ORACLE®

Impacto del ENS: Propuesta Oracle

Jose Manuel Rodríguez de Llano
Sales Manager Identidad y Seguridad

Objetivo del Esquema Nacional de Seguridad

La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de **confianza en el uso de los medios electrónicos**, a través de medidas para **garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos**, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.

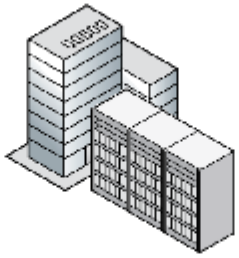
Persigue fundamentar la confianza en que los sistemas de información **prestarán sus servicios y custodiarán la información** de acuerdo con sus especificaciones funcionales, **sin interrupciones o modificaciones fuera de control, y sin que la información pueda llegar al conocimiento de personas no autorizadas.**

Una nueva Era de Riesgos

Tendencias en TI

Cloud Computing

- Amenazas sofisticadas
- Accesos no autorizados



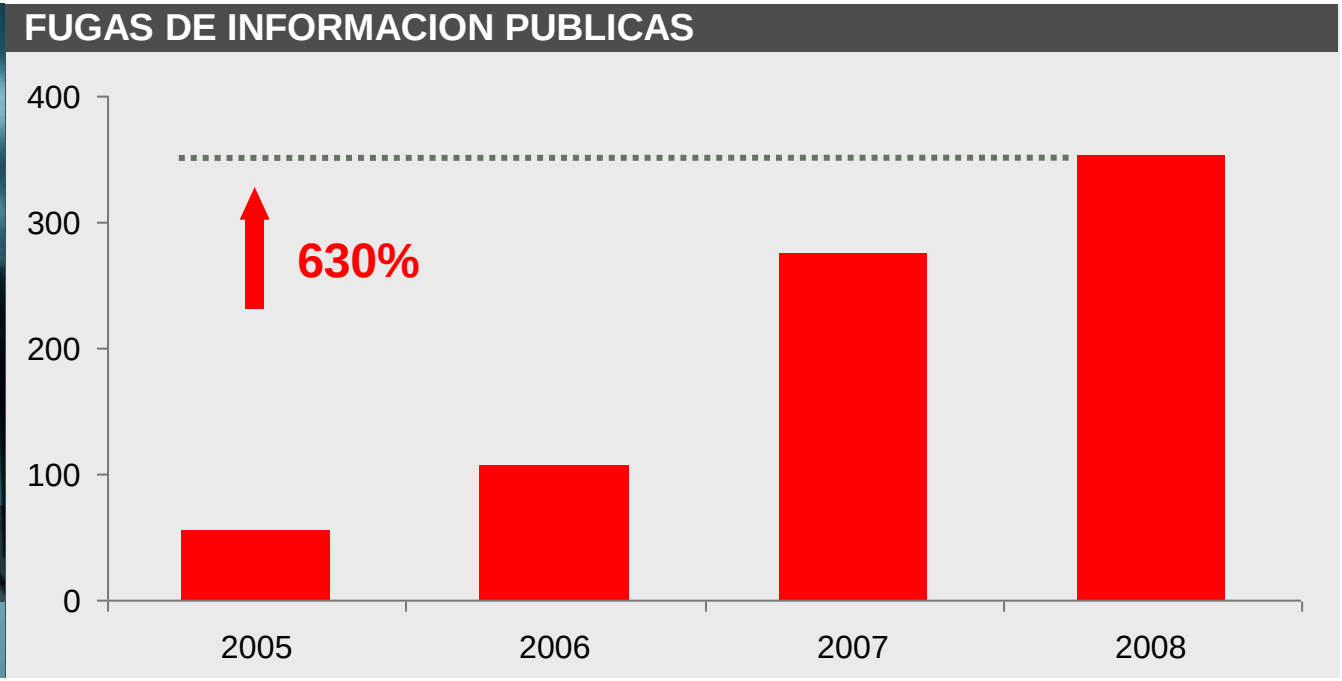
Data Centers

- Acceso de usuarios privilegiados
- Fugas de información

Virtualizacion

- Proliferación de Maquinas Virtuales
- Falta de Control y Visibilidad

Más fugas de información que nunca…

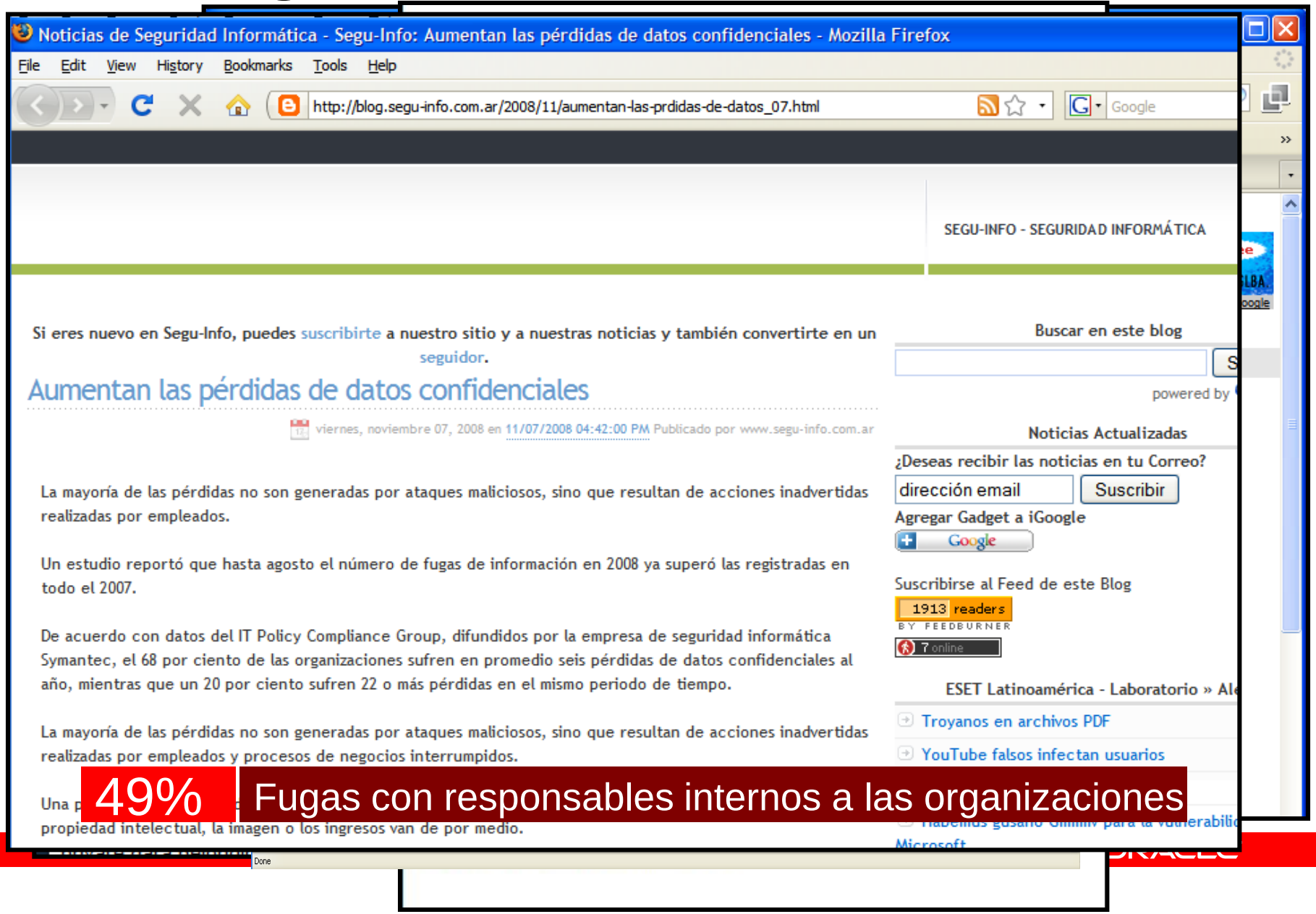


Coste medio: $202 por registro

Coste total medio por fuga: $6.6 millones

Source: DataLossDB, Ponemon Institute, 2009

Más fugas de información que nunca…



49% Fugas con responsables internos a las organizaciones

Más fugas de información que nunca…

Sony PlayStation suffers massive data breach

Recomendar 3138 recomendaciones. Regístrate para ver qué recomiendan tus amigos.

By Liana B. Baker and Jim Finkle
NEW YORK/BOSTON | Tue Apr 26, 2011 7:38pm EDT

(Reuters) - Sony suffered a massive breach in its video game online network that led to the theft of names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.

Sony learned that user information had been stolen from its PlayStation Network seven days ago, prompting it to shut down the network immediately. But Sony did not tell the public until Tuesday.

The electronics conglomerate is the latest Japanese company to come under fire for not disclosing bad news quickly. Tokyo Electric Power Co was criticized for how it handled the nuclear crisis after the March earthquake. Last year, Toyota Motor Corp was slammed for being less than forthright about problems surrounding its massive vehicle recall.

Tweet 162
Share this
Share 75
2 diggs
Email
Print

Factbox
Sony breach latest in string of cyber attacks
Tue, Apr 26 2011

Analysis & Opinion
Facebook scam warning pages under fire
Need a loan? 4 tips to improve your debt health

Related Topics
Technology »
Media »

Stocks
Sony Corp
6758.T
¥2,268
+8.00 +0.35%
05/02/2011
TOYOTA MOTOR CORP

Sony suffers second major user data theft

Recomendar 135 recomendaciones. Regístrate para ver qué recomiendan tus amigos.

By Liana B. Baker
NEW YORK | Mon May 2, 2011 7:54pm EDT

(Reuters) - Sony disclosed on Monday hackers had stolen the names, addresses and passwords of nearly 25 million more users than previously known less than a day after the Japanese company apologized for one of the worst break-ins in Internet history.

Sony's latest revelation comes after Sony No. 2 Kazuo Hirai announced measures had been put in place to avert another Playstation-type cyberattack, hoping to repair its tarnished image and reassure customers who might be pondering a shift to Microsoft's Xbox.

Tweet 196
Share this
Share
1 digg
Email
Print

Related News
Sony to keep pursuing network strategies after security breach
Mon, May 2 2011
Sony: no impact from data breach on tablet, NGP launch
Mon, May 2 2011

Analysis & Opinion
Tech wrap: Microsoft earnings fail to excite
Fear, loathing and apathy about digital security

Related Topics
Technology »
Hot Stocks »
Asian Markets »
Personal Finance »
Media »

Cual es la fuente principal de las fugas?

Table 7. Types of compromised assets by percent of breaches and percent of records*

Type	Category	% of Breaches	% of Records
Database server	Servers & Applications	25%	92%
Desktop computer	End-User Devices	21%	1%
Web app/server	Servers & Applications	19%	13%
Payment card	Offline Data	18%	<1%
POS server (store controller)	Servers & Applications	11%	<1%
Laptop computer	End-User Devices	7%	<1%
Documents	Offline Data	7%	<1%
POS terminal	End-User Devices	6%	<1%
File server	Servers & Applications	4%	81%
Automated Teller Machine (ATM)	End-User Devices	4%	<1%
FTP server	Servers & Applications	2%	3%
Mail server	Servers & Applications	2%	4%
Customer (B2C)	People	2%	<1%
Regular employee/end-user	People	2%	<1%

* Only assets involved in 2% or more of breaches shown

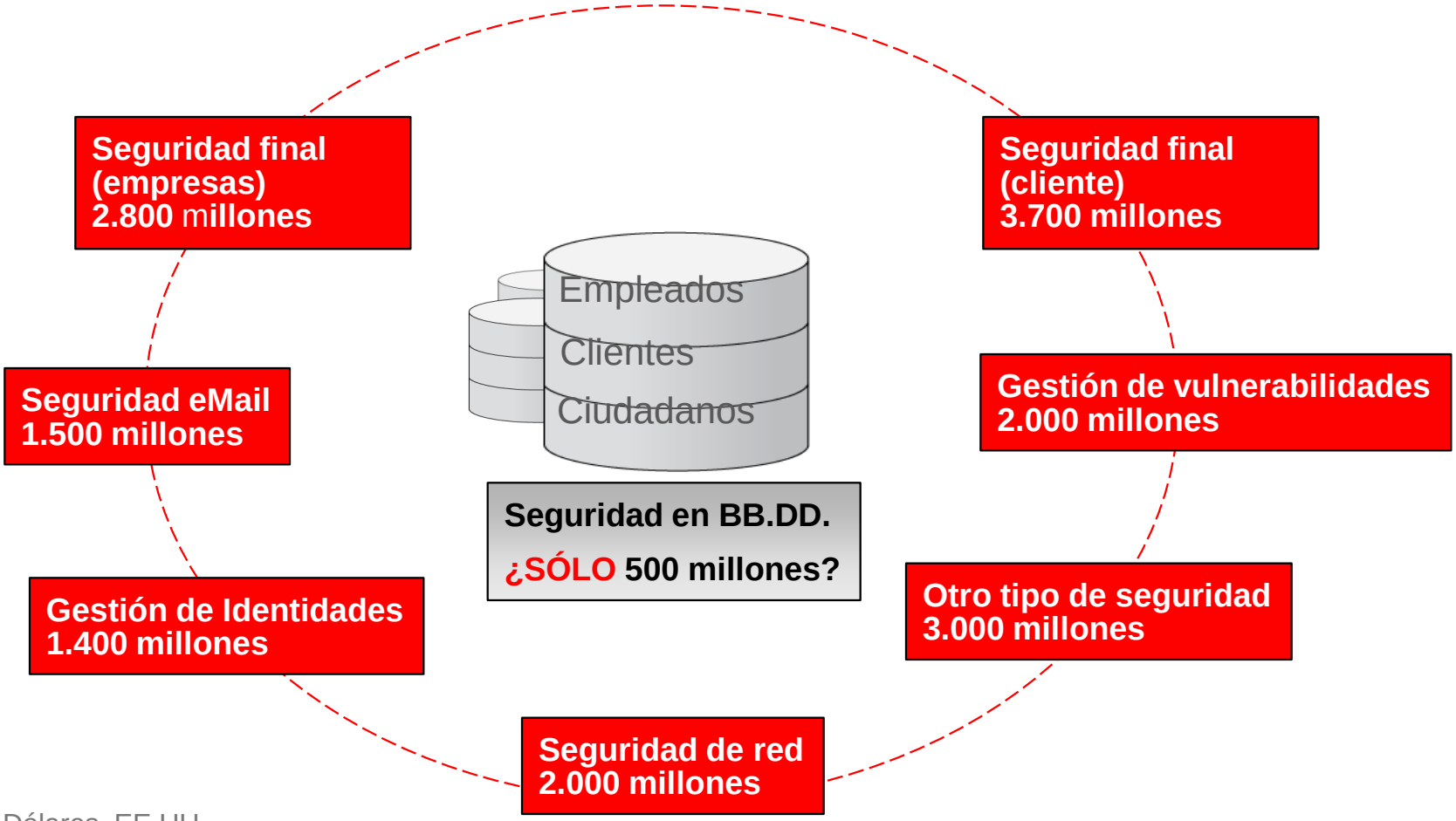
verizonbusiness

2010 Data Breach Investigations Report

92% Registros afectados proceden de Bases de Datos comprometidas

Mercado global de la seguridad

Gasto estimado en 2009: 17.000 millones



Cifras en Dólares EE.UU.

Una paradoja

- **La seguridad de los datos esta identificada como la primera prioridad en el ámbito de la Seguridad IT (Forrester 2010)**
- **La primera fuente de fugas de información (92%) son los servidores de base de datos**

2010 Data Breach Investigations Report

- **Sólo un 3% del presupuesto invertido en securizar las bases de datos (Gartner 2009)**

Bases de Datos: vulnerables

IOUG independent oracle users group

For the Complete Technology & Database Professional

The 2010 IOUG Data Security Report

28%	Cifra sin excepciones la informacion personal identificable en las BB.DD	Los datos pueden ser leidos por cualquier usuario con privilegios de acceso a la base de datos
24%	Tiene medios para evitar que un usuario privilegiado lea informacion sensible	Los DBA o cualquiera con los privilegios necesarios pueden acceder a los datos almacenados
68%	No pueden detectar si sus usuarios estan abusando de sus privilegios	Los usuarios de base de datos pueden realizar actividades no permitidas sin ser detectados

Bases de Datos: vulnerables

IOUG independent oracle users group
For the Complete Technology & Database Professional

The 2010 IOUG Data Security Report

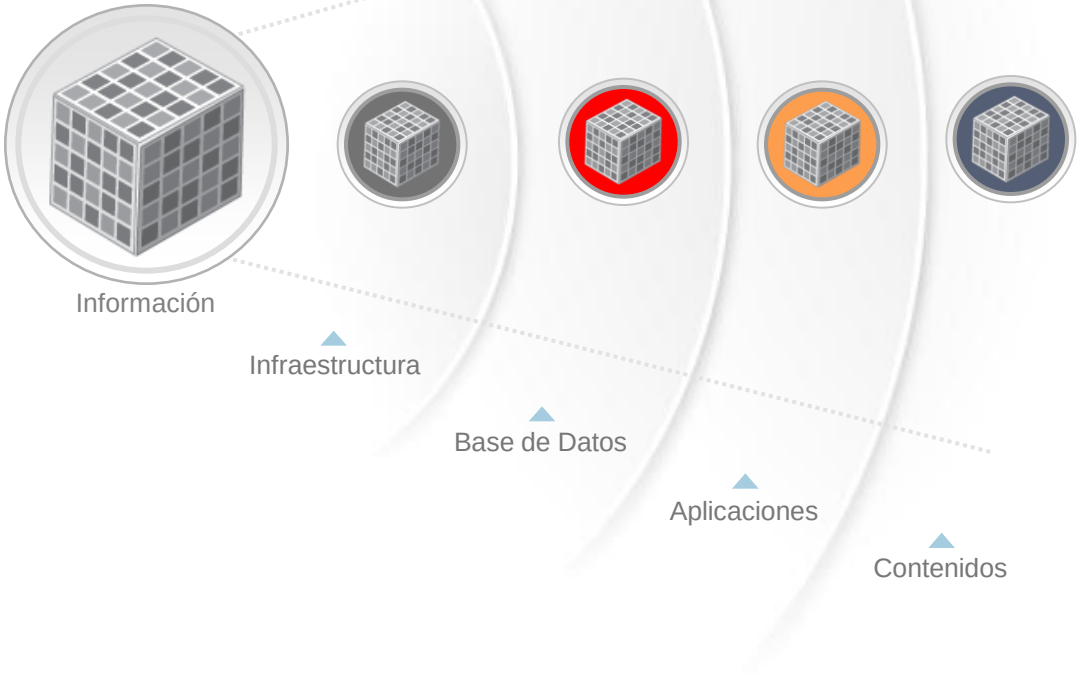
66%	No estan seguros de si sus aplicaciones pueden sufrir "SQL injection"	Los datos pueden ser manipulados desde el exterior por hackers que acceden desde las aplicaciones
48%	Copian informacion sensible a entornos fuera de produccion	Los desarrolladores pueden acceder a los datos reales de produccion

ENS: Requisitos Mínimos

Todo órgano de la Administración Pública, deben disponer formalmente de una **Política de Seguridad** que cubra los siguientes **requisitos mínimos**, en función de los riesgos identificados:

- Organización e implantación del proceso de seguridad
- Análisis y gestión de los riesgos
- Gestión de personal
- Profesionalidad
- Autorización y control de los accesos
- Protección de las instalaciones
- Adquisición de productos
- Seguridad por defecto
- Integridad y actualización del sistema
- Protección de la información almacenada y en tránsito
- Prevención ante otros sistemas de información interconectados
- Registro de actividad
- Incidentes de seguridad
- Continuidad de la actividad
- Mejora continua del proceso de seguridad

Seguridad Oracle



Seguridad en BBDD

- Cifrar y enmascarar
- Control usuarios privilegiados
- Autorización multi-factor
- Monitorización y auditoría

Gestión de Identidades

- Provisión de usuarios
- Gestión de roles
- Gestión de autorizaciones
- Risk-Based Access Control
- Directorio virtual

Information Rights Management

- Monitorización uso de documentos
- Control de acceso a documentos
- Seguridad dentro y fuera del Firewall

Service-Oriented Security

La Identidad como Servicio

Oracle Apps

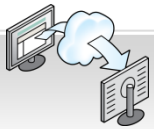
Aplicaciones 3os/Desarrollos

Proveedores Servicios Cloud

Servicios Web

Declarative Security Services


Autorización

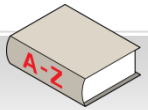

Federación


Autenticación


Auditoría


ID Admin


Role Mgmt



Servicios de Directorio

Almacén de Identidad, Credenciales, Políticas y Acceso al Dato.


Access Management

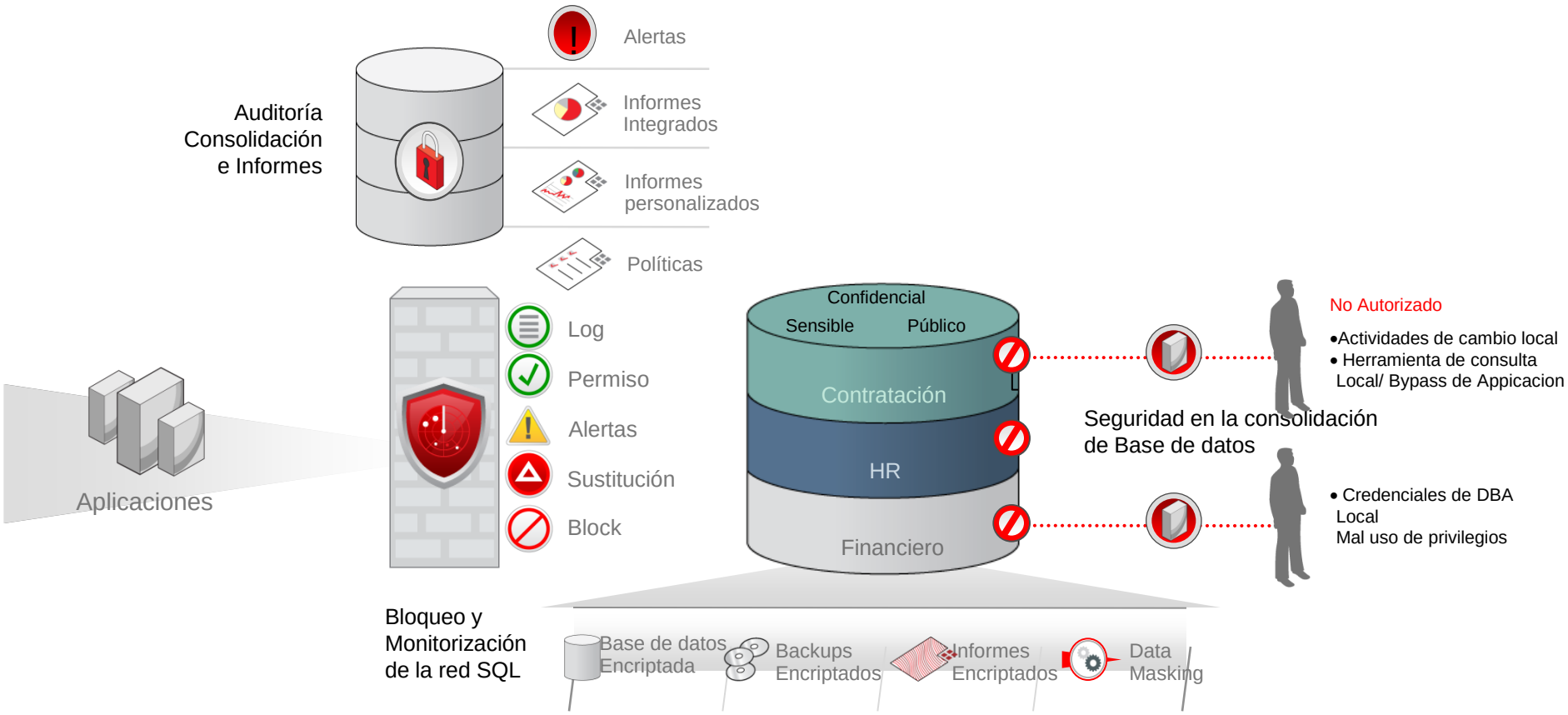

Identity Administration

Directory Services


BBDD

Seguridad en Base de Datos

Externalización, Consolidación de Base de Datos, Warehouses



Protección de documentos

Wikileaks

global defense of sources and press freedoms, circa now—

Saturday 14 February, 2009

Have documents the world needs to see?

We help you safely get the truth out.

We are of assistance to peoples of all countries who wish to reveal unethical behavior in their governments and institutions. We aim for maximum political impact...(more)

WikiLeaks Document Release

http://wikileaks.org/wiki/CRS-RL31555

February 2, 2009

Congressional Research Service

Report RL31555

China and Proliferation of Weapons of Mass Destruction and Missiles: Policy Issues

Shirley A. Kan, Specialist in Asian Security Affairs

January 7, 2009

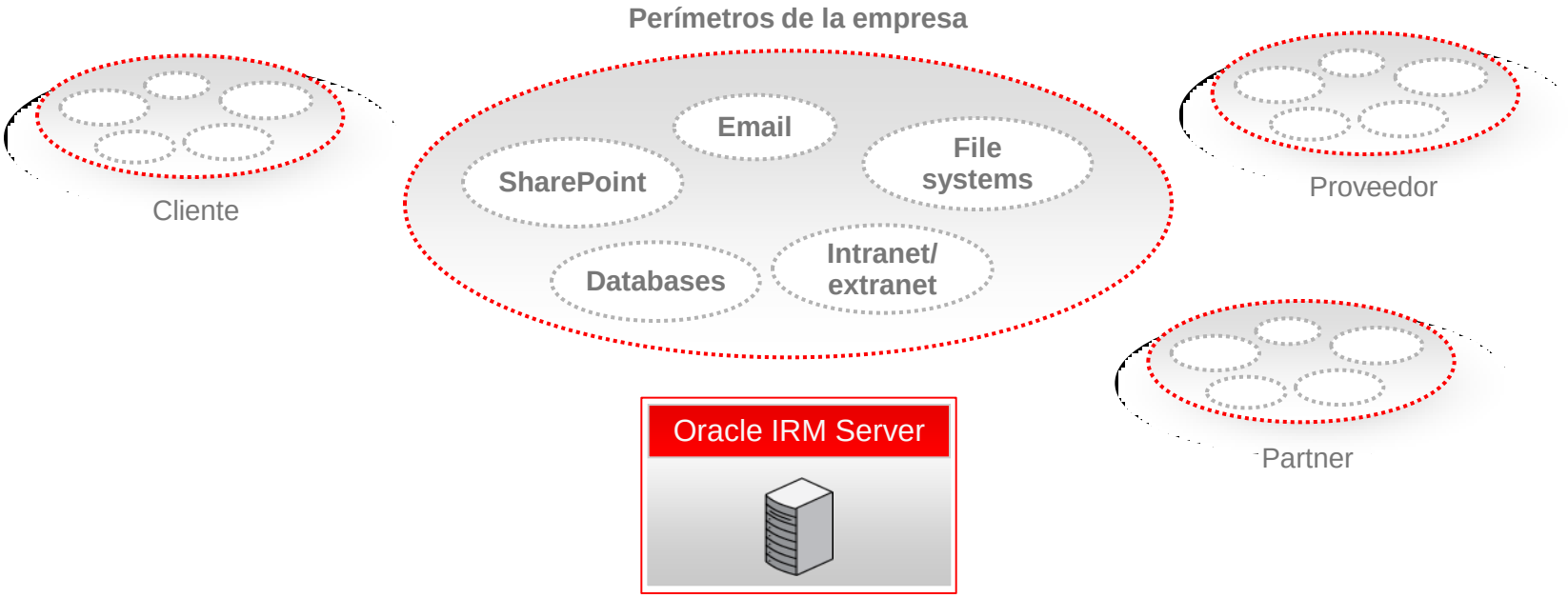
Abstract. Congress has long been concerned about whether U.S. policy advances U.S. security interests in reducing the role of the People's Republic of China (PRC) in the proliferation of weapons of mass destruction (WMD) and missiles as well as obtaining China's cooperation in weapons nonproliferation. This problem refers to the threat of nuclear, chemical, or biological weapons and missiles that could deliver them. Some have argued that certain PRC transfers violated international treaties or guidelines, and/or have contravened various U.S. laws requiring sanctions to shore up those international standards. Even if no laws or treaties are violated, many

Change you can download

Wikileaks has released nearly a billion dollars worth of quasi-secret reports commissioned by the United States Congress. The 6,780 reports, current as of this month, comprise over 127,000 pages of material on some of the most contentious issues in the nation, from the U.S. relationship with Israel to abortion legislation. Nearly 2,300 of the reports were updated in the last 12 months, while the oldest report goes back to 1990. The release represents the total output of the Congressional Research Service (CRS) electronically available to Congressional offices. The CRS is Congress's analytical agency and has a budget in excess of $100M per year...(more)

Information Rights Management

Protege todas las copias de información sensible y confidencial



- En todo lugar donde los contenidos cifrados por IRM sean almacenados, transmitidos o usados
  - LOS USUARIOS NO AUTORIZADOS NO TIENEN ACCESO
  - Acceso transparente y revocable para los usuarios autorizados
  - Políticas centralizadas y auditoría para contenidos ampliamente distribuidos
- Protección del Contenido mas allá de la Base de Datos, la Aplicación y el Firewall

Preguntas


ORACLE®