C0R0N4CON DICIEMBRE 2020

SEGURIDAD EN EL COMERCIO ELECTRÓNICO OPEN SOURCE

QUIÉN SOY

Silvia Suria Torres, ingeniera técnica informática

Consultora independiente de comercio electrónico y plataformas de formación, con un librillo sobre el comercio electrónico, que podéis ver aquí: https://cutt.ly/GhOCkNk.

¡¡Formo parte de un equipo!!

PLATAFORMAS OPEN SOURCE

Un comercio electrónico es una gran responsabilidad

Fundamentalmente trabajo con

- Magento
- Woocommerce

Existen otras Open Source

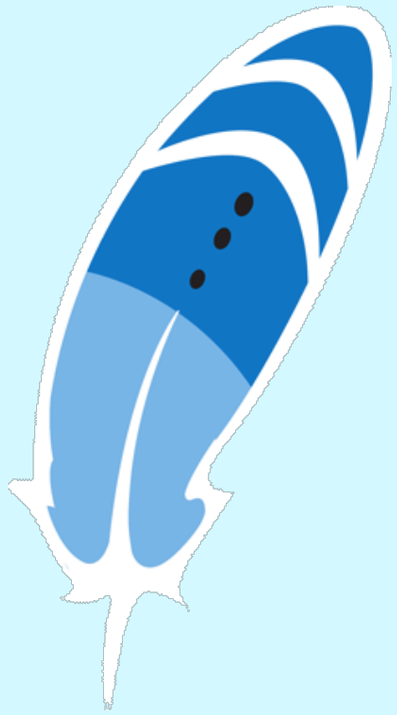
Las plataformas deben permitir una cierta independencia a su dueño y éste debe ser responsable y consecuente

El problema de las Open Source, que es virtud a la par:
los bugs se reportan públicamente

QUIÉN ES EL RESPONSABLE DE LA SEGURIDAD EN UN C.E.

El equipo de desarrollo

Los equipos satélites que acceden a la plataforma (marketing, responsables de producto)



El cliente final

El responsable de la tienda

El ISP (y sysadmins)

CÓMO HACER MÁS SEGURA LA EXPERIENCIA

Cliente final, dueño de la plataforma, equipos periféricos: antivirus, chequeo de tu seguridad, vigilando keyloggers, troyanos, phishing etc

No se instalan plugins sin el visto bueno del equipo de desarrollo.

Dueño de la plataforma: no elegir el ISP por lo barato de su servicio o por su nombre.

Elige siempre, personal cualificado para todas las tareas (desarrollo, marketing, sysadmin...).

CÓMO HACER MÁS SEGURA LA EXPERIENCIA

ISP: tener los servidores y firewalls al día. Definir medidas de contingencia, seguridad, actuación... ante ataques, monitorización de servidores...

Equipo de programación: **El core no se toca**. Estudiar un plugin antes de instalarlo. No confiar ciegamente en nuestro código propio, puede ser el eslabón más inseguro. No dejar códigos y plataformas en beta abiertas.

Dejar definido una política de backups (y restauración en caso de desastre total).

PARA TODOS: ¡¡¡FORMACIÓN!!!!

COMO EQUIPO DE DESARROLLO...

- **Seguridad**

Si estamos en un WC concretamente, podemos ayudar a la seguridad:

* Wordfence y otras herramientas
* Recaptcha invisible
* Akismet
* 2-Factor ID

Si estamos en un Magento, también existen herramientas de seguridad, como el factor de doble autenticación o recaptcha invisible. Se presupone un mayor control sobre el servidor y delegar más en el equipo sysadmin.

- **Buenas prácticas**

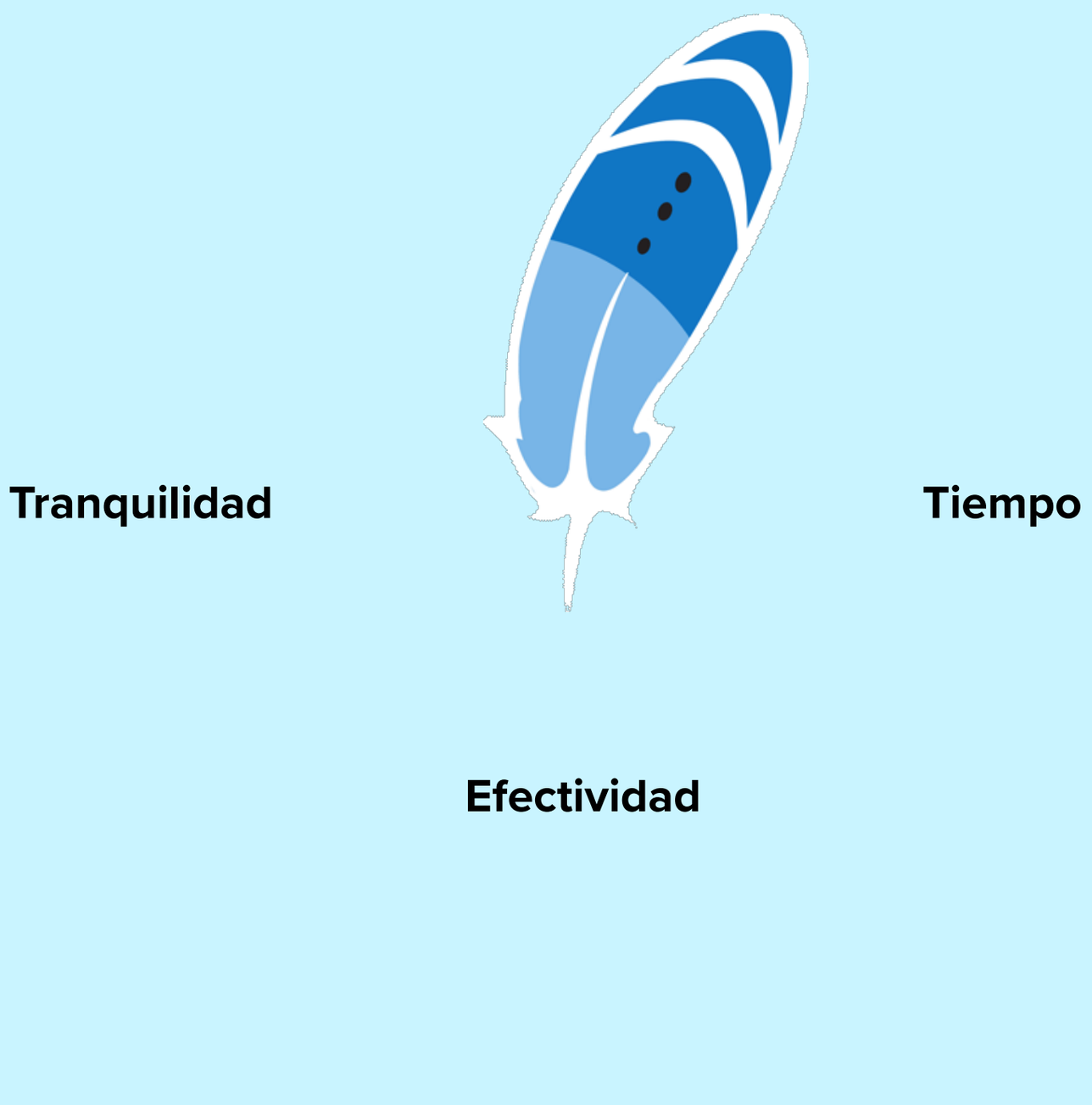
Hay un equilibrio entre código propio, plugins ajenos y el presupuesto.

Si la plataforma al entregarla queda sin mantenimiento exhaustivo, hay que tenerlo en cuenta.

No utilizar plataformas que no conocemos. Formación antes de empezar.

EL DESARROLLO DE UNA PLATAFORMA HA TERMINADO...

- Y ahora qué? Realmente nunca termina
- Prescindir por completo de cualquier equipo de desarrollo o sysadmin es un error
- Hay que asegurarse de backups y si es el caso, del correcto balanceo y sistema de alta disponibilidad
- Definir política de actualizaciones, contingencias ante desastres y ataques masivos.
- Chequeo periódico de bugs y vulnerabilidades



CÓMO DESCUBRO VULNERABILIDADES. ¿QUÉ HACER SI ME ATACAN?

- Desde el mantenimiento de la plataforma, se da este tipo de servicio
- Hay sites que te chequean servidores y plataformas, periódicamente o de forma puntual
- Ante una vulnerabilidad, hay que buscar la solución a la misma. Patches, actualizaciones, desactivación temporal del código donde está
- Ante un ataque, “keep calm and …” busca ayuda si no sabes qué hacer
- Muchas veces, el propio ISP tiene medidas de contención
- Estudiar cómo es el ataque, si atacan a una vulnerabilidad, a un problema del servidor, o es algo genérico

DATOS DE CONTACTO

Puedes ponerte en contacto con nosotros a través de los siguientes medios:

- 657092970
- info@esencialsistemas.com

https://ecurriculum.es/silvia-suria-torres

https://www.linkedin.com/in/silvia-suria-torres/

FORMACIÓN INTEGRADA

Plataforma de profesionales para profesionales

Queremos compartir lo que hemos ido aprendiendo

formacionintegrada.com/elige-tu-formacion