



Mi sitio Web ha sido hackeado ¿y ahora qué?

Carlos Solís Salazar

Profesor/Investigador - CUFM

Leader Chapter - OWASP Venezuela

carlos.solis@owasp.org

@csoliss

Un Código Seguro

es como una poceta...



Limpia,
compacta,
no hay fugas,
se ocupa de cualquier mi...,
y todavía se mantiene limpia.

Zappos
•com

The Zappos logo consists of the word "Zappos" in a large, bold, black sans-serif font. Below the "os" part of "Zappos" is a blue rounded rectangle containing a white dot followed by the text ".com" in white. To the right of the ".com" is a blue icon of a shoe, viewed from the side, with a white sole and a white lacing pattern.



**PLAYSTATION®
Network**

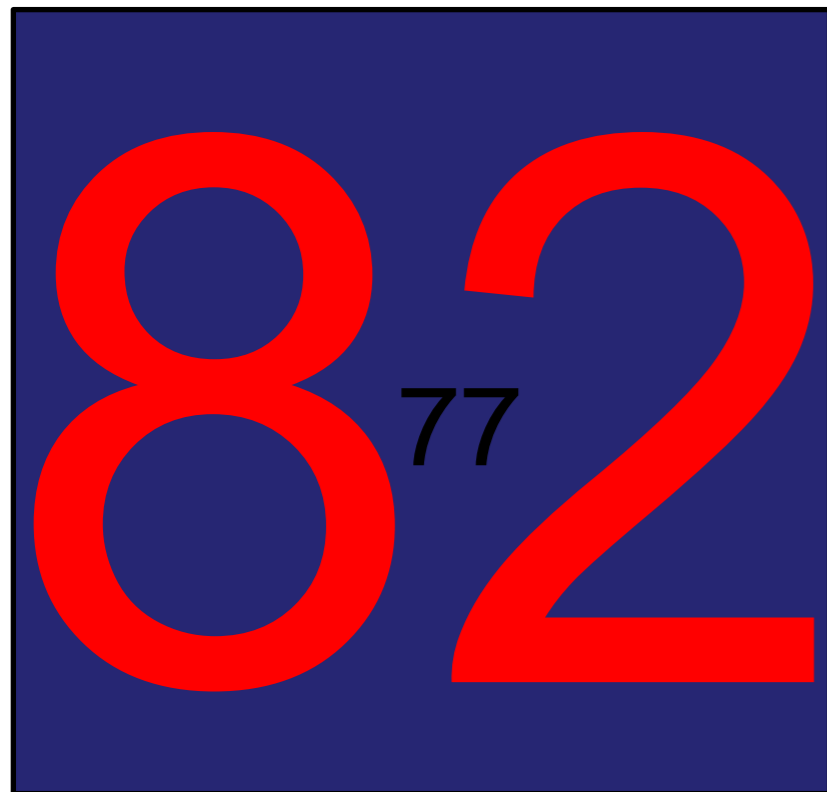






Algunos datos interesantes

2011

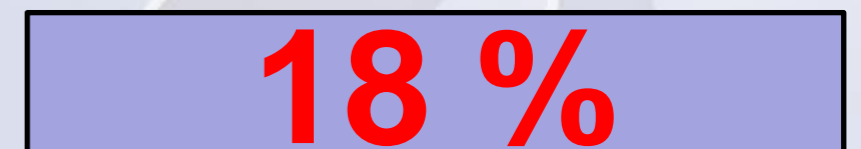



**Ataques
dirigidos
diarios**

Empresas
> 2500
Personas

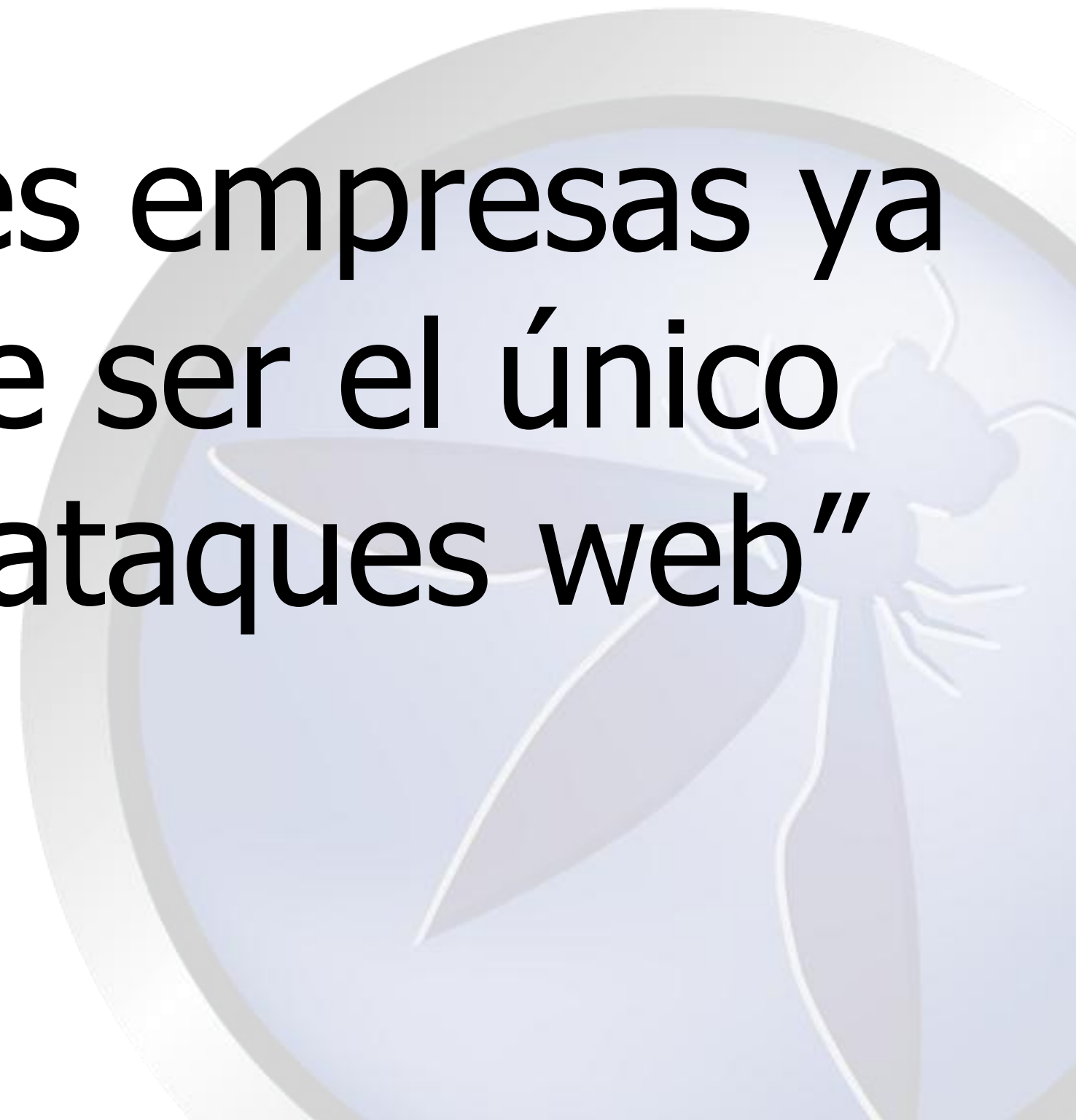


Empresas
> 250
Personas





“Las grandes empresas ya dejaron de ser el único vector de ataques web”





¡QUÉ DESASTRE!
¡LO HEMOS PER-
DIDO TODO!

MENOS MAL, JEFE, QUE
TOMÉ LA PRECAUCIÓN
DE FOTOCOPIAR EL DIS-
CO DURO.



BACHILLERATO GENERAL COLEGIO ISABEL LA CATÓLICA
 REPORTE DE EVALUACIÓN PARCIAL Y FINAL
 CICLO ESCOLAR 2009 - 2010

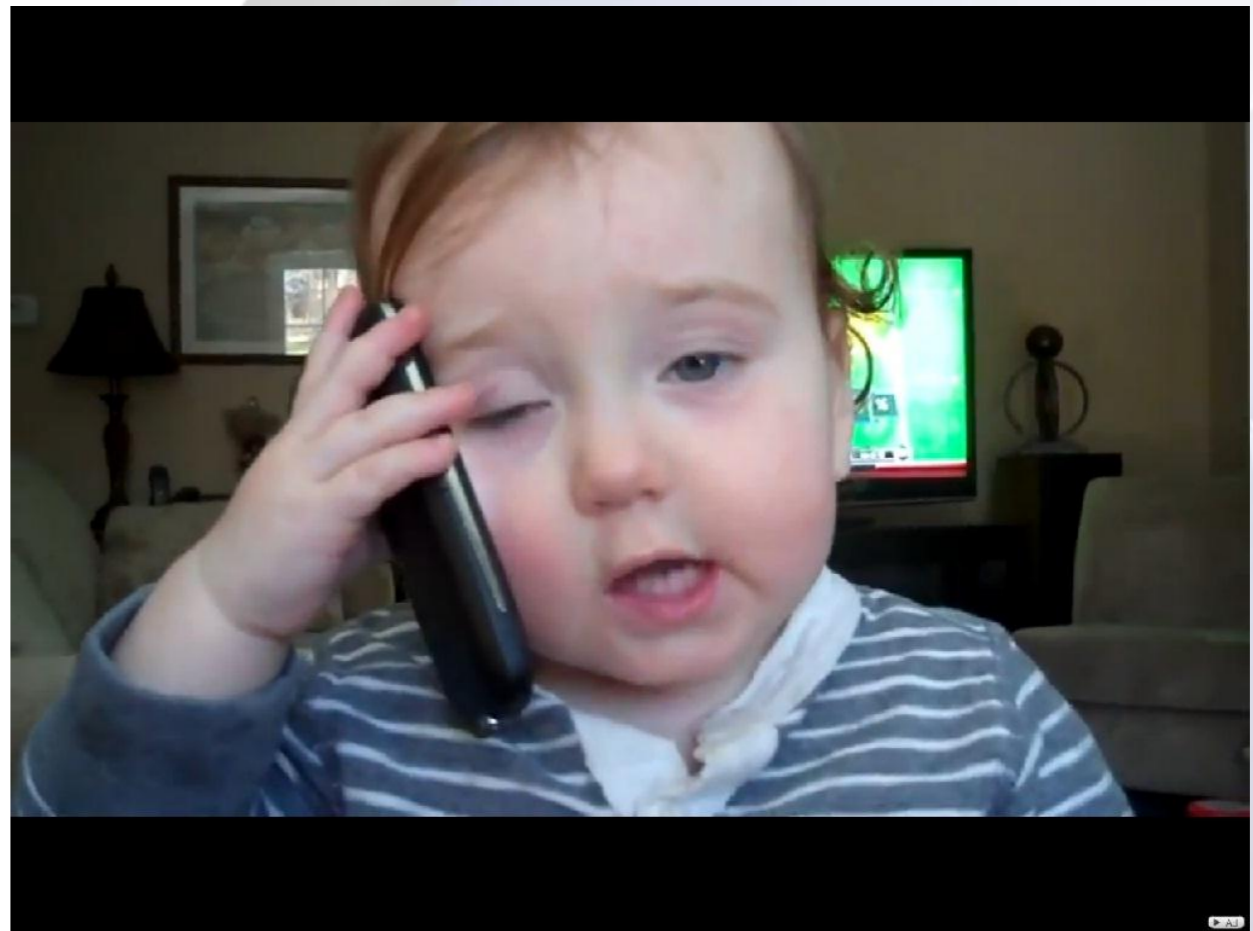


NOMBRE: PAGES CAHUANTZI VANTA SAIDY						No. 29						
TERCER SEMESTRE						CUARTO SEMESTRE						
EVALUACIÓN	SEPT.	OCT.	NOV.	DIC.	CALIFICACIÓN FINAL	OBSERVACIONES	EVALUACIÓN	FEB.	MAR. ABRIL.	MAY. JUN.	CALIFICACIÓN FINAL	OBSERVACIONES
ASIGNATURA							ASIGNATURA					
GEOM. ANALÍTICA Y FUN.	10	10	10	10	10		CALCULO	10				
TALLER DE LECT. Y RED. III	9	10	10	10	10		TALLER DE LECT. Y RED. IV	10				
HISTORIA DE MÉXICO I	10	10	10	10	10		EST. SOCIOECONÓMICA DE MEX.	10				
ORI. VOCACIONAL	10	10	10	10	10		BIOLOGÍA I	10				
FISICA I	10	10	10	10	10		FÍSICA II	10				
INFORMATICA	10	10	10	10	10		APLIC. INFORMÁTICA	10				
INGLES III	9	10	10	10	10		INGLES IV	10				
CONTABILIDAD BÁSICA	10	10	10	10	10		CONTABILIDAD FINANCIERA	10				
ADMINISTRACIÓN I	10	10	10	10	10		ADMINISTRACIÓN II	10				
QUÍMICA	10	10	10	10	10		QUÍMICA	10				
EDUCACIÓN FISICA	10	10	10	10	10		EDUCACIÓN FÍSICA	10				
FORMACIÓN EN VALORES	10	10	10	10	10		FORMACIÓN EN VALORES	10				
EDUCACIÓN EN LA FE	9	9	9	9	9		EDUCACIÓN EN LA FE	9				
HÁBITOS PERSONALES	10	10	10	10	10		HABITOS PERSONALES	10				
INASISTENCIAS HORA/CLASE							INASISTENCIAS HORA/CLASE					
FIRMA DEL PADRE O TUTOR	OCT. - NOV.		DIREC.				FEB.	MAY. - JUN.		DIREC.		
SEPT.	DIC.						MARZO - ABRIL					

Activar
registros
de sistemas



Cifrado de datos sensibles



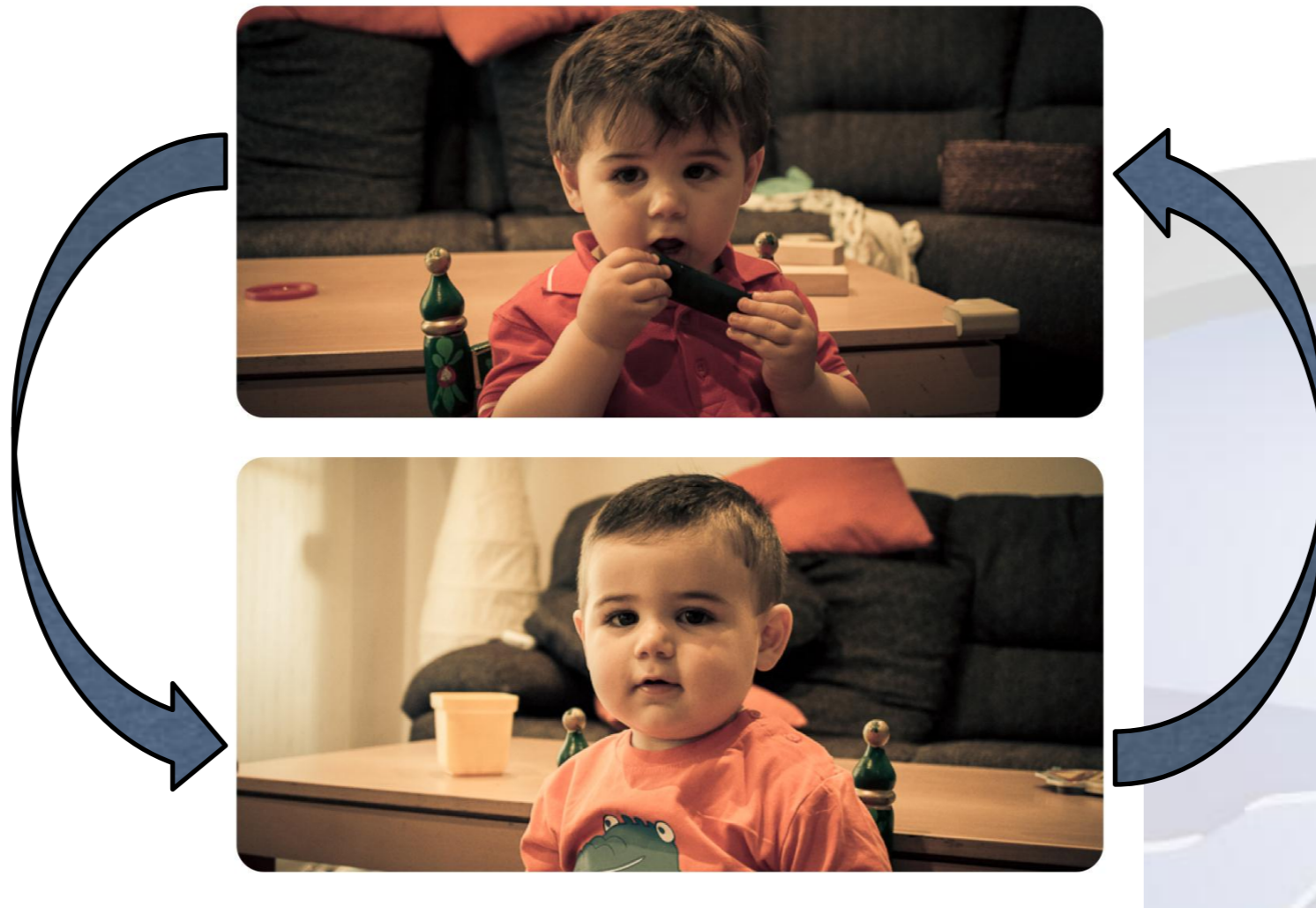
Análisis de vulnerabilidades





Proteger los Endpoints

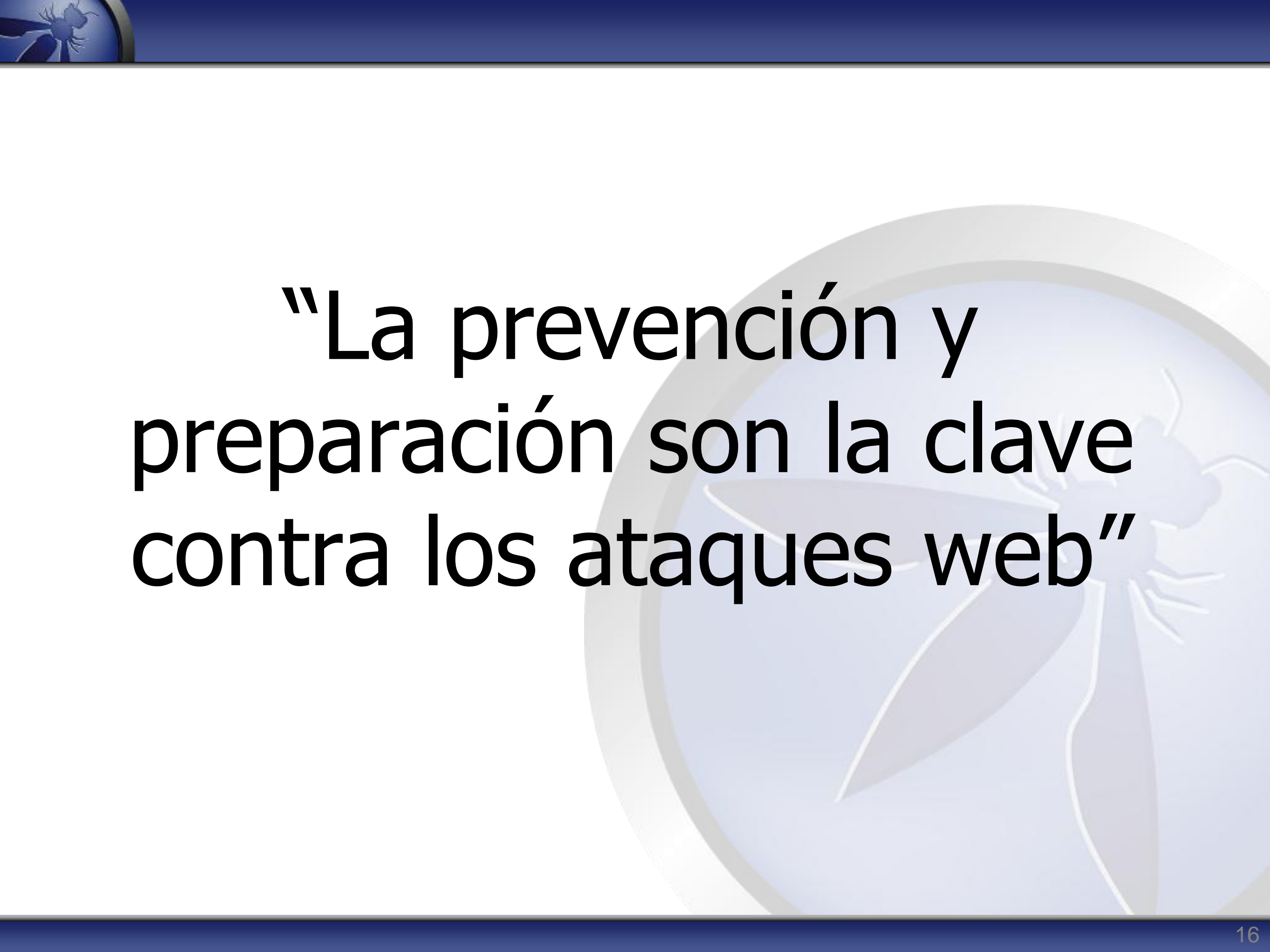




Actualizaciones críticas



Educación al personal

The slide features a dark blue header and footer. The main content area is white with a large, faint, light blue circular graphic on the right side. Inside this circle is a stylized dragonfly. The text is centered and reads:

“La prevención y preparación son la clave contra los ataques web”

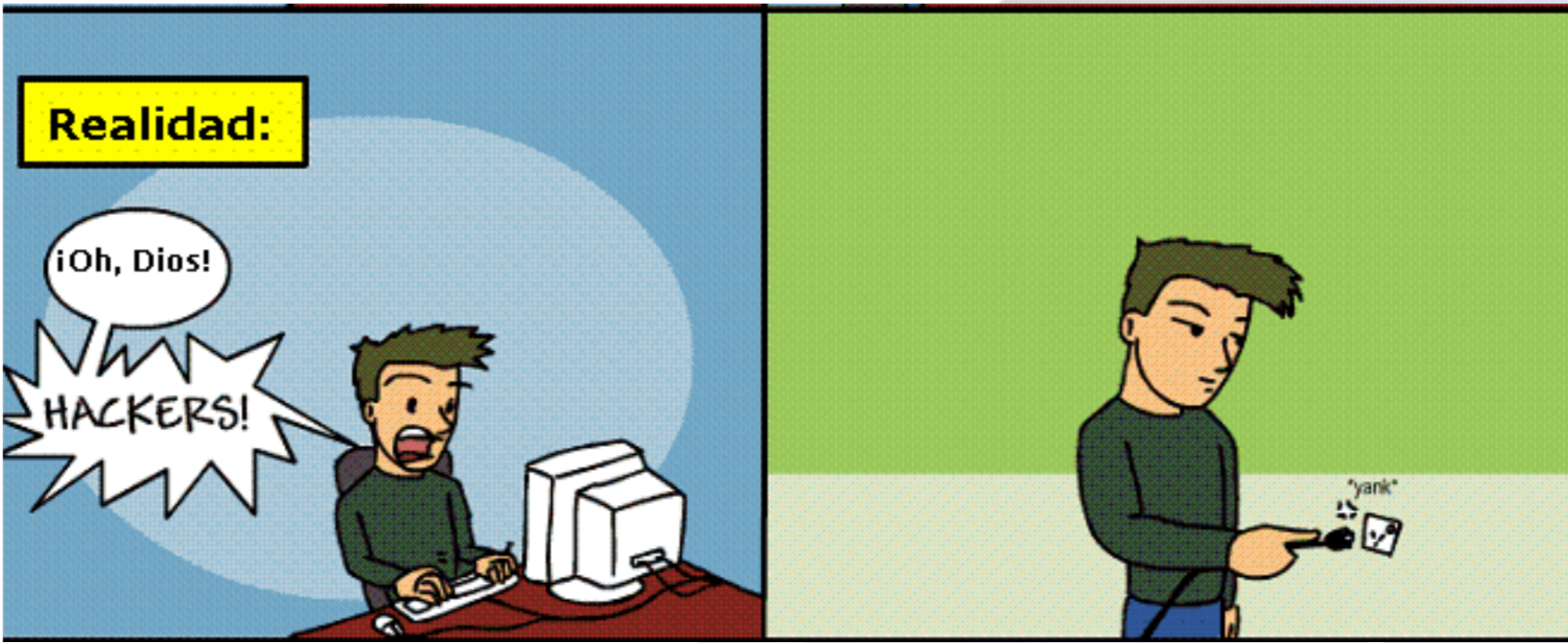
-Bueno, tendré que poner otra ruta para los cifrados... Para ello pondré un algoritmo genético que proteja el kernel del ordenador.

-Hackers!!! Oh no, han logrado entrar a través del proxy y del firewall.

-¡No! Él está corrompiendo la base de datos, tengo que.....

-iiiEl troyano no está funcionando!!! ¡Quizás con un password secundario de configuración!.







**Evidentes
cambios (y
no tanto) del
sitio web**

Mensajes de advertencia




Anomalías FTP y HTTP




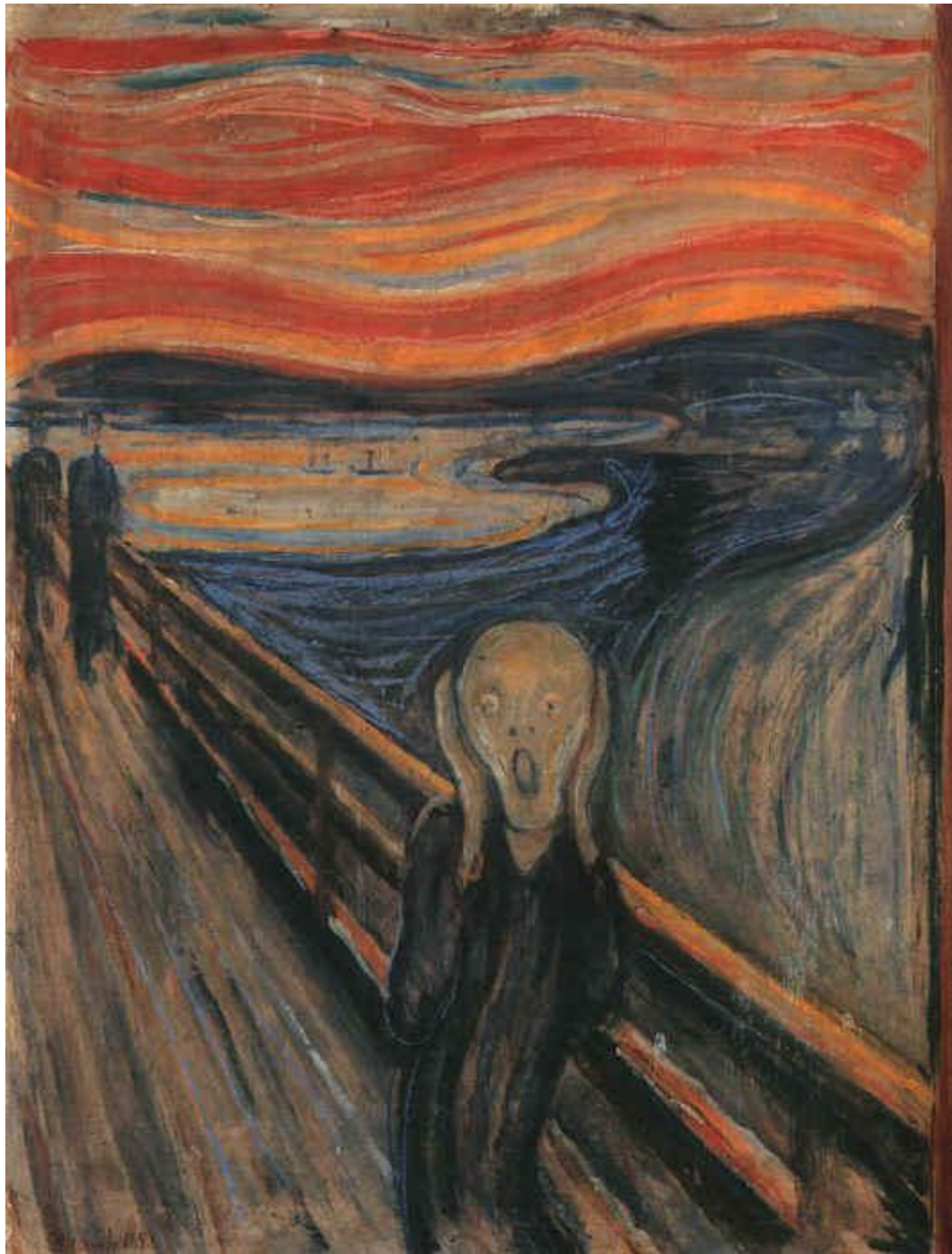


**Código sospecho en
los archivos web**



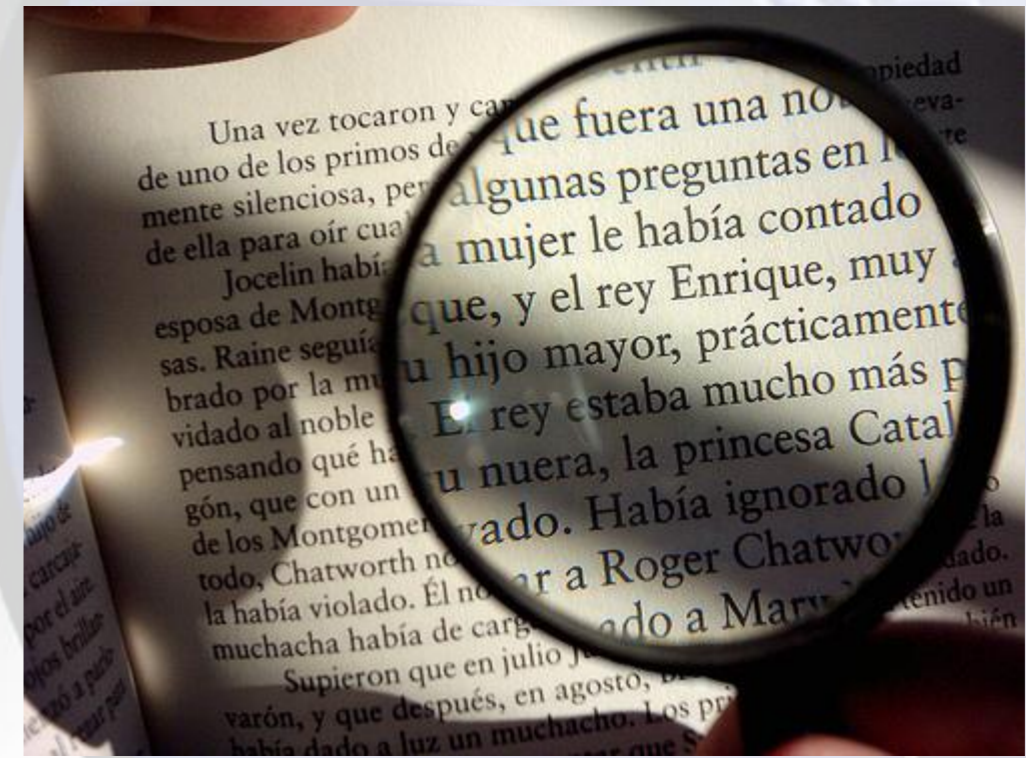
**“Contar con personal
especializado en
monitoreo y gestión”**





No entrar
en pánico

Revisar registros de sistemas

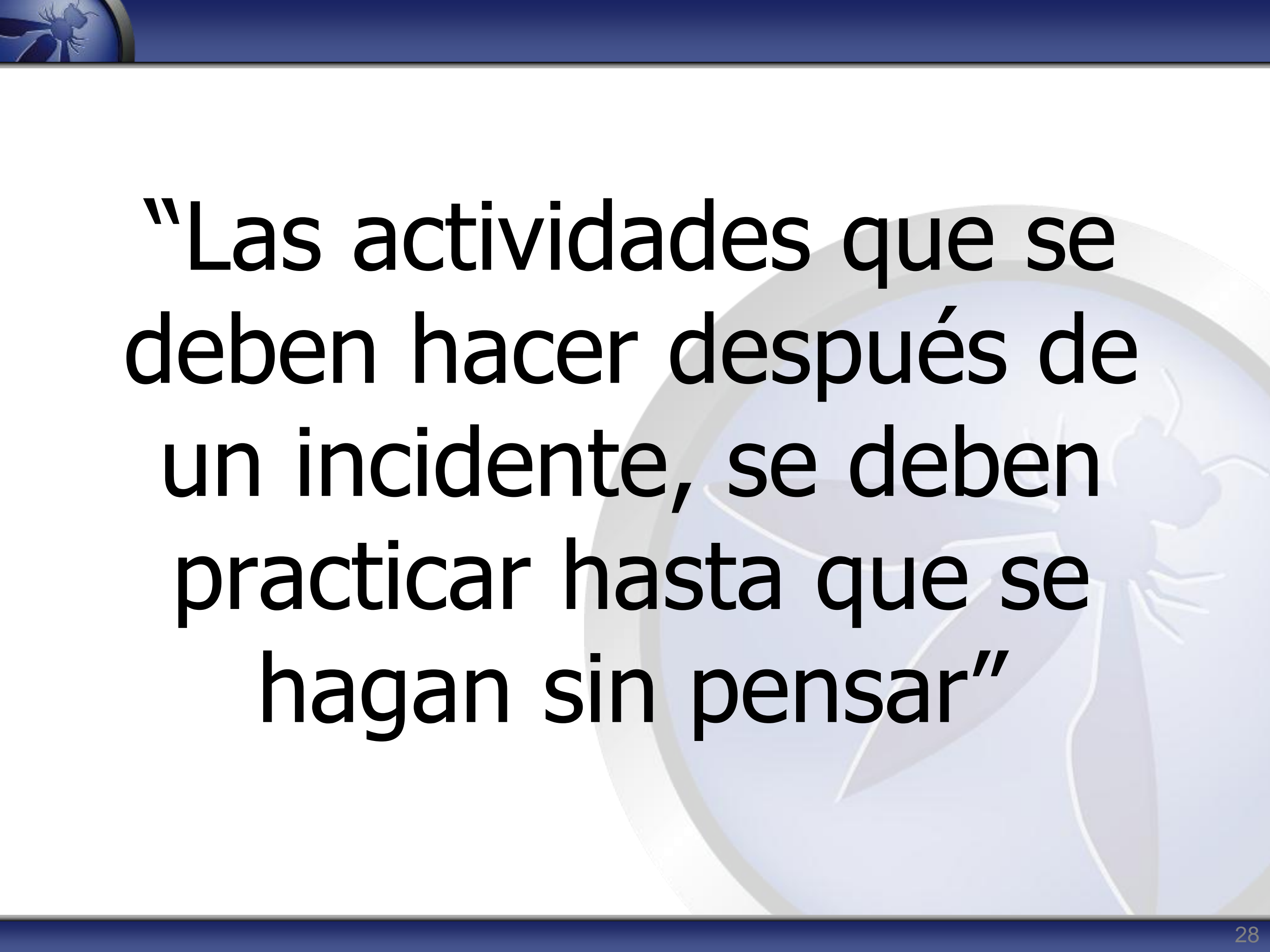


Reparar los sistemas





**Informar a los
usuarios y clientes**



“Las actividades que se deben hacer después de un incidente, se deben practicar hasta que se hagan sin pensar”



Conclusiones



- Las grandes empresas ya dejaron de ser el único vector de ataques web.
- La prevención y preparación son la clave contra los ataques web.
- Contar con personal especializado en monitoreo y gestión.
- Las actividades que se deben hacer después de un incidente, se deben practicar hasta que se hagan sin pensar.



???

Carlos Solís Salazar
carlos.solis@owasp.org
www.solis.com.ve
@csoliss