INICIO GRABACIÓN

SANJOSÉ
FUNDACIÓN DE EDUCACIÓN SUPERIOR

CIBERSEGURIDAD MIPYMES

TU WEB, ES TU TARJETA DE PRESENTACIÓN

PARTE

OBJETIVOS

- Concienciar sobre la necesidad de **proteger la web**, comprendiendo las motivaciones de los ciberdelincuentes.
- Describir los pasos a seguir para dotar a una web o una tienda online de un nivel de **ciberseguridad** aceptable, tanto para el **propietario** como para el **cliente**.
- Establecer unos **requisitos de seguridad** en las aplicaciones web, para que los clientes tengan una experiencia digital segura.
- Describir las principales **ciberamenazas** y las **recomendaciones** que hay que aplicar para **reducir el riesgo** de que se produzcan.
- Conocer como se puede aumentar la **confianza de los clientes** en la web o en la tienda online, ofreciendo un valor añadido con respecto a la competencia.

1. ¿POR QUÉ PROTEGER MI WEB Y MI TIENDA ONLINE?

¿Por qué querrían atacar nuestra tienda?

- Para **robar** nuestros **datos de clientes**, sus contraseñas, datos de pago, correos electrónicos, … y **utilizarlos**, **publicarlos** o **venderlos**.
- **Utilizar nuestro servidor** web para simular ser otro negocio fraudulento o instalar publicidad engañosa.
- Dejar **fuera de servicio** nuestra web para desprestigiarnos.
- Utilizar nuestro servidor web para **reivindicar ideas** políticas, sociales,…
- Robar nuestras **contraseñas de acceso a otros sistemas**, acceder y utilizarlos para fines maliciosos (spam, distribución de malware, lanzar ataques de denegación de servicio …)

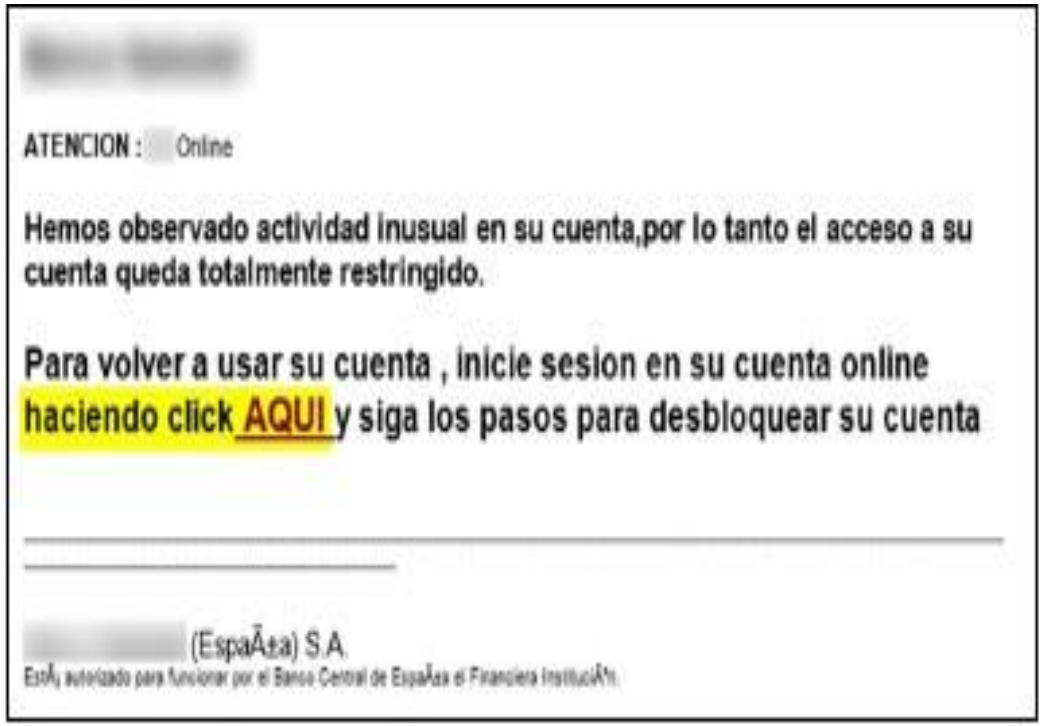
¿CÓMO NOS PUEDEN ATACAR? VECTORES DE ATAQUE

- Las amenazas a nuestra tienda online utilizan bien el **factor humano** bien el **fallo tecnológico** o una **combinación de ambos**.
- En cuanto al **factor humano**, se aprovechan de la ingenuidad o de la buena disposición de las personas para conseguir lo que quieren.
- En cuanto a los **fallos tecnológicos** (del software o de su configuración), son en muchos casos fallos conocidos, que no están parcheados o no se protegen correctamente.

¿CÓMO NOS PUEDEN ATACAR? FORMAS DE ATAQUE

FORMAS DE ATAQUE
ATAQUES DE INGENIERÍA SOCIAL: ¿SABES IDENTIFICARLOS?

FORMAS DE ATAQUE
INGENIERÍA SOCIAL: MENSAJES DE PHISHING Y SPEAR PHISHING



FORMAS DE ATAQUE
FALLO TECNOLÓGICO: PHISHING A NUESTRA WEB

¡Mi página web está suplantando a una entidad bancaria!

FORMAS DE ATAQUE
FALLO TECNOLÓGICO: PHISHING A NUESTRA WEB

FORMAS DE ATAQUE FALLO TECNOLÓGICO: INYECCIÓN SQL

FORMAS DE ATAQUE
FALLO TECNOLÓGICO: FALSIFICACIÓN – CROSS SITE SCRIPTING (XSS)

Qué permiten:

- Robo de **cookies de sesión** (las del carrito de la compra en tiendas online p. ej.) para capturar la sesión del usuario y:
  - cambiar su contraseña
  - realizar compras en su nombre
  - fisgar sus datos financieros y transacciones
- Ejecución de **código** malicioso.
- Dirigir al usuario hacia **páginas fraudulentas** para robarles las credenciales de acceso a su banco o pasarelas de pago.

FORMAS DE ATAQUE FALLO TECNOLÓGICO O INGENIERÍA SOCIAL: DEFACEMENT

Qué persiguen:

- Publicidad
- Desprestigiar o dañar la imagen de una organización

FORMAS DE ATAQUE
ATAQUES A NUESTRA IDENTIDAD Y REPUTACIÓN ONLINE

¿QUÉ ES IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE?

La **identidad digital** corporativa puede ser definida como el conjunto de la información sobre una empresa expuesta en Internet (datos, imágenes, registros, noticias, comentarios, etc.) que conforma una descripción de dicha organización en el plano digital.

¿QUÉ ES IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE?

- la **reputación corporativa** es el concepto que mide cuál es la valoración que hace el público de una compañía. Esta definición es trasladable al mundo de Internet y a la Web Social o Web 2.0, donde aparece la idea de reputación online corporativa.
- La **reputación online** puede definirse como la valoración alcanzada por una empresa a través del uso, o mal uso, de las posibilidades que ofrece Internet.

¿CÓMO GESTIONAR NUESTRA IDENTIDAD Y REPUTACIÓN ONLINE?

- Para gestionar adecuadamente nuestra **identidad** y monitorizar nuestra **reputación online**, debemos tener en cuenta estas situaciones que pueden influir negativamente:
- la utilización no consentida de nuestra marca;
- **cybersquatting** y **typosquatting** o el registro abusivo de nombre de dominio (y extorsión);
- publicaciones por terceros de **informaciones negativas;**
- **fuga de información** con repercusiones legales;
- suplantación de identidad con **phishing** y **pharming** (redireccionan a páginas que suplantan al original);
- **ataques de denegación de servicio.**

WEBS y TIENDAS ONLINE: LA SEGURIDAD CLAVE PARA LA SUPERVIVENCIA DEL NEGOCIO

- **La ciberseguridad es clave para la supervivencia del negocio en el entorno digital:**
- Identidad y reputación: nuestra imagen está en juego.
- Generar confianza:
  - proteger las transacciones
  - respetar la privacidad y los derechos de los consumidores
- Evitar fraude online, la fuga de datos, quedar fuera de servicio, daños de imagen, sanciones legales,…

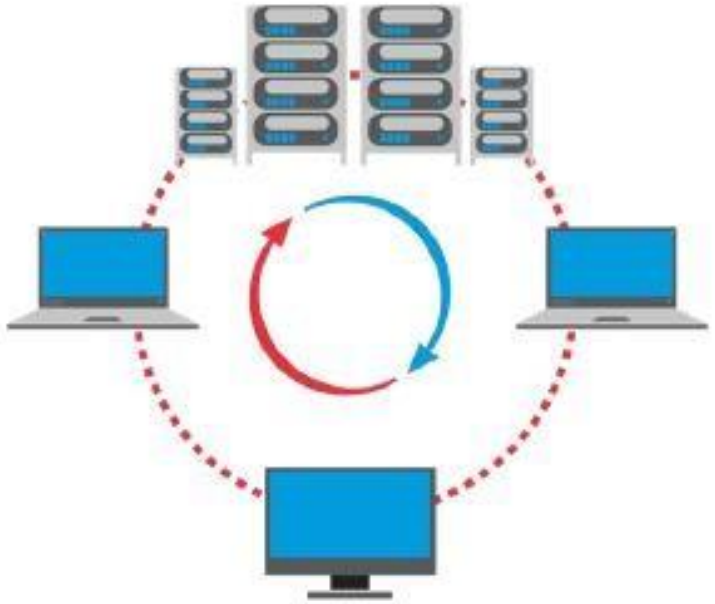
¿CÓMO GENERAR CONFIANZA?

- Cumpliendo con la **legislación**.
- Ofreciendo **interfaces de acceso** y **comunicaciones seguras** para autenticación y transacciones.
- Garantizando la **confidencialidad de los datos** recibidos.
- Manteniendo la **disponibilidad de los servicios.**
- Mostrando nuestro **compromiso** con la seguridad.

2. CONTRATANDO EL DESARROLLO Y EL ALOJAMIENTO

- La selección de proveedores TIC ha de hacerse siempre, además de con criterios económicos, de calidad y de funcionalidad, con **criterios de seguridad**.
- El desarrollador de nuestra web o el proveedor de servicios de alojamiento web deben demostrarnos su **compromiso** con la seguridad.
- **Nosotros** debemos exigirlo.
- La **seguridad** incluye aspectos como:
- La **confidencialidad**, **integridad** y **disponibilidad** (evitar ataques, backup,…)
- El **control de acceso** (quién tiene acceso a qué)
- **Aspectos legales** (dónde estarán mis datos)

ALOJAMIENTO WEB ¿QUÉ TENEMOS QUE EXIGIR Y COMPROBAR?



- Si utilizamos un servicio de **alojamiento externo** comprobaremos que los **acuerdos/contratos** incluyen:
- Aspectos relativos a **confidencialidad de los datos**
- **Copias de respaldo**
- **Actualizaciones** (parcheado) del software
- **Interfaces y comunicaciones** seguras para el administrador
- **Auditorías externas** para verificar la seguridad de la web

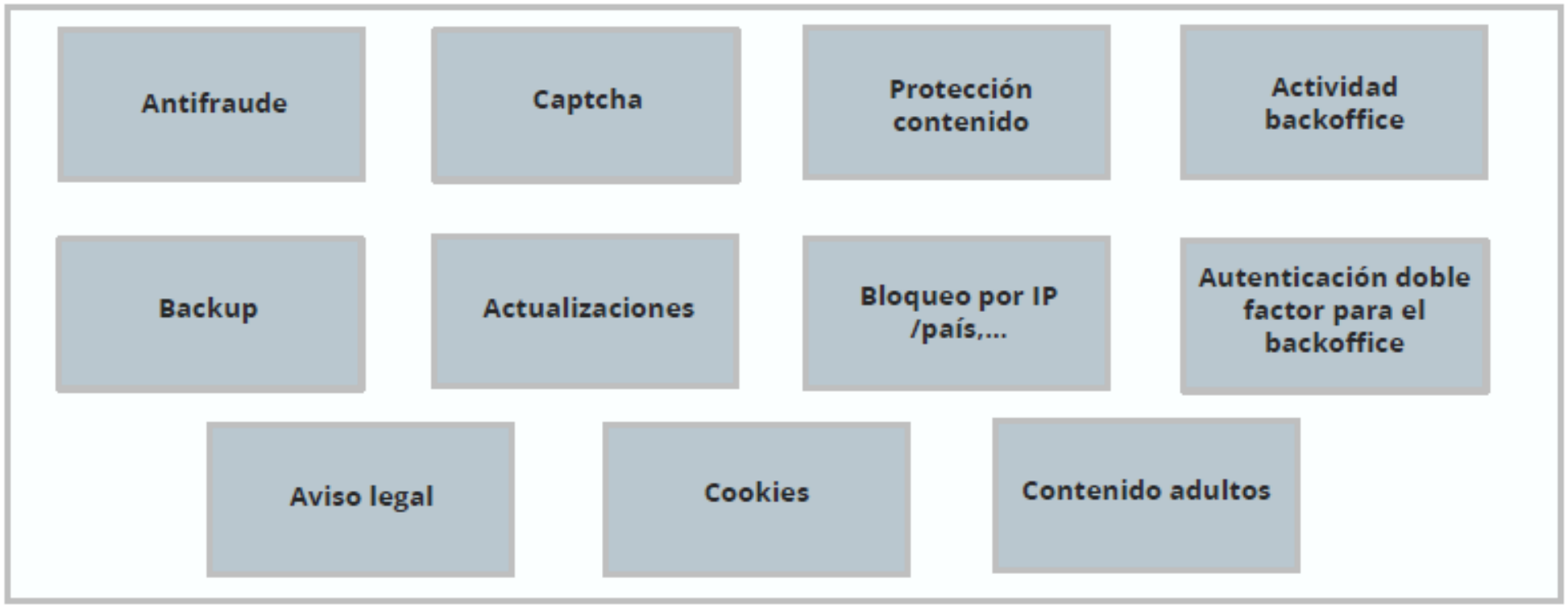
ALOJAMIENTO WEB ¿QUÉ TENEMOS QUE PREGUNTARLES?

- Y si quiero **migrar** a otro proveedor, ¿cómo **volcaré mis contenidos**?
- ¿Es el servicio **escalable**? (almacenamiento y ancho de banda)
- ¿Cómo es el **panel de administración o backend**?, ¿cómo protegen los **accesos lógicos**?
- Y el **servicio técnico**, ¿es telefónico o por email?, ¿en mi idioma?, y ¿qué horario?
- Hacen **backups**, instalan las **actualizaciones**, **certificados**, **antivirus**,…¿Cómo lo verifico?
- ¿Cómo podemos **monitorizar el servicio** (logs)?
- ¿En qué **país** se alojará mi tienda online?

DESARROLLO WEB
SI NOS HACEN LA WEB, ¿QUÉ TENEMOS QUE COMPROBAR? X

- Que se tienen en cuenta **los requisitos de seguridad** desde el principio.
- Que utilizan **prácticas y metodologías de desarrollo seguro** (como **OWASP** y **SAMM**).
- **Si auditan** el código.
- Que desarrollan en **sistemas actualizados.**
- Que **separan entornos de producción y desarrollo.**

MÓDULOS / EXTENSIONES ¿QUÉ TIPOS DE MÓDULOS DE SEGURIDAD PUEDO INCLUIR?



3. ¿CÓMO CUMPLO CON LA LEY?

Asociación Colombiana de la Propiedad Intelectual

Habeas Data

El derecho constitucional que tienen todas las personas a :

Conocer
Actualizar
Rectificar

→ Las informaciones que se hayan recogido sobre ellas en bases de datos o archivos

Derecho a la Información: ART. 20. Se garantiza a toda persona la libertad de (...) informar y recibir información veraz e imparcial (...)

¿QUÉ BENEFICIOS TIENE CUMPLIR LA LEY?

Beneficios de cumplir la ley:

- evitaremos sanciones;
- evitaremos tener problemas con terceros;
- generamos confianza en nuestros clientes;
- nuestra imagen mejora.

4. COMUNICACIONES Y MEDIOS DE PAGO ¿SEGUROS?

- En nuestra empresa hemos comprado un dominio, tenemos una marca elegante y atractiva. Nuestra tienda online o nuestra web está preparada para publicarse con toda su funcionalidad. Ahora debemos conseguir que nos conozcan y que **nos reconozcan**. Veremos que esto último se hace comprando un CERTIFICADO para nuestro dominio.
- Además en Internet, las comunicaciones e intercambios electrónicos que **no se protegen adecuadamente** pueden ser **interceptados** y **manipulados**. Para ello tendremos que **CIFRAR** las comunicaciones. Tenemos pues que **garantizar la seguridad de todas las comunicaciones** y en particular de los pagos. Si tenemos una tienda online tendremos que elegir **MÉTODOS DE PAGO FIABLES** (para que los compradores confíen en nosotros para comprar).

¿CÓMO HACEMOS QUE LAS COMUNICACIONES SEAN SEGURAS?
CERTIFICADOS

- Un certificado se asocia a un dominio web por una **Autoridad de Certificación** que **AUTENTICA que somos quienes decimos ser** (aparece un candado en la barra de navegación). Como usuarios debemos saber que los ciberdelincuentes también utilizan webs con certificados por lo que cuando navegamos debemos **verificar** (en la barra del navegador) que la web tiene certificado y las comunicaciones están cifradas (candado y HTTPS://) y que el **titular del certificado es quien debe ser.**

¿CÓMO HACEMOS QUE LAS COMUNICACIONES SEAN SEGURAS? NIVELES DE SEGURIDAD PARA LOS CERTIFICADOS

Existen dos niveles de seguridad fundamentales para los certificados emitidos por AUTORIDADES DE CERTIFICACIÓN:

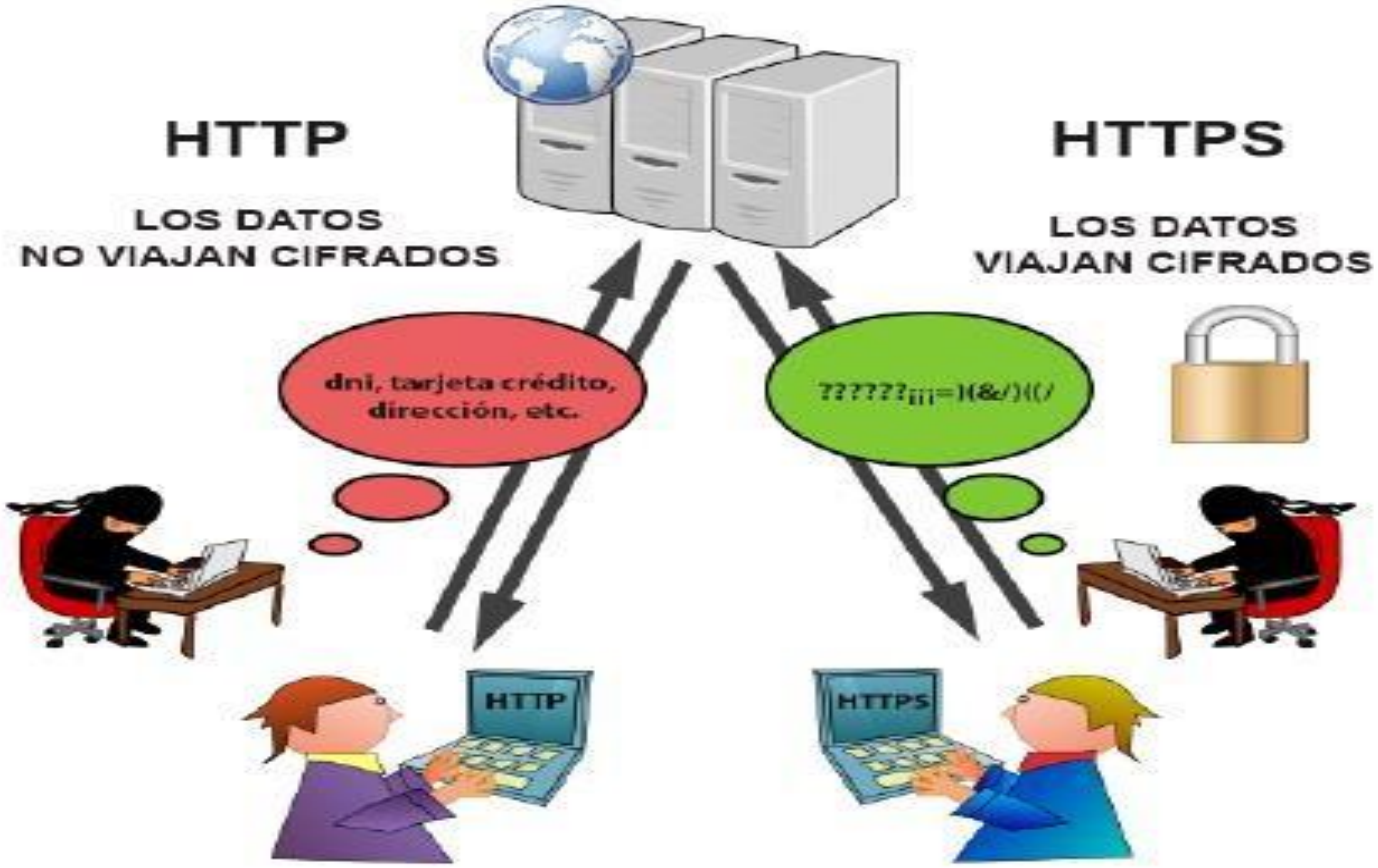
- **SSL sin EV** o **sin validación extendida:** el dominio está **certificado,** aparece un candado en la barra de navegación, pero **no se verifica que la web pertenece a una entidad real**.
  - El usuario no recibirá ninguna alerta de que el certificado no es confiable, pero si inspecciona la información de seguridad en su navegador **no podrá asegurar que dicho dominio pertenece a una organización real**.
- **SSL con EV con validación extendida:** el sello de Validación Extendida se obtiene en base a una **certificación internacional de gestión de certificados y seguridad** que se expide, previa auditoría, de las autoridades de certificación.
  - El usuario podrá comprobarlo en su la barra de navegación de su navegador pues aparece el **nombre de la entidad y el candado en color verde**. La autoridad de certificación ha comprobado físicamente, mediante auditoría, que somos los verdaderos propietarios de esa web.

¿CÓMO HACEMOS QUE LAS COMUNICACIONES SEAN SEGURAS?

Requisitos de las COMUNICACIONES SEGURAS:

- **Confidencialidad o privacidad:** que sea ilegible para terceros.
- **Integridad:** que no se pueda cambiar el contenido de lo enviado.
- **Autenticación:** con garantías de que los participantes son quienes dicen ser.
- **No repudio:** que el destinatario no pueda negar que lo ha recibido

¿CÓMO HACEMOS QUE LAS COMUNICACIONES SEAN SEGURAS?: CIFRADO



¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO?

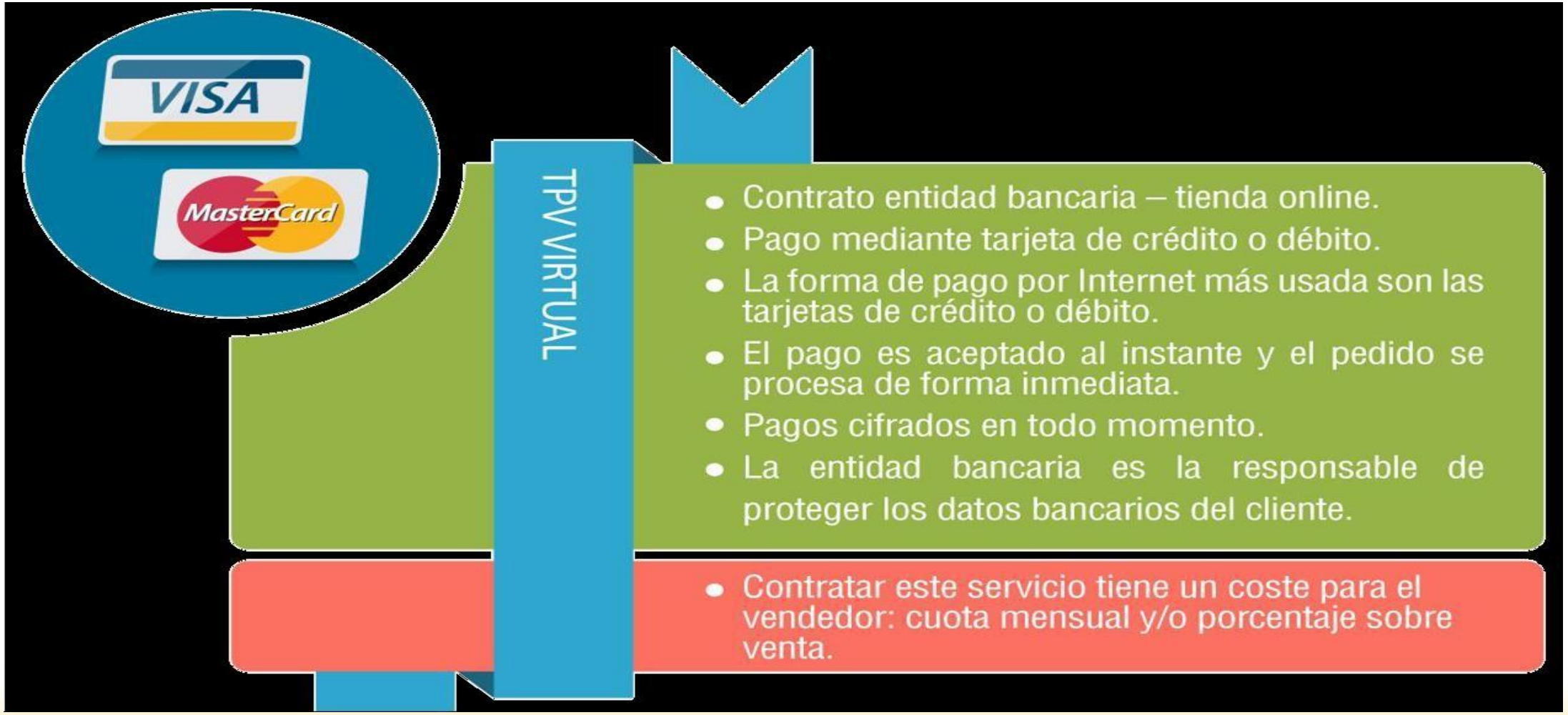
En cuanto a la selección de **medios de pago para nuestra web,** tendremos que considerar:

- Preferir aquellos en los que **NO** tengamos que tomar **datos bancarios ni de autenticación de las tarjetas de pago de nuestros clientes**.
- Que las **comunicaciones** hacia nuestros clientes y hacia el proveedor **utilicen protocolos seguros (SSL).**
- Que el proveedor de la pasarela o del TPV virtual cumpla la normativa para medios de pago online (PCI-DSS).
- **Que ofrezcan otras garantías para el cliente** (devoluciones, seguros,…)

¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO?

- **MEDIOS DE PAGO :**
- **Pago electrónico:**
- con tarjeta (TPV Virtual)
- sin tarjeta (Pago con intermediario)
- Transferencia (externo, no es a través de nuestra web).
- Contra reembolso (no es electrónico).

¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO? PAGO ELECTRÓNICO CON TARJETA



¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO? PAGO ELECTRÓNICO CON TARJETA

Tipos de TPV Virtual o PAGO DIRECTO CON TARJETA:

TPV o PASARELA SET (es segura)

- Está poco extendida.
- Utiliza **certificados, firmas y cifrado**, es decir garantiza autenticación, **confidencialidad, integridad y no repudio.**

TPV o PASARELA SSL (cifrado) garantiza el **secreto en las comunicaciones y la integridad de los datos** transmitidos. Existen tres tipos:

- **Lineal (no es segura)**
  - El cliente cumplimenta un formulario online con los datos necesarios para efectuar la compra y el pago.
  - **El vendedor tiene acceso a los datos del cliente** lo que hace posible el fraude.
- **Triangular (algo más segura)**
  - Redirige al cliente a la entidad bancaria.
  - El banco sólo conoce la transacción y el vendedor sólo conoce los productos.
- **De tres dominios (la más segura)**
  - Como la triangular pero con **autenticación previa del cliente** que realiza la entidad emisora que le asigna un código privado cuando se registra. Algunos servicios de autentificación son **Verified by Visa** y **MasterCard SecureCode**.
  - **Autenticación del servidor** lo que ofrece más garantías al comprador.

¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO?
PAGO ELECTRÓNICO SIN TARJETA

¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO? PAGO ELECTRÓNICO SIN TARJETA

¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO? PAGO ELECTRÓNICO SIN TARJETA

¿CÓMO SELECCIONAMOS LOS MEDIOS DE PAGO? PAGO ELECTRÓNICO SIN TARJETA

5. ¿CÓMO ASEGURO MI SERVIDOR Y MI CMS?

¿CÓMO PROTEJO MI WEB?: DEBILIDADES Y PRINCIPIOS DE SEGURIDAD

DEBILIDADES DE LAS PÁGINAS WEB

SISTEMA

- Software desactualizado
- Autenticaciones débiles
- Servicios innecesarios
- Cifrados débiles

SERVIDOR

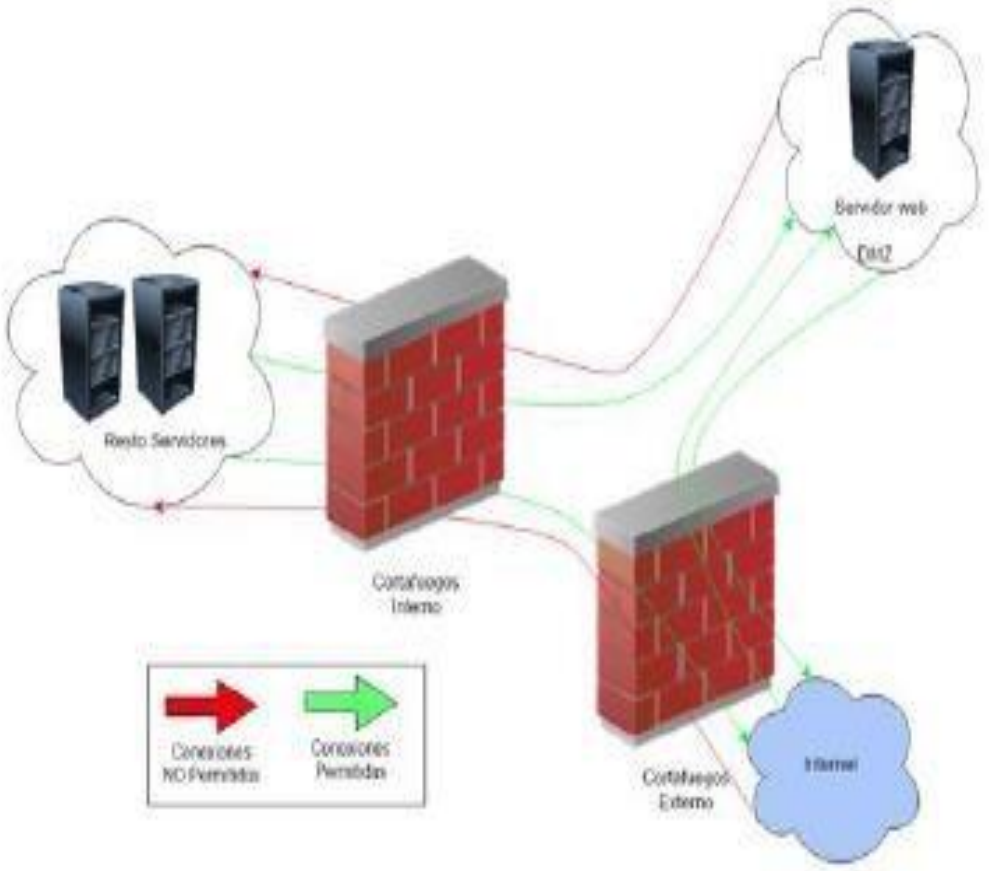
- Autorización incorrecta
- Exposición de información
- Funcionalidades no controladas
- Seguridad por defecto

APLICACIÓN

- Parámetros no controlados
- Lógica de negocio no controlada
- Abuso de valores por defecto
- Prácticas de desarrollo inseguras

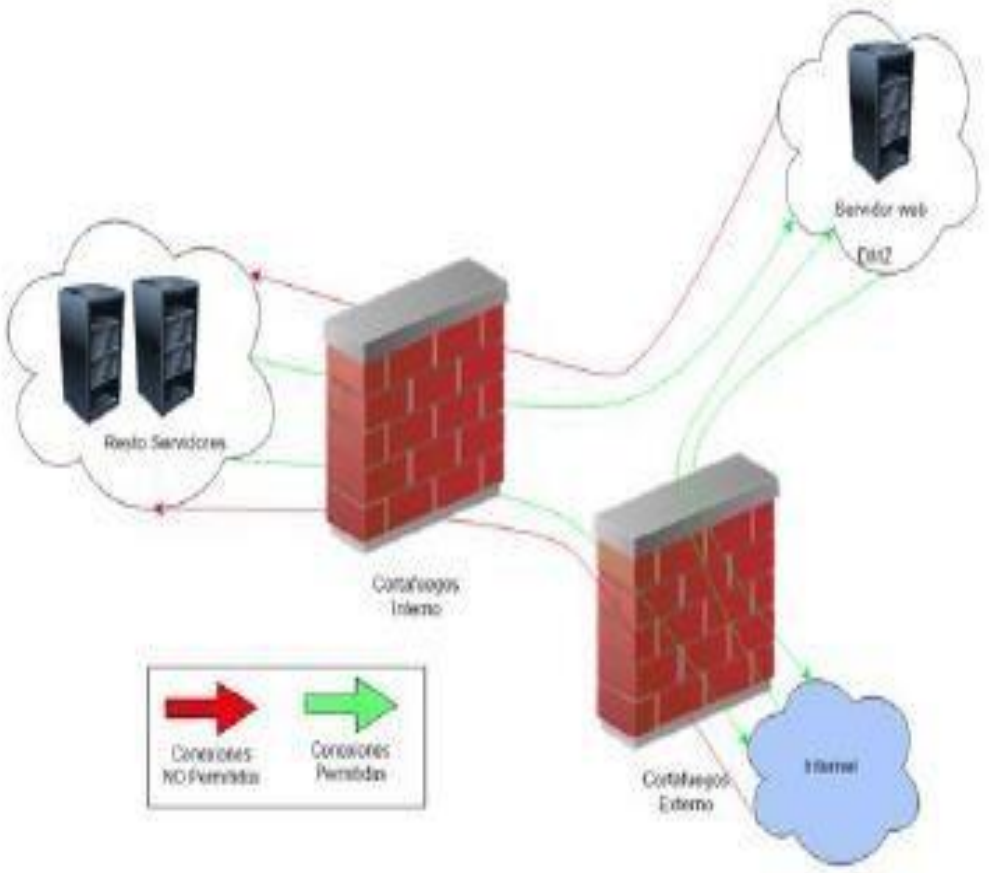
MEDIDAS DE SEGURIDAD PARA EL SERVIDOR

- **Actualizar** el software y realizar **backups.**
- Instalar **certificados** SSL.
- Eliminar usuarios por defecto.
- Ocultar información sobre el sistema.
- Instalar el servidor en una **DMZ** (zona desmilitarizada).
- **Deshabilitar** los servicios y puertos que no se utilicen.

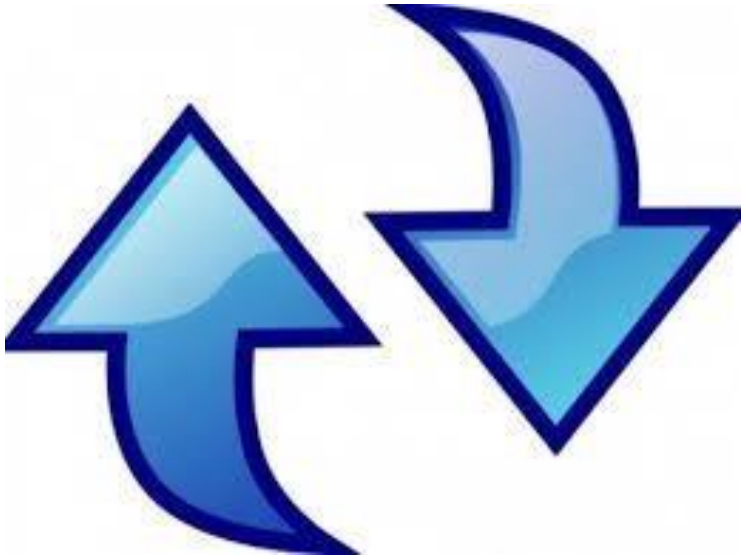


MEDIDAS DE SEGURIDAD PARA EL SERVIDOR

- Protegerlo con un **cortafuegos**, **IDS/IPS** y contra el **malware.**
- Establecer límites a privilegios de los usuarios. Reducir los permisos de acceso a los archivos y directorios.
- Limitar el número de peticiones concurrentes (evitar ataques DoS) que se le pueden realizar.
- **Monitorizar** el uso de los recursos y guardar los registros (logs).



MEDIDAS DE SEGURIDAD PARA EL GESTOR DE CONTENIDOS



- **Actualizar** el software del CMS y los complementos.
- Realizar **backups** y comprobarlos.
- Realizar **auditorías** externas.

MEDIDAS DE SEGURIDAD PARA EL GESTOR DE CONTENIDOS

- **Deshabilitar** los módulos que no se utilicen.
- Proteger al **administrador** (contraseñas fuertes y cambios frecuentes de contraseña, doble factor de autenticación,...).
- Utilizar **comunicaciones seguras** para administradores y usuarios.
- Eliminar usuarios por defecto y el directorio de instalación.
- Cambiar el nombre del usuario «admin» y el prefijo de la base de datos.
- Utilizar **CAPTCHAS** en los formularios (evitar spam).
- Eliminar metadatos de los documentos e imágenes.
- Vigilar los cambios en los contenidos y los accesos al *backend*.

6. EN LAS OPERACIONES DE CADA DÍA ¿CÓMO GARANTIZO LA SEGURIDAD?

OPERACIONES DE CADA DÍA ¿QUÉ DEBO COMPROBAR?

- que tenemos copias de seguridad y que sabemos restaurarlas;
- que no ha habido modificaciones no controladas de los contenidos;
- que no hay fraudes en los pagos/compras;
- quién accede al CMS y qué permisos tiene;
- que se cambian las contraseñas y que son fuertes (de usuarios yadministradores);
- que no hay variaciones en las analíticas de tráfico SEO (si no hemos hecho una campaña);
- que no recibimos opiniones negativas de clientes en redes sociales,
- que estamos suscritos a los boletines de seguridad de los fabricantes del software que utilizamos (CMS, servidor, etc.)

COMPRAS FRAUDULENTAS
¿CÓMO DETECTAR UNA COMPRA FRAUDULENTA?

Si tenemos una tienda online, para detectar una posible **compra fraudulenta** debemos estar atentos a las siguientes situaciones:

- muchos clientes o muchas tarjetas de crédito **con la misma dirección de** entrega (mula);
- varios **intentos de compra erróneos** en el TPV (con distintas tarjetas) antes de que la operación sea aceptada;
- solicitud de **envío urgente** del pedido;
- un **gran pedido** por parte de un cliente;
- un cliente de un **país extranjero** si no hemos hecho publicidad allí.

7. EN CASO DE DESASTRE ¿QUÉ HAGO?

DETECTAR UN ATAQUE ¿CÓMO LO DETECTO?

- comprobar la **apariencia** y **funcionalidad** de la web;
- revisar los **sistemas de monitorización** y el log de conexiones http y ftp;
- comprobar desde que **IP** se han conectado vía **FTP;**
- comprobar el **listado de ficheros** en busca de **cambios:** directorios y subdirectorios, permisos, bases de datos, nuevos archivos, etc.
- comparar el **código fuente de la tienda** contra **copias de seguridad;**
- comprobar si hemos recibido alguna **notificación** de proveedores de servicios de alojamiento o de un tercero.

RESPUESTA A INCIDENTES ¿Y SI OCURRE LO PEOR?

En caso de sufrir un **incidente de ciberseguridad** que afecte a nuestra tienda online o a nuestra web, debemos adoptar las siguientes medias:

- poner **off-line** la tienda o la web y conectar con el **proveedor;**
- obtener una **copia de la web comprometida** (evidencia forense del ataque) y **guardar la cadena de custodia** para hacer una denuncia;
- **denunciar**, aportando las evidencias;
- pasar el **antivirus**, cambiar las **contraseñas** y **restaurar el servicio** con una copia de seguridad;
- comprobar si nuestra página web o dirección IP está en alguna **lista negra** y si es así **notificarlo** al proveedor.

CONTINUIDAD DE NEGOCIO
¿TIENES UN PLAN B?

La mejor forma de **evitar o sortear los incidentes, y sus consecuencias**, es conocer bien en qué **estado está nuestra seguridad** y hacia **dónde queremos dirigirnos** para mejorarla. Para conseguir este objetivo, debes poner en práctica los siguientes consejos:

- tener un **plan B** para activar en caso de desastre con **un procedimiento de actuación** (responsables, teléfonos,…);
- **disponer de copias de seguridad**, comprobadas y alojadas en un lugar separado;
- contratar un **sitio de respaldo** (en caso de estar sin nuestra web suponga grandes pérdidas para nuestro negocio).

8. ¡SI OFRECES SEGURIDAD, LA RECOMPENSA ES LA CONFIANZA!

FIN DE GRABACIÓN