Comercio electrónico

Políticas de seguridad para la pyme

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

ÍNDICE

1. Comercio electrónico 3

1.1. Antecedentes 3
1.2. Objetivos 3
1.3. Checklist 4
1.4. Puntos clave 6

2. Referencias 9

1. COMERCIO ELECTRÓNICO

1.1. Antecedentes

El comercio electrónico ha cambiado los hábitos de compra de la población. Su aceptación y continuo crecimiento entre comerciantes se debe a los beneficios asociados: mayor alcance de público objetivo, oportunidad de crecimiento, no requiere una gran inversión, flexibilidad en los medios de pago, etc.

Para conseguir que los clientes confíen en la tienda online debemos contemplar los siguientes aspectos de seguridad:

- Seguir una política de web segura [1].
- Contemplar los aspectos legales mostrando el aviso legal, la política de cookies y las condiciones de contratación.
- Si utilizas un Marketplace (eBay, Amazon, Vibbo, etc.) hay que tener en cuenta sus particularidades legales y de seguridad [2].
- Utilizar una pasarela de pago segura [3] que ofrezca canales cifrados para las transacciones (https) o bien verificar que las pasarelas de pago contratadas cumplen con el estándar de seguridad PCI-DSS que garantiza que los titulares de tarjetas pueden realizar compras seguras y que la información de sus tarjetas está protegida ante posibles fraudes online.
- Avalar la seguridad mostrando sellos de confianza [4] preferiblemente aquellos que auditen la web periódicamente.
- Disponer de copias de seguridad que permitan restaurar el sitio web en caso de sufrir un ataque.
- Vigilar las transacciones para evitar el fraude [12].

1.2. Objetivos

Verificar que se aplican las medidas necesarias para garantizar la seguridad de los clientes, y evitar el fraude en las compras online.

1.3. Checklist

A continuación se incluyen una serie de controles para revisar el cumplimiento de la política de seguridad en lo relativo a **comercio electrónico**.

Los controles se clasificarán en dos niveles de **complejidad**:

- Básico (**B**): el esfuerzo y los recursos necesarios para implantarlo son asumibles. Se puede aplicar a través del uso de funcionalidades sencillas ya incorporadas en las aplicaciones más comunes. Se previenen ataques mediante la instalación de herramientas de seguridad elementales.
- Avanzado (**A**): el esfuerzo y los recursos necesarios para implantarlo son considerables. Se necesitan programas que requieren configuraciones complejas. Se pueden precisar mecanismos de recuperación ante fallos.

Los controles podrán tener el siguiente **alcance**:

- Procesos (**PRO**): aplica a la dirección o al personal de gestión.
- Tecnología (**TEC**): aplica al personal técnico especializado.
- Personas (**PER**): aplica a todo el personal.

NIVEL	ALCANCE	CONTROL	
A	PRO	**Cumplimiento Políticas relacionadas** Cumples con lo establecido en la Política de seguridad web y la Política de relación con proveedores si aplicara.	☐
A	PRO	**Certificado web con validación extendida** Adquieres un certificado web para tu tienda online que asegure las transacciones de los clientes, preferiblemente con validación extendida	☐
A	PRO	**Sellos de confianza para el comercio electrónico** Obtienes sellos de confianza para garantizar la seguridad y la calidad de tu web.	☐
A	PRO/TEC	**Medidas de carácter legal** Te aseguras de que tu web cumple todas las medidas legales (Aviso Legal, condiciones de contratación, Cookies,…)	☐
B	PRO/TEC	**Prevención compras fraudulentas** Elaboras listas blancas y negras de tus clientes. Contratas servicios de empresas IPSP.	☐
A	TEC	**Pago virtual con tarjetas de crédito** Cumples, o revisas el cumplimiento de las pasarelas de pago que contrates, con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS).	☐
B	TEC	**Control de acceso** Aplicas la Política de control de acceso y la Política de contraseñas para acceder al gestor de contenidos.	☐
A	TEC/PER	**Detección de compra fraudulenta** Compruebas los intentos de compra, los datos del comprador y las opciones de envío.	☐

NIVEL	ALCANCE	CONTROL	
A	PER	**Prevención del fraude: comprobaciones a realizar para aceptar nuevos clientes** Compruebas si los datos del cliente están incluidos en alguna lista negra, si la cuantía del pedido es muy elevada, si la dirección destino es nacional o internacional, si el método de pago mantiene registros de fraude y si éste se realiza con tarjeta compruebas que la dirección destino del pedido coincide con los datos de localización del cliente.	☐
A	PER	**Prevención del fraude: comprobaciones a realizar para clientes registrados** Compruebas si los datos del cliente están en la lista blanca, si en el historial aparece algún problema en el pago, si el método de pago es el habitual y si los datos bancarios y la dirección destino coinciden con los de los pedidos anteriores.	☐
B	PER	**Actuación ante la detección de compra fraudulenta** No envías la mercancía, contactas con el banco para comprobar la transacción, contactas con el cliente para que verifique sus datos, no usas el dinero proveniente de la compra, acudes a las FCSE para interponer una denuncia.	☐

Revisado por: _____ **Fecha:** _____

1.4. Puntos clave

Los puntos clave de esta política son:

- **Cumplimiento de políticas relacionadas.** La tienda online es una página web y como tal está sujeta a la **Política de seguridad web**. Por otra parte si contratamos el servicio de alojamiento, el desarrollo o su mantenimiento tendremos en cuenta la **Política de Relación con proveedores.**
- **Certificado web con validación extendida.** La tienda online debe contar con un certificado web preferiblemente con validación extendida [13]. Los certificados web proporcionan garantías en la identificación de nuestra web (candado) y en el cifrado (https://) de las comunicaciones entre el cliente web y el servidor: Estas garantías están avaladas por una Autoridad de Certificación. En el caso de los de validación extendida la verificación de la seguridad de la tienda online es más exhaustiva ofreciendo por tanto mayores garantías y mayor confianza a los clientes en sus compras.
- **Sellos de confianza para el comercio electrónico.** Para cumplir las expectativas de seguridad del cliente, la web debe contar con sellos de confianza. Estos distintivos son proporcionados por empresas privadas, entidades públicas y organizaciones sin ánimo de lucro. Algunas de estas organizaciones realizan auditorías para comprobar si la web cumple los requisitos para obtener el sello de confianza y otras ofrecen mecanismos para adherirse a códigos de buenas prácticas. Para las tiendas online se recomiendan aquellos que realizan auditorías de seguridad.
- **Medidas de carácter legal:** las tiendas de comercio electrónico deben cumplir las cuestiones legales recogidas en:
  - LSSI-CE (Ley de Servicios de la Sociedad de Información y Comercio Electrónico) [5].
  - El Reglamento europeo de protección de Datos (RGPD) [6].
  - Ley de Cookies [7].
- **Prevención compras fraudulentas.** Para evitar posibles compras fraudulentas se recomienda:
  - La creación de listas blancas y listas negras. Las blancas contendrán los clientes fiables, mientras que las negras los clientes con los que se ha tenido problemas, especificando cuál es el motivo del mismo.
  - Contratar los servicios de empresas especializadas en pagos online denominadas IPSP (*Internet Payment Service Providers*). Este tipo de empresas (PayPal, Google Wallet, Amazon Payments, etc.) sirven como intermediario entre el cliente y la entidad bancaria de la tienda virtual. Proporcionan herramientas antifraude, pasarelas de pago seguras y un panel de administración para realizar el seguimiento de todas las operaciones.
- **Pago virtual con tarjetas de crédito.** El método de pago virtual con tarjetas de crédito debe de cumplir con el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (*Payment Card Industry Data Security Standard*) o PCI DSS [9]. Se trata de un conjunto de requerimientos y procesos para ayudar a garantizar que los titulares de tarjetas pueden realizar compras seguras y que la información de sus tarjetas está protegida ante posibles fraudes online. En cualquier caso se

recomienda elegir pasarelas de pago que no nos obliguen a guardar ningún dato de las tarjetas o cuentas de los clientes.

- **Control de acceso** [8]**:** seguiremos la Política de control de accesos y la Política de contraseñas para el acceso al panel de administrador del gestor de contenido y del servicio de alojamiento de la tienda online. Si es posible se utilizara doble factor de autenticación [11]. Tendremos cuidad de acceder siempre desde un ordenador cuya seguridad esté controlada y verificar que la conexión es cifrada (https://)
- **Detección de compra fraudulenta.** Existen diferentes indicadores para detectar una posible compra fraudulenta a los que hay que prestar una especial atención:
  - Comprobar que no se han producido varios intentos de compra erróneos en el TPV antes de que la operación sea aceptada.
  - Verificar que la dirección de email existe y los datos del cliente son coherentes.
  - Sospechar cuando se elige la opción de envío urgente del pedido cuando esta encarece considerablemente el producto.
  - Comprobar que no existen distintos clientes con la misma dirección de destino. Puede tratarse de un mismo receptor intermediario que después entregará las compras fraudulentas a sus destinatarios.
- **Prevención fraude: comprobaciones a realizar para aceptar nuevos clientes.** Para garantizar la fiabilidad de la compra de un cliente nuevo debemos comprobar:
  - Si los datos del cliente están incluidos en alguna lista negra corporativa.
  - Si la cuantía del pedido realizado es muy elevada.
  - Si la dirección destino del pedido es nacional o internacional.
  - Si el método de pago seleccionado mantiene registros de fraude, comprobar si existen datos del cliente para verificar su reputación.
  - Si el método de pago seleccionado es tarjeta, comprobar que la dirección destino del pedido coincide con los datos de localización del cliente (ubicación del registro de la tarjeta, localización de la IP desde la que se realiza el pedido, configuración regional del dispositivo desde el que se realiza el pedido,…).
  - Si algún dato del pedido nos resulta extraño, llamar al cliente para realizar la comprobación de una manera más directa e inmediata.
- **Prevención del fraude: comprobaciones a realizar para clientes registrados.** Cuando el cliente está registrado por compras anteriores debemos comprobar:
  - Si los datos del cliente están incluidos en la lista blanca corporativa.
  - Si en el historial de pedidos aparece algún problema previo en el pago.
  - Si el método de pago seleccionado es el habitual.
  - Si los datos bancarios del pedido coinciden con los de los pedidos anteriores.
  - Si la dirección destino del pedido concuerda con la de los pedidos anteriores.
- **Actuación ante la detección de compra fraudulenta.** Cuando se sospecha ser víctima de una compra fraudulenta esta es la forma correcta de actuar:
  - No enviar nunca la mercancía.
  - Contactar con el banco para comprobar que la transacción es correcta pidiendo una respuesta por escrito.
  - Contactar con el cliente para que verifique los datos. Pedir que envíe sus datos personales por correo electrónico.
  - Nunca usar el dinero proveniente de una posible compra fraudulenta ya que puede ser reclamado por la entidad emisora de la tarjeta.

- Acudir a las Fuerzas y Cuerpos de Seguridad del Estado para interponer una denuncia.

2. REFERENCIAS

[1]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Protección de la página web https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[2]. Incibe – Protege tu empresa – Blog – Barato, barato,… ¿son seguros los marketplaces para vender tus productos? · https://www.incibe.es/protege-tu-empresa/blog/barato-barato-son-seguros-los-marketplaces-vender-tus-productos

[3]. Incibe – Protege tu empresa – Blog – Pago seguro: ¿Cuál de estas dos empresas es la tuya? · https://www.incibe.es/protege-tu-empresa/blog/pago-seguro-cual-de-estas-dos-empresas-es-la-tuya

[4]. Incibe – Protege tu empresa – Sellos de confianza – Comercio electrónico https://www.incibe.es/protege-tu-empresa/sellos-confianza/comercio-electronico

[5]. LSSICE, Ley de Servicios de la Sociedad de Información y Comercio Electrónico · http://www.lssi.gob.es/paginas/Index.aspx

[6]. REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016. Reglamento general de protección de datos · http://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32016R0679&from=ES

[7]. Agencia española de protección de datos personales – Cookies http://www.agpd.es/portalwebAGPD/canaldocumentacion/cookies/index-ides-idphp.php

[8]. Incibe – Protege tu empresa – Herramientas – Políticas de seguridad para la pyme – Contraseñas https://www.incibe.es/protege-tu-empresa/herramientas/politicas

[9]. Incibe – Protege tu empresa – Avisos – Empieza la cuenta atrás para adecuarse a PCI DSS v3.2 · https://www.incibe.es/protege-tu-empresa/avisos-seguridad/cuenta-atras-adecuaresPCIDSSv32

[10]. Incibe – Protege tu empresa – Blog – Requisitos para ofrecer el pago virtual con tarjetas en la web de tu empresa · https://www.incibe.es/protege-tu-empresa/blog/requisitos-ofrecer-pago-virtual-tu-empresa

[11]. Incibe – Protege tu empresa – Blog – Dos mejor que uno: doble factor para acceder a servicios críticos https://www.incibe.es/protege-tu-empresa/blog/dos-mejor-uno-doble-factor-acceder-servicios-criticos

[12]. Incibe – Protege tu empresa – Blog – ¿Tienes una tienda online? ¡Conoce cómo prevenir compras fraudulentas! https://www.incibe.es/protege-tu-empresa/blog/tienda-online-conoce-como-prevenir-compras-fraudulentas

[13]. Incibe – Protege tu empresa – Blog – ¿Qué aporta un certificado digital SSL a mi sitio web? ¿Cómo seleccionar uno? https://www.incibe.es/protege-tu-empresa/blog/certificado-digital-ssl-sitio-web-seleccionar-uno

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

INSTITUTO NACIONAL DE CIBERSEGURIDAD