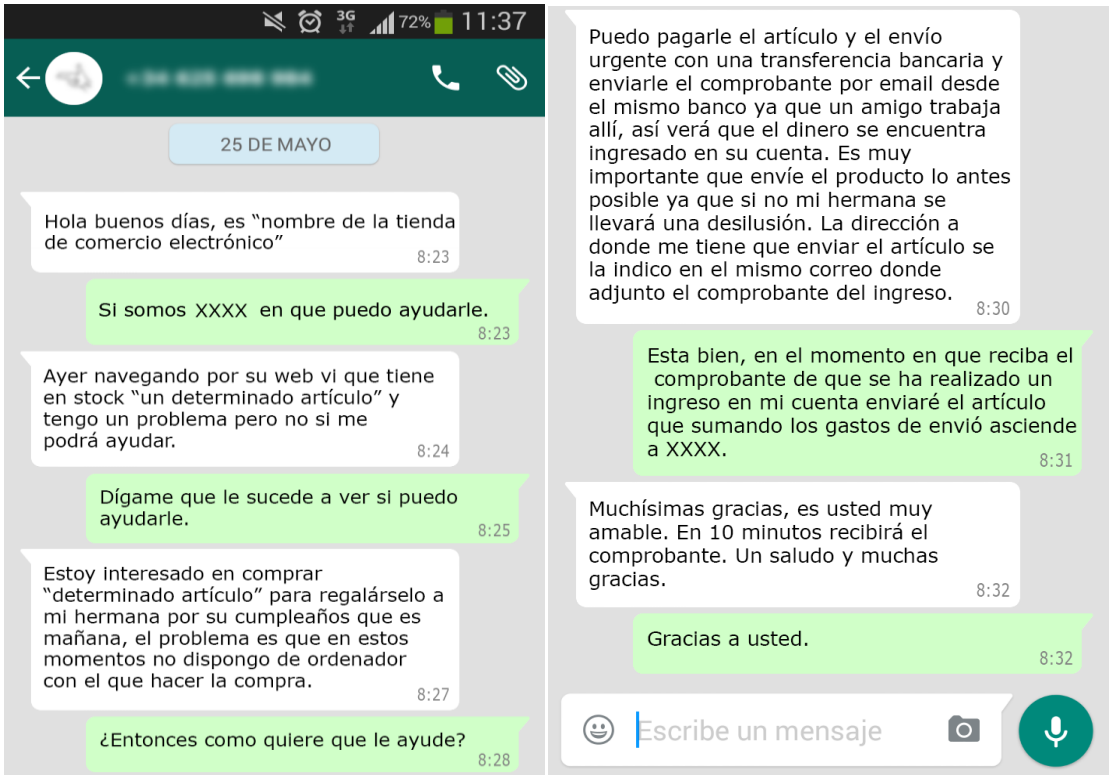

Ilustración 5 Fraude envío urgente

3.1.3 Spear phishing

El *spear phishing* consiste en realizar ataques dirigidos, que se centra 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 ciberdelincuente se basa en información obtenida en redes sociales, blogs personales, y cualquier información personal que esté publicada en Internet.

El siguiente ejemplo muestra a un ciberdelincuente utilizando esta técnica:

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 ciberdelincuente ha recabado información personal de la víctima por medio de las redes sociales. Después de cierta indagación descubrió que la víctima y su familia eran unos apasionados del esquí, además descubrió que su hijo pertenece a una escuela de esquí. Con estos datos el ciberdelincuente preparo su engaño:

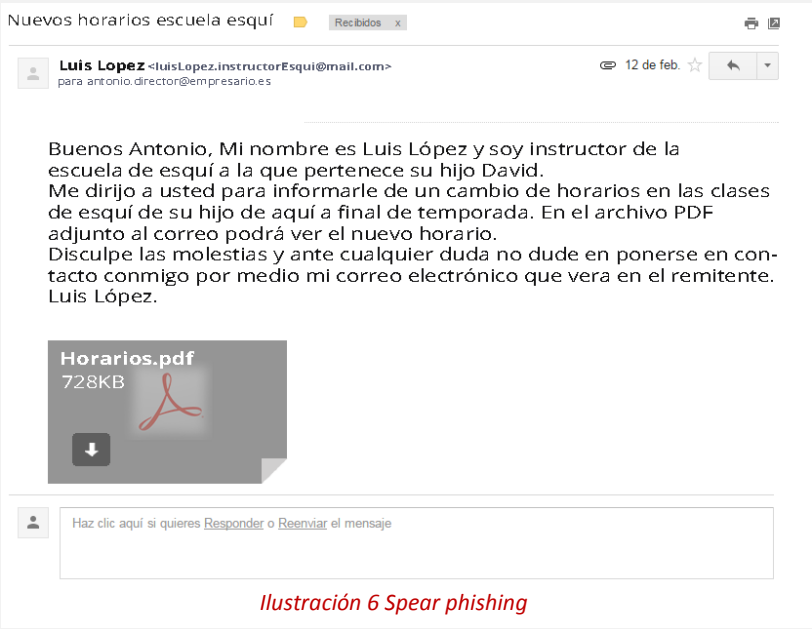

Ilustración 6 Spear phishing

Una vez que la víctima descargue el documento PDF adjunto y lo ejecute -lo intente abrir es el modo más habitual, aunque realmente ejecuta instrucciones introducidas en él-, instala 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 Otros tipos de ciberamenazas

Además de las ciberamenazas anteriormente descritas existen otras que también centran su atención en el personal de la tienda:

- Fraude amigo: En este caso el proceso de compra es legítimo, el pago, la entrega, etc. Sin embargo, una vez realizadas todas las actividades, el cliente declara la compra como fraudulenta en su banco, y el vendedor recibe una petición de devolución, no pudiendo recuperar la mercancía, se haga efectiva o no.

- La triangulación: este método consiste en que el cliente realiza una compra en un comercio virtual fraudulento sin saberlo. El comercio fraudulento realiza el pedido a una tienda legítima pero paga por medio de una tarjeta robada, una vez el estafador ha recibido el producto le enviará el artículo al cliente legítimo. De esta manera el cliente y comerciante ven la transacción como legítima.

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 es el gestor de contenidos o el servidor web donde está alojada la tienda entre otros.

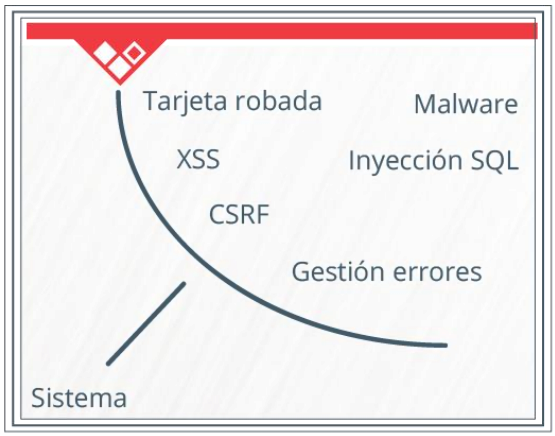

Ilustración 7 Ciberamenazas contra el sistema

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.

- ***Cross-Site Scripting "XSS":*** Brecha de seguridad que se produce en páginas web generadas dinámicamente. En un ataque por XSS, una aplicación Web envía con 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 sitios restringidos y hasta instalar publicidad en el sitio víctima.

- ***Ataques de inyección SQL:*** 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 de ayuda de ingeniería social (como el envío de un enlace por correo electrónico), un atacante puede engañar al usuario de una aplicación web para 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.

- ***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

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.

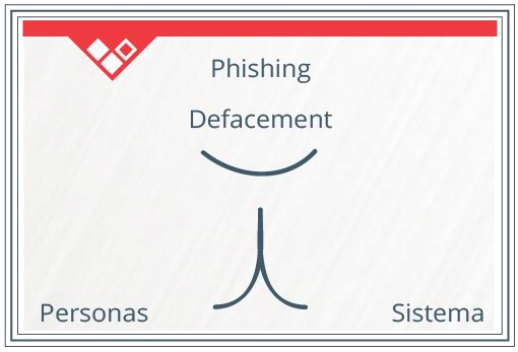

Ilustración 8 Ciberamenazas contra sistema y personas

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 las ciberamenazas 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, mensajes de texto o SMS (*smishing*), redes sociales, mensajería instantánea, etc.

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

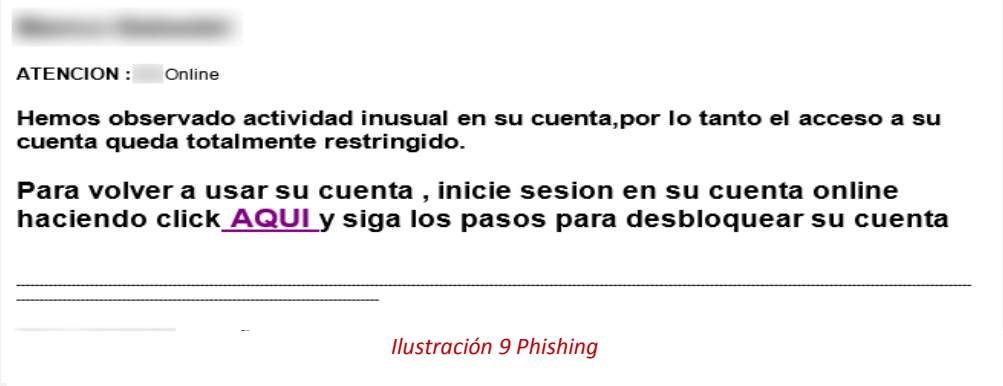

Ilustración 9 Phishing

Una vez que la víctima cae en el engaño y hace click en el enlace adjunto esta será redirigida a una página web fraudulenta con la misma estética que la página web original. Una vez que la víctima es redirigida a la web fraudulenta se la pedirá que se autentifique por medio de su DNI (Documento Nacional de Identidad) y clave de acceso. Una vez que la víctima es validada se la pedirá que introduzca los datos de su tarjeta de crédito. Cuando ha terminado de introducir los datos la víctima es redirigida a la web oficial del banco por lo que esta no será consciente de que la han robado información confidencial.

Phishing alojado en el sistema

El *phishing* alojado el sistema informático de una tienda virtual tiene un objetivo muy distinto al realizado contra las personas. Mientras que el ejemplo anterior tenía como objetivo el robo de información confidencial el *phishing* alojado en el *software* de la organización tiene como objetivo alojar las campañas fraudulentas en los servidores de la empresa.

Para acceder al sistema informático de la organización el cibercriminal explota vulnerabilidades del *software* de la tienda virtual debido a malas configuraciones o falta de actualizaciones del sistema. También puede acceder por medio de cualquier técnica descrita en los ataques realizados contra las personas.

Una vez que ha conseguido acceder por ejemplo al servidor web de la organización almacenará la página web fraudulenta de la entidad a la que está suplantando. Utilizando esta técnica el ciberdelincuente se aprovecha de la capacidad computacional de la organización para perpetrar sus delitos.

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 pueden acceder al gestor de contenidos o el servidor web de la organización por medio de dos vías de entrada como es el personal de la organización o el sistema informático que da soporte a la tienda virtual.

Defacement realizado contra los miembros de la organización

En este caso el cibercriminal accede a la organización gracias a una mala forma de actuar de alguno de los miembros de la organización. El delincuente consigue acceder a la tienda virtual generalmente utilizando técnicas de ingeniería social, *phishing* o *malware* o una combinación de ambas. Por medio de las técnicas anteriores obtendrá las credenciales necesarias para acceder a la tienda virtual y poder cometer el delito.

***Defacement* realizado contra el sistema**

En este caso el cibercriminal explota vulnerabilidades de la tienda virtual debido a malas configuraciones o falta de actualizaciones. Un gestor de contenidos desactualizado o mal configurado podría ser una vía de entrada a la tienda virtual por parte del cibercriminal.

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.

Desde el blog de empresas de INCIBE disponemos de un caso real en el que una tienda virtual fue víctima de esta amenaza:

Historias reales: Mi web ha sido atacada por un grupo Yihadista.

4 MEDIDAS DE PROTECCIÓN

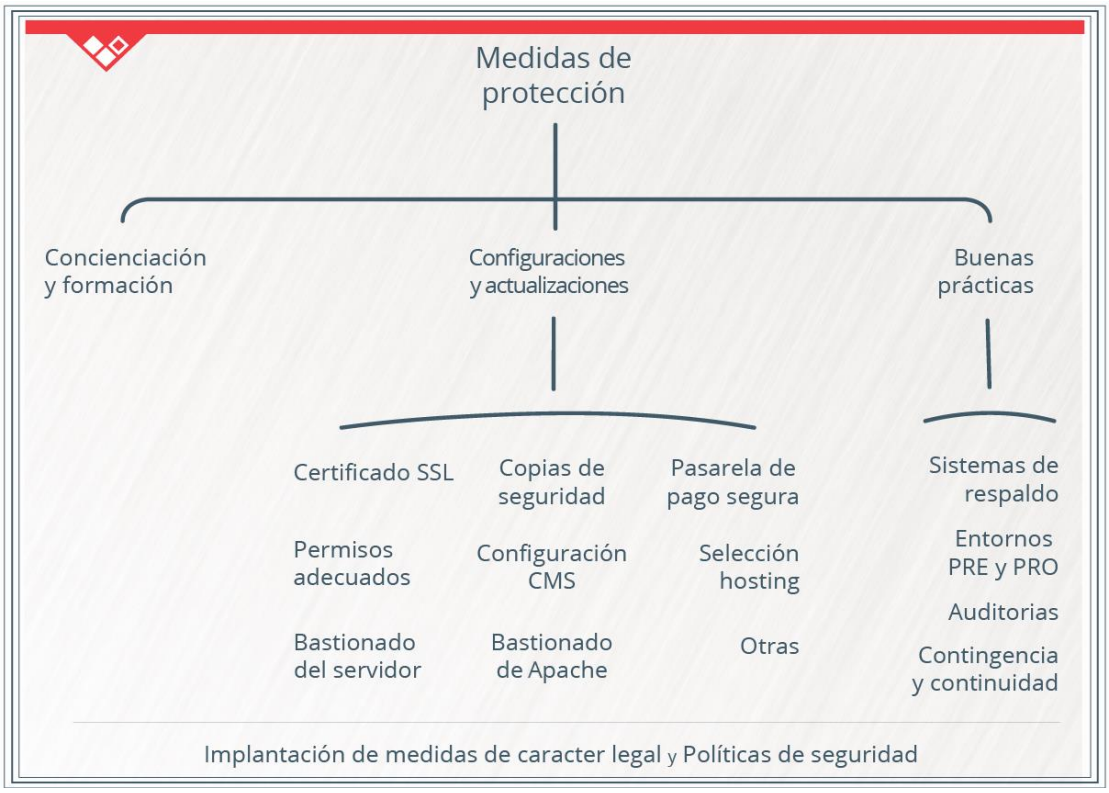

Ilustración 10 Medidas de protección

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 ciberseguridad en la empresa.

Ilustración 11 Personas

En las organizaciones no suele existir 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 permita 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 a 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.

Kit de concienciación gratuito para los miembros de la organización.

4.2 Configuraciones y actualizaciones

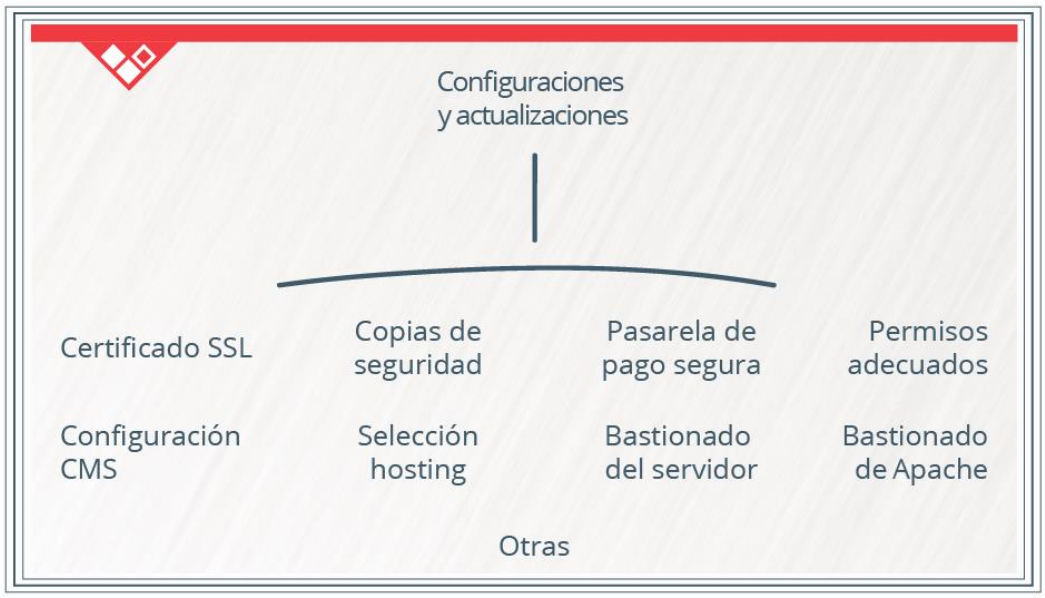

Ilustración 12 Configuraciones y actualizaciones

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

Disponer de un certificado SSL (*Secure Socket Layer*) 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 se intercepta.
- 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 avisara de que está intentando acceder a un sitio web que no se ha podido verificar su legitimidad.

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 lanzara 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 lanzara 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.

Aunque tener instalado un certificado SSL en la tienda virtual no es un requisito imprescindible, sí que es recomendable que la pasarela de pago lo tenga implementado, ya que en este paso se transmite información sensible de los clientes como es su número de tarjeta.

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 que ha sido atacada por un cibercriminal y ha conseguido que ejecutar dentro de la empresa un virus del tipo ransomware. Este virus cifrará gran cantidad de información perteneciente a la empresa pero no supondrá un problema grave ya que 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 a la empresa continuar con su 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 DVD o CD.
- Almacenamiento de copias en la nube.

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 almacenara de cada elemento y su periodo de conservación, esta forma de actuar se la 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 almacena 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.

4.2.3 Pasarela de pago segura

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 de tener un certificado SSL de validación extendida, de esta manera el cliente identificará la entidad bancaria a la que pertenece de manera inequívoca y sus datos bancarios viajaran cifrados.

Utilizar una pasarela de pago de una entidad bancaria hace que la tienda al no tener acceso a los datos bancarios del cliente no tiene la obligación de protegerlos como indica la LOPD (Ley Orgánica de Protección de Datos).

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 "pre-producción" 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 pro-producción. La pasarela de pago que se implemente en la tienda debe de 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 y

en un futuro será su utilización de obligado cumplimiento en toda transacción online. 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 de introducir un numero PIN que solo él debe saber por lo que no podrá terminar el proceso de compra alguien que no sea su propietario.

El numero PIN pedido por el sistema 3DSecure puede ser de tres tipos dependiendo del protocolo de seguridad que tenga asignado la entidad bancaria propietaria de la tarjeta:

- Número PIN de la tarjeta: el mismo número que solicitan los cajeros cuando se hace cualquier operación.
- Número PIN específico: número PIN especial y que es necesario solicitar al banco emisor de la tarjeta. El uso de este número PIN es común en la banca online.
- Número PIN enviado por SMS: número PIN enviado por mensaje de texto o SMS al teléfono del propietario de la tarjeta. Este número PIN es válido para un único uso.

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.

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.

Los permisos es la manera que tiene un sistema operativo en gestionar qué puede, o no puede, hacer un usuario con los documentos y directorios. Puede obtener más información acerca de permisos y de cómo hay que aplicarlos en la siguiente guía:

Guía de seguridad en el gestor de contenidos Joomla.

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* y 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, pero siguiendo estos pasos se conseguirá un CMS seguro.

- Contraseña de la base de datos: los CMS requieren para su funcionamiento una base de datos en 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 condiciones:
    - Longitud igual o superior a ocho caracteres.
    - Incluir, al menos, tres de estos cuatro grupos de caracteres: mayúsculas, minúsculas, números y símbolo especiales (¡, $, %, &, ?, #)
    - Debe de ser diferente y no contener el *nombre de usuario.*
    - No debe de estar basada en diccionario.

- Prefijo de las tablas de la base de datos: es de dominio público y ampliamente conocidos los nombres por defecto que cada CMS aplica a cada tabla por lo que es especialmente importante añadir un prefijo a cada tabla. 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.

- 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, es por ello que mantener el CMS actualizado es fundamental para evitar posibles fallos de seguridad.

  En los CMS es muy común usar complementos o *plug-ins* que dotarán a la

tienda de nuevas funcionalidades. Es importante utilizar *plug-ins* con una gran cantidad de usuarios ya que así se garantiza una continuidad de desarrollo y mantenimiento. También como en el caso de los CMS es importante mantener actualizados los *plug-ins* ya que si están desactualizados estos pueden contener vulnerabilidades que comprometan la tienda.

- Usuario y contraseña de la zona de administración (*back-end*): 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.

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 así hacer la mejor elección:

- Reputación del proveedor: este es un aspecto clave, preferiblemente hay que elegir una empresa con bastante experiencia en este tipo de servicios.

- Tipo de alojamiento (*arquitectura del servicio*): la mayoría de proveedores de alojamiento web ofrecen dos tipos de alojamiento, basados en Windows o en Linux. La mayoría de tiendas online actualmente se encuentran desarrolladas con gestores de contenido orientados a la venta online (*CMS e-commerce*). La gran mayoría de gestores de contenido por razones de compatibilidad se comportan mejor en servidores basados en Linux aunque también es factible que se aloje en un servidor basado en Windows.

- Soporte: es necesario saber qué política tiene el proveedor de alojamiento en cuanto a posibles fallos o problemas como puede ser 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 es el acceso a la base de datos de la tienda, comúnmente con *phpMyAdmin*. Herramientas que realicen copias de seguridad también son de gran utilidad o que permitan subir archivos al servidor de manera segura.

- Políticas de seguridad: conocer qué políticas aplica ante fallos de seguridad en el servidor o la política de copias de seguridad. Estos aspectos es importante conocerlos ya que así se podrán tomar las medidas necesarias para mitigarlos. Si no lo deja claro en las condiciones es recomendable informarse.

- Política de uso y condiciones del servicio: hay que poner especial atención en este punto y detenerse sobre cuáles son las condiciones de contratación y otros aspectos a tener en cuenta 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.

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. 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 o 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 Bastionado de Apache

Apache es un servidor web de *software* libre y de código abierto, siendo uno de los más usados en la actualidad debido a su estabilidad y fácil configuración. Apache se usa principalmente para servir aplicaciones web como las páginas que conforman una tienda virtual.

Apache presenta otra ventaja y es que permite aplicar directivas que modifican la configuración del servidor sin afectar a su configuración global gracias a los archivos de configuración *.htaccess*. Esta característica permite aplicar una configuración específica a una aplicación web y poder aplicar otra configuración a otra aplicación sin afectar a la configuración global del servidor Apache.

Las directivas que permite configurar Apache pueden ser de gran ayuda para el administrador de la tienda virtual ya que permite aplicar configuraciones que aumentan la seguridad de la tienda virtual. Algunas de estas directivas pueden restringir el acceso a la tienda virtual a direcciones IP de un determinado país o implementar una doble autenticación para acceder al *back-end* de la tienda entre otras.

Apache puede tener vulnerabilidades debido principalmente a malas configuraciones por parte de los administradores que afecten de una u otra forma a la seguridad de la tienda. Estas vulnerabilidades pueden permitir al ciberdelincuente alojar *malware* en la tienda virtual o utilizar el servidor de la organización para realizar una campaña de *phishing* entre otros tipos de ataques posibles.

Para evitar fallos de seguridad en el servidor Apache desde INCIBE disponemos de una guía con las pautas necesarias para bastionar Apache:

Guia bastionado software Apache

4.2.9 Otras medidas de protección

Mínimos privilegios

Una aplicación web para funcionar necesita de distintos *software,* para ejecutarlos es necesario que los inicie 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 PDFs 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 evitar que un ciberdelincuente introduzca información con propósitos maliciosos.

Utilizar sistemas captcha

Cuando la tienda tenga un área en 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.

4.3 Buenas prácticas

4.3.1 Sistema de respaldo

Este sistema debe de 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 producción

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.

4.3.3 Auditorias

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 que sirve para descubrir vulnerabilidades y que soluciones será necesario aplicar para corregirlas.

4.3.4 Planes de contingencia y continuidad

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 de estar presente en todas las organizaciones independientemente del tamaño de esta. El plan de contingencia y continuidad debe de 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 una empresa más pequeña dedicada a la venta online podría ser suficiente con que realizara copias de seguridad periódicas almacenándolas en una ubicación distinta al servidor principal o en la nube y disponer de un servidor de respaldo con el que la página web siga funcionando.

Dentro de la web INCIBE existe un artículo que indica las fases de un plan de contingencia y continuidad y cómo abordarlo de forma correcta.

Plan de contingencia y continuidad de negocio

4.4 Políticas de seguridad

Es muy común escuchar noticias sobre incidentes de ciberseguridad como fue el robo de información confidencial de la multinacional Sony a finales del 2014.

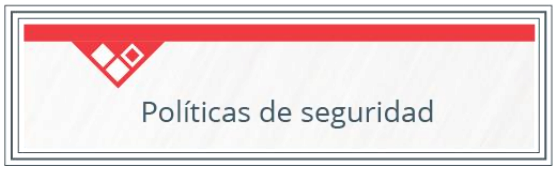

Ilustración 13 Políticas de seguridad

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 es su página web.

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

- 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.

4.5 Implantación de medidas de carácter legal

Además de las medidas de seguridad y en ocasiones como causas de las mismas, es necesario que la tienda cumpla con otras medidas de carácter legal:

Ilustración 14 Medidas legales

- La LSSICE (Ley de Servicios de la Sociedad de Información y Comercio Electrónico) es una Ley que protege a los consumidores de la red y regula aspectos como la información sobre los prestadores del servicio, los pasos necesarios para contratar el servicio, condiciones generales, etc.

- La LOPD (Ley Orgánica de Protección de Datos) la cual establece requisitos como notificar a la Agencia Española de Protección de Datos (AGPD) el tipo de datos que tratamos, así como implantar diferentes medidas de seguridad según la sensibilidad de nuestra información y documentar todos los aspectos relacionados con la seguridad de los datos en un documento de seguridad.

- Otro elemento legal a considerar es la normativa aplicable a las cookies como indica la Agencia Española de Protección de Datos (AGPD). Las cookies son pequeños ficheros que las páginas web guardan en nuestro equipo. Se utilizan para mejorar nuestra navegación o mostrar publicidad personalizada según nuestros hábitos de navegación. Las cookies se encuentran reguladas por la ley según el decreto 13/2012 también conocido como Ley de Cookies. Esta ley obliga a las páginas web a informar a los usuarios del uso de cierto tipo de cookies, y a solicitar el consentimiento expreso del usuario para poder utilizarlas.

5 SEGURIDAD DE LAS OPERACIONES EN EL COMERCIO ELECTRÓNICO

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

Es 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.

Ilustración 15 Operaciones

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 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 si hay que estar más atento a ese cliente:

- 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 estar atento 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. La 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 ha 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.

- Otra forma es 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*) en 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.

- Ponerse en contacto con el banco para que comprueben si tienen indicios de que esa transacción es fraudulenta. Si es por vía telefónica pedirles que respondan también por 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 lleva 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

Hoy en día el cliente es el que manda y exige cierto nivel de seguridad y calidad en las compras que realiza por internet. Si la tienda online quiere vender no basta con tener unos precios que compitan con los de las demás tiendas de su sector sino que tiene que inspirar confianza para que compre en nuestra tienda y no se vaya a la competencia. 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 son proporcionados tanto por empresas privadas, entidades públicas y organizaciones sin ánimo de lucro. Estas organizaciones realizan una serie de auditorías para comprobar si sigue las pautas necesarias para obtener el sello de confianza.

Desde INCIBE disponemos de un servicio con el que en función de tu negocio puedes ver que sello se adapta mejor a tus necesidades.

Herramienta Haz negocios con 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 termino 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.

Plug-in: complemento que sirve para otorgar una nueva funcionalidad a otro software.

Servidor: maquina 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] Guía básica de seguridad en Magento. Junio de 2014 disponible en: https://www.incibe.es/CERT/guias_estudios/guias/guia_magento

[2] Guía básica para la securización del gestor de contenidos Joomla. Febrero de 2013 disponible en: https://www.incibe.es/CERT/guias_estudios/guias/guia_securizacion_joomla

[3] Guía básica para la securización de Wordpress. Septiembre de 2012 disponible en: https://www.incibe.es/CERT/guias_estudios/guias/guia_securizacion_wordpress

[4] Guía básica para la securización del servidor web Apache. Agosto de 2012 disponible en: https://www.incibe.es/CERT/guias_estudios/guias/guia_apache

[5] Guía sobre la seguridad y privacidad en el comercio electrónico. Enero 2010 disponible en: https://www.incibe.es/file/LskjzZLl7XTCI6RE5arRRg

[6] Guia de seguridad de las TIC (CCN-STIC-812) Seguridad en ento4rnos y aplicaciones web. Octubre de 2011 disponible en https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/812-Seguridad_en_Entornos_y_Aplicaciones_Web/812-Entornos_y_aplicaciones_web-oct11.pdf

[7] Protege tu web de INCIBE. Disponible en: https://www.incibe.es/empresas/que_te_interesa/Protege_tu_web/

[8] Protección de la información de INCIBE. Disponible en: https://www.incibe.es/empresas/que_te_interesa/Proteccion_de_informacion/

[9] Buenas prácticas en el área de informática de INCIBE. Disponible en: https://www.incibe.es/empresas/que_te_interesa/Buenas_practicas_en_informatica/

[10] Fraude y gestión de la identidad online de INCIBE. Disponible en: https://www.incibe.es/empresas/que_te_interesa/Fraude_y_gestion_de_la_reputacion_online/

[11] Archivo robots.txt. Disponible en: http://www.robotstxt.org/

[12] ¿Qué son las cookies? ¿Cómo nos aplica su ley? Mayo de 2014 en: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/cookies_empresas_ciberseguridad

[13] ¿Qué aporta un certificado digital SSL a mi sitio web? ¿Cómo seleccionar uno? Enero de 2015 disponible en: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/certificado_digital_SSL_sitio_web_seleccionar_uno

[14] Últimas tácticas de phishing y sus posibles consecuencias para las empresas. Disponible en: http://www.roadtoprofitability.com/campaigncentral/campaignFiles/15272%20Symantec%20phishing-tactics-cala%20v2.pdf

[15] Políticas, normas, procedimientos de seguridad y otros documentos de un SGSI. Agosto de 2008 disponible en: https://www.incibe.es/blogs/post/Seguridad/BlogSeguridad/Articulo_y_comentarios/Politicas_normas_procedimientos_de_seguridad_y_otros_documentos_de_un_SGSI

[16] Estableciendo el rumbo de un SGSI. Junio de 2009 disponible en: https://www.incibe.es/blogs/post/Empresas/BlogSeguridad/Articulo_y_comentarios/Estableciendo_el_rumbo_de_un_SGSI