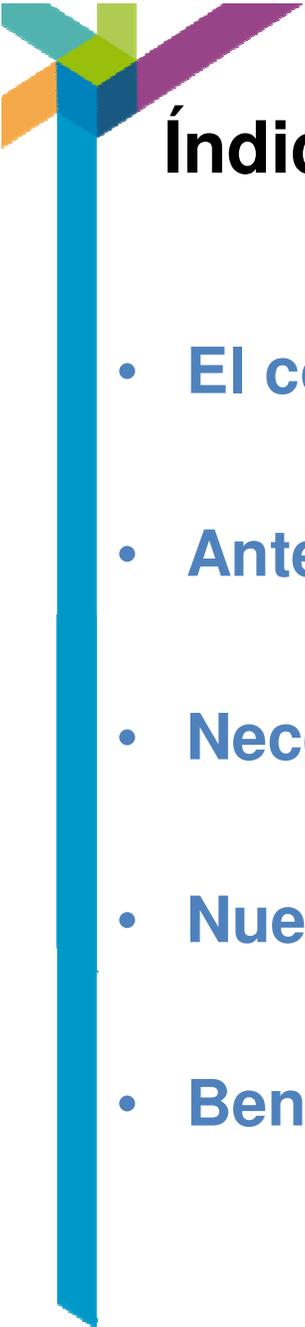




Monitorización, Protección y Auditoría de Bases de Datos en tiempo real

Cumplimiento normativo y protección de
acceso en Euskaltel

The Atos logo, consisting of the word "Atos" in a bold, blue, sans-serif font.



Índice

- El coste del cumplimiento
- Antecedentes legales y normativos
- Necesidades y requisitos
- Nuestra solución
- Beneficios para el cliente

Atos





El coste del cumplimiento

El coste económico

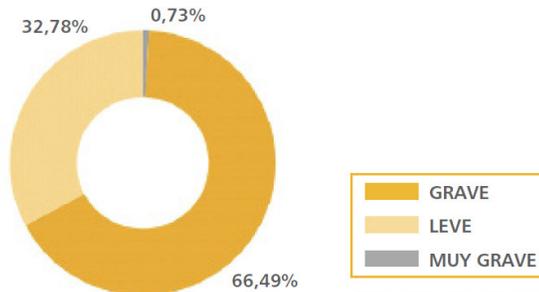


- Situación de sanciones con el cumplimiento de la LOPD

Mayoría de sanciones graves

Aumento del importe de las sanciones

SANCIONES IMPUESTAS SEGÚN GRAVEDAD 2011



SANCIONES IMPUESTAS

	2009 (€)	2010 (€)	2011 (€)	% VAR. 2010/11
TOTAL SANCIONES	24.872.979,72	17.497.410,02	19.597.905,97	12

* La tabla recoge el total de sanciones declaradas.

DISTRIBUCIÓN DE LAS ACTUACIONES PREVIAS

ACTIVIDAD	2009	2010	2011	% RELATIVO	% VAR. 2010/11
Telecomunicaciones	908	1.170	1.378	25,57	17,78
Videovigilancia	721	819	871	16,16	6,35
Entidades financieras	768	691	841	15,61	21,71
Servicios de Internet (excepto spam)	156	168	288	5,34	71,43
Comunicaci. electrónicas comerciales - spam (LSSI)	180	126	270	5,01	114,29

*Agencia Española de Protección de Datos. Memoria 2011

- Más el coste de implantación de las medidas de seguridad...



El coste del cumplimiento

El coste técnico

- **Problemática** del registro de accesos a datos de nivel alto:
 - **Registro de todos los accesos** a todos los registros (quién, cuándo, a qué, que acción, autorizado o no autorizado...).
 - Impacto en almacenamiento
 - Impacto en rendimiento (auditorías propias)
 - Tradicionalmente la generación del registro de actividad ha encontrado un gap a veces insalvable de **mapear la información de actividad en las bases de datos con el usuario de aplicación** que las realiza.
 - **Desarrollos ad-hoc** no cubren entornos heterogéneos o no son fácilmente escalables.
 - **Aplicación a entornos de desarrollo con datos reales.**
 - **Los procesos de desarrollo** de aplicaciones y de despliegue en producción no incorporan políticas de **mínimo privilegio.**



Atos



Antecedentes legales y normativos

Atos



- **Legislaciones de aplicación en el ámbito de las telecomunicaciones** que establecen medidas de seguridad sobre datos de carácter personal:
 - Ley de Servicios de la Sociedad de la Información y de Comercio electrónico (Ley 34/2002).
 - Ley General de Telecomunicaciones (Ley 32/2003).
 - Reglamento sobre servicios de comunicaciones electrónicas, el servicio universal y la protección de los usuarios (Real Decreto 424/2005).
 - Ley de Impulso de la Sociedad de la Información (Ley 56/2007).
 - Ley sobre de conservación de datos relativos a las comunicaciones electrónicas y a las redes públicas de comunicaciones (Ley 25/2007).
- **Todas ellas hacen referencia a la LOPD y su reglamento de desarrollo.**
 - **El Artículo 81.4., equipara al nivel alto** de los datos especialmente sensibles, **los datos de tráfico y localización tratados por los operadores de telecomunicaciones.**



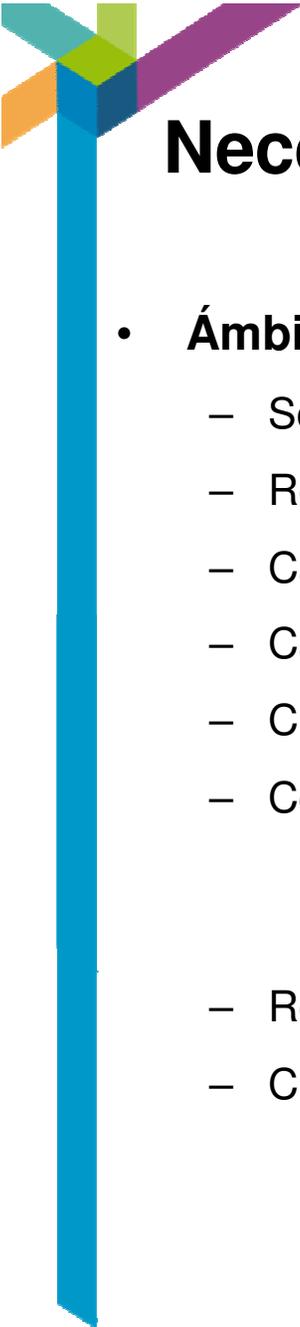
Antecedentes legales y normativos

Atos



- **Euskaltel**, como operador global de telecomunicaciones del País Vasco, **está sujeto a obligaciones de cumplimiento normativo** que le exigen el establecimiento de estrictos controles de auditoría de seguridad, encaminados a proteger el acceso a las bases de datos que contienen la información más sensible de la compañía.
- Adicionalmente al cumplimiento legal, el propio **proceso interno de gestión de la seguridad de la información** de Euskaltel, ha identificado la necesidad de reducir el riesgo asociado al acceso a la información presente en sus Bases de Datos.



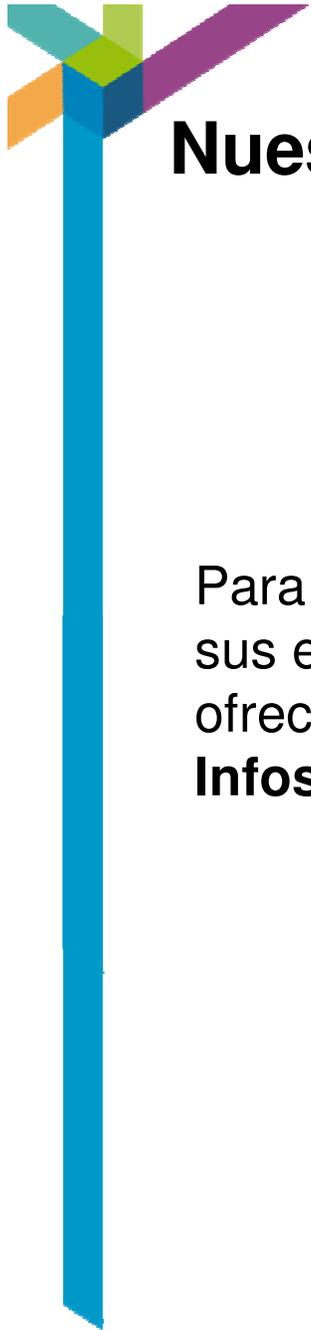


Necesidades y requisitos

- **Ámbitos de requisitos requeridos**
 - Soporte a entornos de BBDD heterogéneos
 - Rendimiento
 - Capacidad de definición de políticas de control de acceso
 - Capacidad de definición de políticas de auditoría
 - Cumplimiento normativo (registro de accesos LOPD)
 - Control de acceso
 - Autenticación contra diferentes repositorios
 - Capacidad de definición de niveles de acceso (roles)
 - Reporting
 - Cifrado de información

Atos





Nuestra solución

Para la realización de este proyecto **Atos** aúna sus esfuerzos y conocimiento junto con IBM para ofrecer un servicio líder en el mercado DAM, **Infosphere Guardium**.

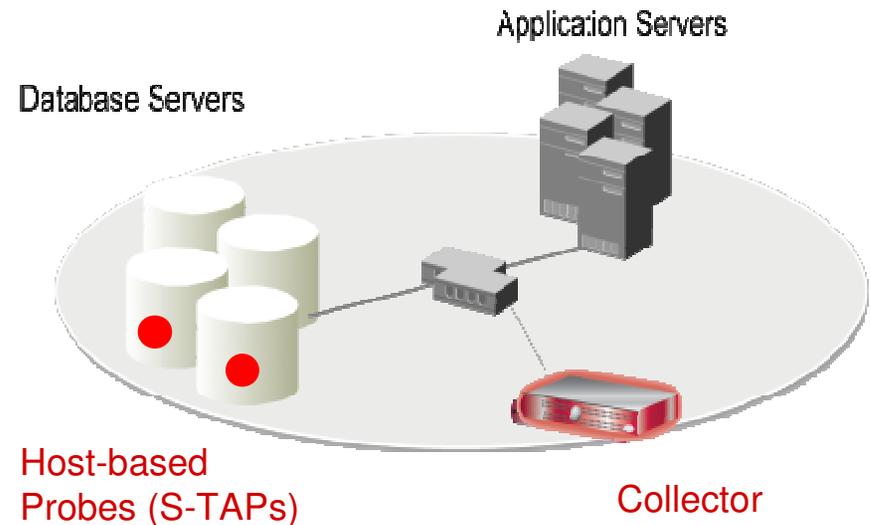


Nuestra solución

IBM Infosphere Guardium

- Da **respuesta a los requisitos técnico / funcionales** establecidos por Euskaltel.
- **Supervisa la actividad** de base de datos a través de entornos heterogéneos y en tiempo real, desde usuarios administradores de BBDD hasta usuarios de aplicación.
- **Registra y controla el acceso** según una gran amplitud de condiciones (intervalo de tiempo, objetos, usuarios, protocolos, segmentos de red, etc.)
- **Permite el enmascaramiento** de datos según patrones.

Atos





Nuestra solución

Atos



Servicios de Seguridad de Atos

- **Conocimiento de la organización** (incluyendo implantación de sistemas del alcance).
- **Larga trayectoria en proyectos de auditoría y adecuación cumplimiento normativo** (LOPD, PCI DSS, ENS,...)
- **Experiencia en proyectos similares** relacionados con la implantación de medidas de Registro de Acceso a datos de nivel alto.
- **Formación / certificación de profesionales en Guardium.**

Governance, Risk & Compliance (GRC)

- Plan director de de Seguridad y SGSI
- Auditoría de Madurez en Seguridad -Diagnóstico global de Seguridad
- Análisis de Riesgos
- Estrategia de Continuidad de Negocio (BCM).
- Adecuación a la legislación (LOPD, Sanidad, ENS, PCI DSS, LISI, Ley 11/2007, SOX,...)
- Desarrollo de Políticas, Normas y procedimientos de seguridad

Security Technology Advisory (STA)

- Diseño de Arquitecturas de Seguridad (física y lógica)
- Selección de productos de seguridad
- Implantación de soluciones de seguridad
- Análisis de vulnerabilidades técnicas
- Plataformas de Gestión de Eventos de Seguridad

Identity and Access Management (IAM)

- Gestión de Identidad, Control de Acceso, SSO
- Infraestructuras de clave pública, autenticación y plat.validación

Managed Security Services (MSS)

- Gestión de Vulnerabilidades, hacking ético
- AV/AS/Contenidos Gestionados
- Servicios de Autenticación/Autorización
- Gestor de Seguridad, SOCs
- Respuesta a Incidentes e Informes



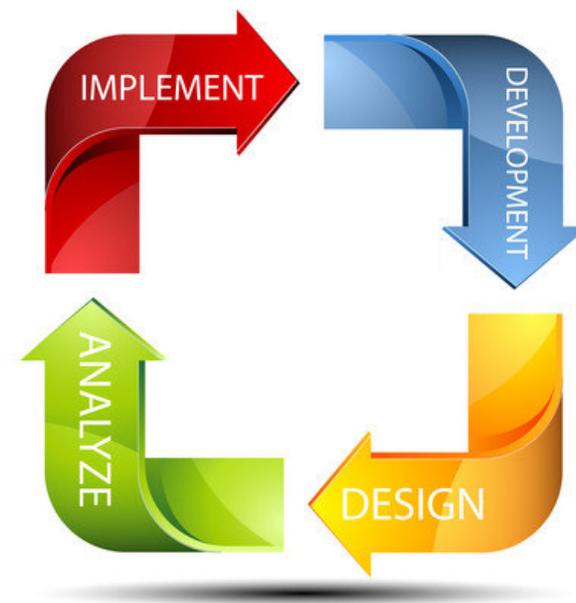
Nuestra solución

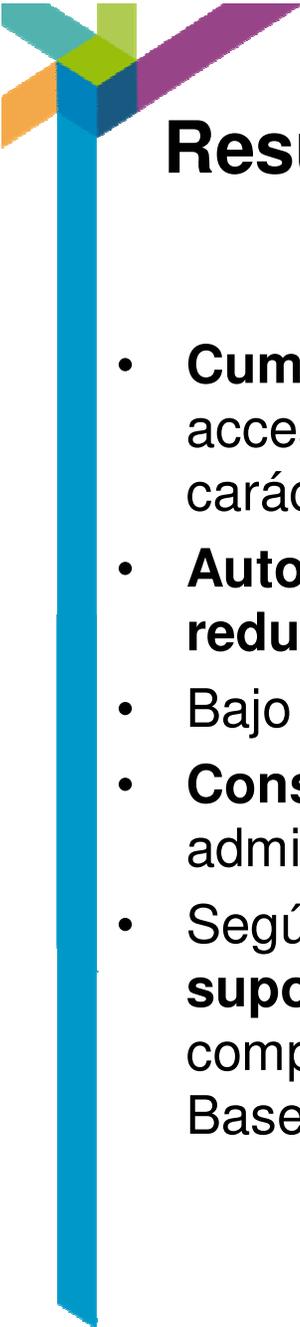
Atos



- **Fases / tareas principales del proyecto:**

- Análisis e identificación de sistemas y datos a proteger.
- Diseño de políticas de acceso y auditoría.
- Instalación y configuración inicial de Guardium.
- Instalación de agentes S-TAP.
- Desarrollo de informes de monitorización.
- Configuración y aplicación de políticas de:
 - Acceso
 - Excepción
 - Extrusión





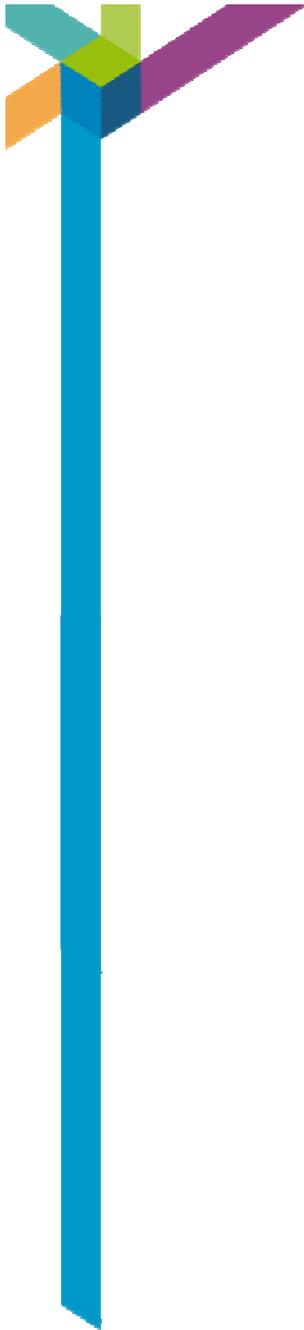
Resultados y beneficios

Atos



- **Cumplimiento normativo y legal específico del mercado** en los accesos a información sensible de la compañía y de datos de carácter personal.
- **Automatización de las tareas del cumplimiento** y, por tanto, **reducción de los costes operacionales** asociados.
- **Bajo impacto en el rendimiento** de los entornos de producción.
- **Consolidación** del registro de accesos **y facilidad** de gestión y administración de los **procesos de seguridad y auditoría**.
- Según la propia experiencia de **Atos** la **implantación de Guardium supone un coste de proyecto un 30% menor** aproximadamente, comparado con otras tecnologías DAM, tecnologías propias de Base de Datos o desarrollos a medida.





José Martínez Vicaria

Senior Manager. Information Security and Risk Management.
CISSP, CISA

Tel: +34.91.214.88.00

Móvil: +34.618.97.27.61

Email: jose.mvicaria@atos.net

Atos

Dirección: c/Albasanz 16, 4º; 28037-Madrid; España

WEB: <http://es.atos.net/>

Atos, the Atos logo, Atos Consulting, Atos Worldline, Atos Sphere, Atos Cloud and Atos WorldGrid are registered trademarks of Atos SA. October 2012

© 2012 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.

