

Protección de la información y cumplimiento normativo

**INFORMATION INTEGRATION
& GOVERNANCE FORUM 2011**
Delivering Trusted Information for Smarter Business Decisions



Problemática en el Negocio / Necesidad del Cliente



Aumento de ataques y robos internos y externos de datos
Aumento del fraude por el robo de datos personales
Multas y sanciones por no cumplir normativa: SOX, PCI, LOPD, DP



Proposición de valor de IBM InfoSphere Guardium



Prevenir peligros Internos

- Identificar accesos y cambios no autorizados
- Prevenir fuga de información



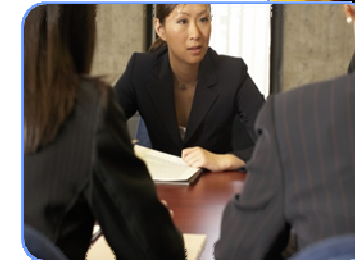
Prevenir peligros Externos

- Prevenir robo
- Bloqueo de acceso a datos confidenciales



Monitorización

- Usuarios privilegiados
- Bases de datos y tablas críticas



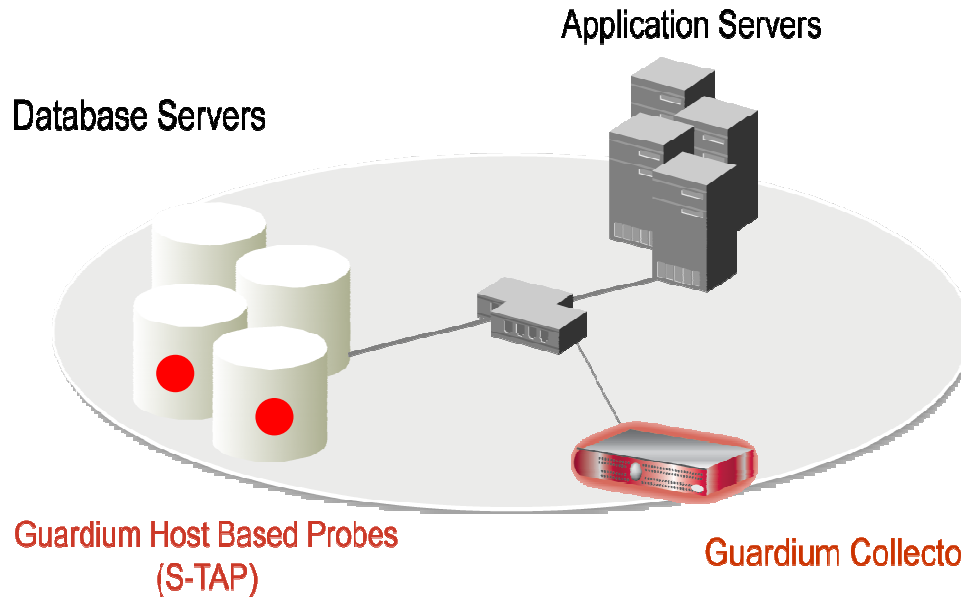
Cumplimiento Regulaciones

- Simplificar y automatizar el proceso de auditoría
- Reducción de costes



Análisis de Vulnerabilidades y gestión de incidencias

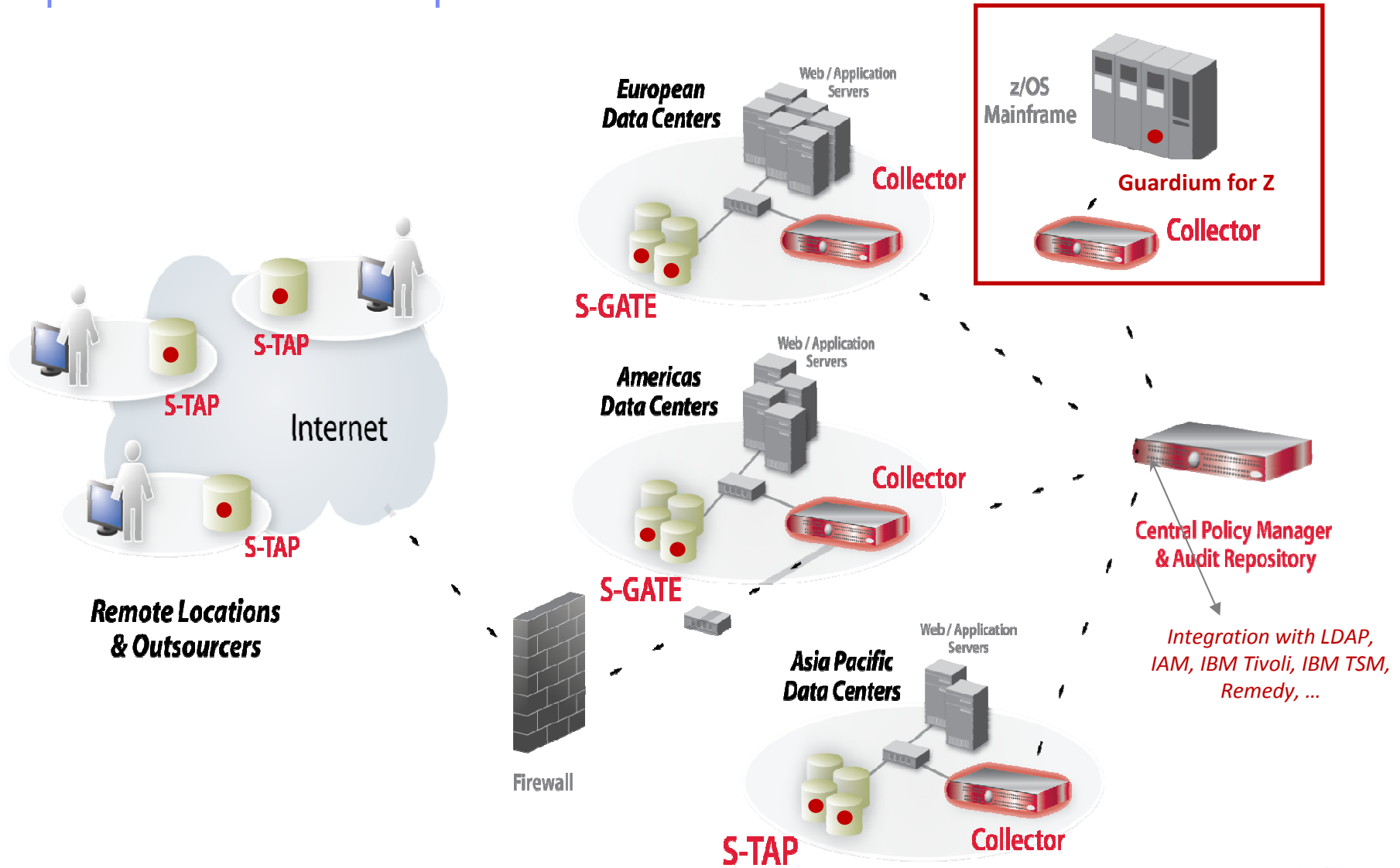
La Solución IBM InfoSphere Guardium



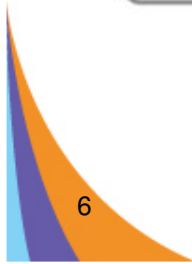
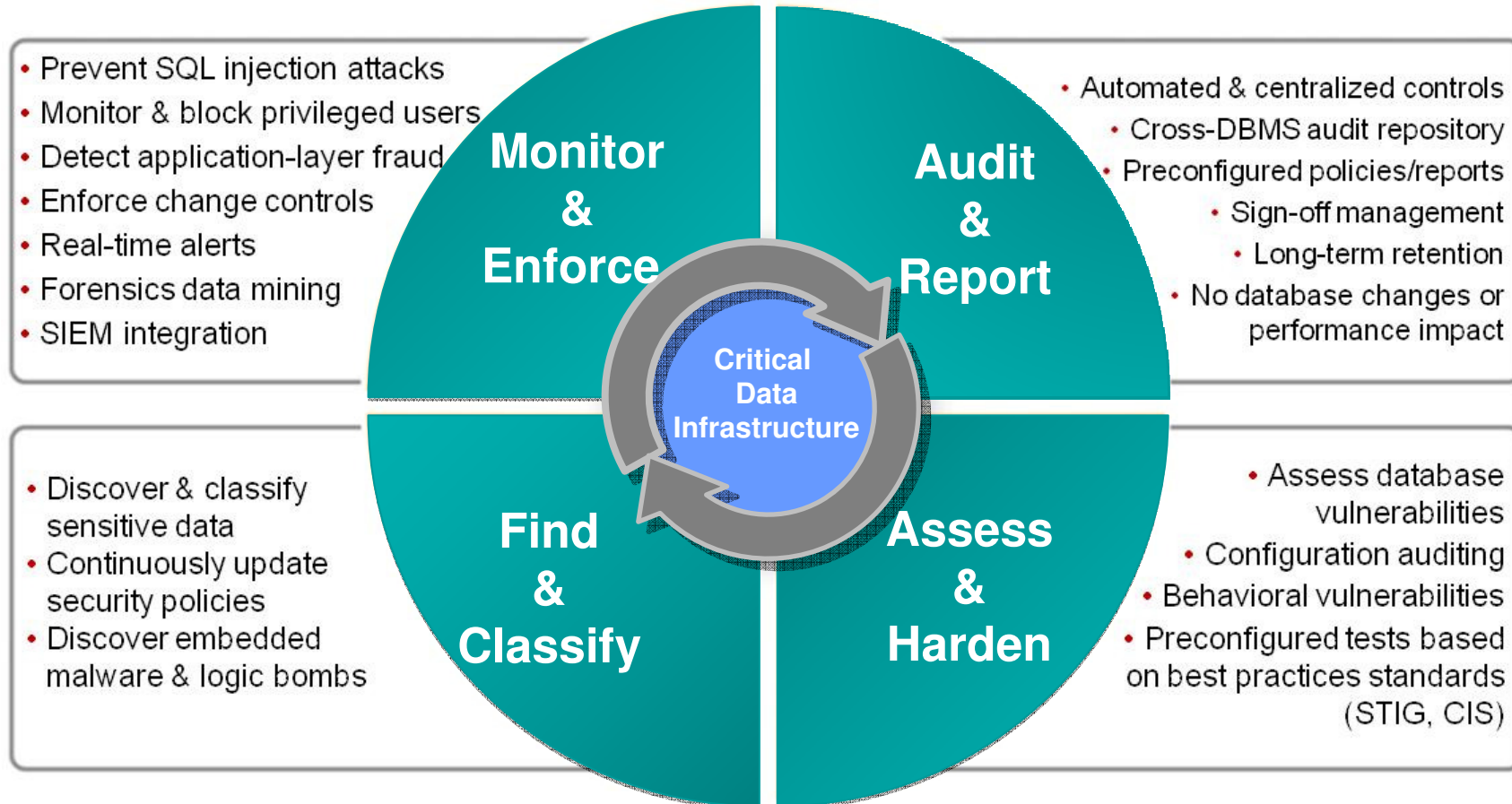
- **Arquitectura no-invasiva**
 Fuera de la Base de Datos
 Impacto mínimo en rendimiento (2-3%)
 Sin cambios al DBMS o aplicativos
- **Solución multi-plataforma**
- **100% visibilidad: accesos locales y remotos**

- **Refuerza segregación de funciones**
 No depende de los logs nativos del DBMS
- **Granular, políticas y auditoría en tiempo real: Quién, dónde, cuándo, cómo**
- **Informes automatizados de cumplimiento, trazabilidad y escalado (SOX, PCI,)**

Arquitectura IBM Infosphere Guardium

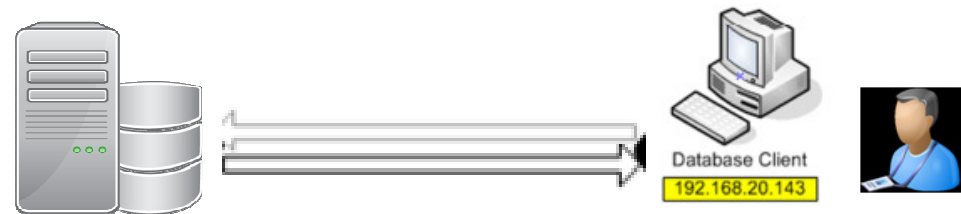


Módulos Funcionales



Monitorización y Fortalecimiento de las Bases de datos

- Monitorizar tráfico local y remoto
- Loggins y conexiones
- Monitorización de la actividad (DDLs, DMLs, DCLs)



IBM InfoSphere™ Guardium

14:13 | Edit Account_poc | Customize | Logout | About | IBM

Standard Reports | My New Reports | Discover | Assess/Harden | Comply | Protect | Quick Start | Sarbanes-Oxley Accelerator | PCI Accelerator | Data Privacy Accelerator

Security Policies | Correlation Alerts | Incident Management

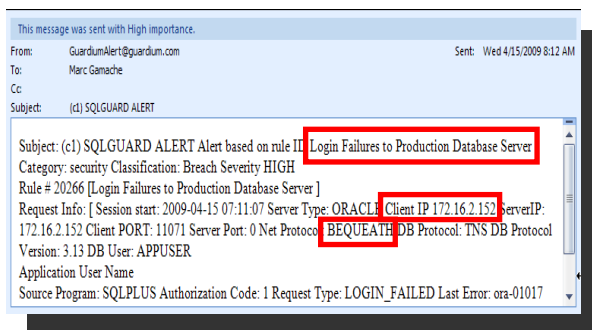
Policy Violations / Incident Management

Start Date: 2010-09-09 12:13:27 End Date: 2010-09-10 14:13:27

Aliases: ON

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String	Severity Description	Incident Number	Count of Policy Rule Violations
2211	2010-09-09 14:13:11.0	PCI	IOD SQL ERRORS	10.10.9.56	10.10.9.56	GUARDIUMDEMO	select * from badtablename	HIGH	0	1
2210	2010-09-09 14:08:03.0	PCI	IOD STAP Terminate access to PCI Table	10.10.9.56	10.10.9.56	SYSTEM	select * from guardiumdemo.pci_table	HIGH	0	1


Records 1 to 2 of 2





- Políticas para la Gestión de Incidencias
- Envío de Alertas y Bloqueos
- Reportes de Gestión de incidencias


Category Name	Access Rule Description	Client IP	Server IP	DB User Name
security	Login Failures to Production Database Server	10.10.9.56	10.10.9.56	APPUSER

Análisis de Vulnerabilidad

- 

Descubrir vulnerabilidades en BD mediante test predefinidos o customizables, basados en Best Practices de la Industria (STIG, CIS, CVE...)
- 

Actualizaciones cuatrimestrales para evitar amenazas
- 

Realizar chequeos regularmente de la vulnerabilidad
- 

Identificar riesgos: Parches no aplicados y críticos, mis-configured privileges, passwords débiles, cuentas por defectos.

Results for Security Assessment: **Guardium Oracle** -- Select another result --

Assessment executed **2009-09-29 21:38:18.0**

From: 2009-09-01 00:00:00.0 Client IP or IP subnet: Any
To: 2009-09-25 00:00:00.0 Server IP or IP subnet: Any Download PDF

Tests passing: **45%**

Based on the tests performed under this assessment, data access of the defined database environments requires improvement. Refer to the recommendations of the individual tests to learn how you can address problems within your environment and what you should focus upon first. Once you have begun addressing these problems you should also consider scheduling this assessment as an audit task to continuously assess these environments and track improvement.

[View log](#)
[Lump to Datasource list](#)

Result Summary Showing 104 of 104 results (0 filtered)

	Critical	Major	Minor	Caution	Info
Privilege	8p 16f	1p 4f	1f		
Authentication	1p 5f	1f	2f		
Configuration	4p	6p 4f 4e	1p 3f 4e	6f 1e	
Version		2f			
Other	2p	6p 4f	4p 2f 1e		8p 3e

Assessment Result History

Current filtering applied:
 Severities: - Show All -
 Scores: - Show All -
 Types: - Show All -

[Reset Filtering](#) [Filter / Sort Controls](#)

Assessment Test Results Compare with Previous Results Showing 104 of 104 results (0 filtered)

Cat.	Test Name	Datasource	P/F	Sev.	Reason
Auth.	Default Accounts Password Changed	ORACLE: Oracle Local	Fail	Critical	5 active pre-defined users have default passwords. <i>Recommendation: Some predefined Oracle user accounts are still enabled and still have the Oracle default password. These predefined Oracle users and passwords are well-known to anyone familiar with Oracle, and represent one of the easiest entry points for attacks and data theft/damage. We recommend that you remove any predefined Oracle user accounts that are not absolutely required, and we strongly recommend that you change the passwords for any of these users who are required.</i>
Priv.	No Access To 'Users' Catalog Tables	ORACLE: Oracle Local	Fail	Critical	Some users or roles without 'SELECT_CATALOG_ROLE' authority have access to 'DBA_USERS' or 'ALL_USERS': CTXSYS, PUBLIC. <i>Recommendation: Access to the DBA_USERS or ALL_USERS tables has been granted to users other than</i>

Los Auditores quieren ver la evidencia de controles, procesos y procedimientos adecuados.

Descubrimiento y Clasificación de Información Sensible



Auto-descubrimiento de Bases de Datos

Administration Console							
Administration Console		Access Management	Tools	Daily Monitor	SQL Guard Monitor	Tap Monitor	Incidents
<ul style="list-style-type: none"> SQL Count Session Count Logged Threshold Alerts Logged R/T Alerts Exception Count Dropped Requests TCP Exceptions Admin User Logins Databases by Type Databases Discovered Retrospective Report Requests Values Changed Throughput 							
Databases Discovered							
Start Date: 2008-06-26 14:48:49 End Date: 2008-06-26 15:48:49							
Time Probed	Server IP	Server Host Name	DB Type	Port	Port Type	#	
2008-06-26 15:31:00	10.10.9.253	10.10.9.253	Oracle	1521	tcp	1	
2008-06-26 15:30:58	10.10.9.253	10.10.9.253	MSSQL	1433	tcp	1	
2008-06-26 15:30:15	10.10.9.55	osprey	Oracle	1521	tcp	1	
2008-06-26 15:30:15	10.10.9.55	osprey	Sybase	4200	tcp	1	
2008-06-26 15:30:32	10.10.9.56	10.10.9.56	Oracle	1521	tcp	1	
2008-06-26 15:30:58	10.10.9.56	10.10.9.56	DB2	50001	tcp	1	



Descubrimiento y Clasificación de la Información Sensible

Catalog	Schema	Table Name	Column Name	Rule Description	Comments	Classification Name	Category	Data Source Description
<input type="checkbox"/>	BANKAPP	CREDITCARD	CARDNUMBER	Send Alert	Date: Monday, July 21, 2008 6:30:07 PM EDT Datasource: ORACLE 10.10.9.56:1521 xe Object: TABLE BANKAPP.CREDITCARD VARCHAR2 (20) CARDNUMBER Category: 'PCI Classification: 'Cardholder Data' Rule: Search For Data: Send Alert TABLE_TYPE='TABLE,VIEW', DATA_TYPE='TEXT', SEARCH_VALUE_PATTERN='[0-9]{4}-[0-9]{4}-[0-9]{4}-[0-9]{4}' Action: Send Alert: Send Alert Urgent Flag='false', Receiver='SYSLOG' Action: Log Policy Violation: Send Policy Violation Severity='10' Action: Add To Group Of Objects: add to group Object Group='PCI Cardholder Sensitive objects', Replace Group Content='false'	Cardholder Data	PCI	10-56-system

Novedades de la V.8 de InfoSphere Guardium

- Solución en Appliance y/o Software
- Nuevos Entitlement Reports
- Automatización del flujo de trabajo de cumplimiento
- Mejora bloqueos: Cuarentena / Fire-ID



- Monitorizar repositorios SharePoint
- Nuevas plataformas soportadas: Netezza & PostgreSQL
- Integration with Tivoli SIEM
- Mejoras en el Vulnerability assessment – 500 nuevos tests
- Nuevas capacidades para el DB2 Z/OS (Mainframe)

Beneficios de la solución IBM InfoSphere Guardium

- Protección, monitorización y auditoría en tiempo real
- Solución escalable y de gestión centralizada
- Con más de 150 políticas e informes pre-configurados: SOX, PCI, DP
- Automatización del flujo de trabajo de cumplimiento
- Depósito de auditorías no modificable



- Seguridad proactiva, en tiempo real
- Rastreo y solución de incidentes de seguridad
- Evaluación de comportamientos, configuración y Vulnerabilidad
- Ubica, clasifica y protege datos confidenciales automáticamente

Líderes en el sector Financiero

JPMORGAN CHASE & Co.	GE Money Bank	Bank of America	Santander	HSBC
BARCLAYS	Allianz	Rosenberg <small>An AXA Investment Managers Company</small>	UniCredit	BBVA Compass
Itaú	Prudential 保德信	SOCIETE GENERALE Corporate & Investment Banking	三井生命	AVIVA
PRUDENTIAL	Standard Bank	QBE	Garanti	MAPFRE
AKBANK	citi	GRUPO BANCO POPULAR	ING	RBS <small>The Royal Bank of Scotland Group</small>

Líderes en el sector Telco

Líderes en el sector Seguros

THANK
YOU