

# Segurança e Auditoria de Dados

## Integridade das informações estratégicas do seu negócio!

O Serviço de Segurança e Auditoria Remota de Bancos de Dados foi desenvolvido pela XTI juntamente com seus parceiros para salvaguardar informações sigilosas por meio da garantia da visibilidade e rastreabilidade dos acessos aos dados.

É uma solução completa e corporativa para monitoramento e auditoria de acesso a bancos de dados, que permite a identificação de eventos de segurança relevantes, como a pesquisa e a atualização de dados, esquemas e permissões de bancos de dados. Oferece uma visão histórica e em tempo real de quem está “mexendo” nos dados da empresa, mais ainda, fazemos isso através de uma abordagem não intrusiva, baseada na rede, com impacto nulo na performance do ambiente.

### Principais Características

- **Transparência** Não requer mudanças em aplicações ou bancos de dados.
- **Completeness** Monitora as atividades de todos os insiders, inclusive de usuários privilegiados. Fornece informações granulares sobre todos os acessos e não por amostragem.
- **Performance** Não causa impacto na disponibilidade ou nos níveis de serviço das aplicações e dos bancos de dados. Utiliza um sistema de monitoramento baseado na rede que não usa recursos dos servidores de bancos de dados monitorados. Por meio de sistemas de espelhamento dos pacotes, o serviço evita que até mesmo a rede sofra qualquer impacto.
- **Escalabilidade** Disponibiliza arquitetura flexível para ambientes heterogêneos e distribuídos com até milhares de bancos de dados.
- **Cobertura** Atende aos principais bancos de dados do mercado, tanto da Baixa como da Alta Plataforma. Desde bancos comerciais como o Oracle até bancos de software livre como o MySQL.
- **Segurança** Controle de riscos operacionais de infra-estrutura e de recursos humanos. Somente pessoas autorizadas têm acesso às salas de monitoramento com um sistema de segurança por câmeras e equipamentos bloqueados contra vazamento de informações.

Todas as trilhas de auditoria geradas pelo serviço de monitoramento são devidamente guardadas em cofres especialmente construídos para o armazenamento de mídias magnéticas e a prova de fogo. Servidores redundantes e com tolerância à falhas de energia garantem a disponibilidade do serviço.

**Atividades da Célula de Monitoramento:** Os serviços prestados pela equipe XTI 24 horas por dia e 7 dias por semana através da célula de monitoramento são:

- **Desenvolvimento:** consultoria e implementação de rotinas específicas para o negócio do cliente relativo à segurança dos dados. Exemplo: intervenção na implementação dos sistemas WEB do cliente para visualizar os usuários finais da aplicação na internet.
- **Alertas e Suporte Técnico:** as atividades suspeitas realizadas nos bancos são informadas em tempo real ao cliente via SMS, e-mail, fax ou celular em conversa direta com o analista de segurança responsável pelo monitoramento. Suporte técnico da XTI na correção emergencial da infra-estrutura monitorada.
- **Relatórios e Análise de padrões:** voltados para auditoria e suporte à tomada de decisão da empresa.

### Especificações Técnicas

#### Plataformas:

Baixa Plataforma e Mainframe.

#### Regulamentações Atendidas:

Sarbanes-Oxley, ISO 17799, CobiT, ITIL, Basiléia II, HIPPA, PIPEDA, FERC/NERC, Cartão Master Card, Cartões Amex e Visa.

#### Bancos de Dados Monitorados:

ADABAS, Caché, DB2, MySQL, PostgreSQL, Oracle, Teradata, Informix, Sybase IQ, MS SQL Server.

#### Eventos Registrados:

Origem do acesso, qual máquina, qual IP, localização geográfica, qual usuário (inclusive da camada de apresentação WEB), quando, durante quanto tempo, com quais ferramentas, mudanças em esquemas de dados com Create, Drop e Alter, mudanças em dados com Insert, Update e Delete, acessos a Dados com Select e Execute, Eventos de Segurança com Grant, Revoke e Deny. Logins válidos, inválidos ou falhos, Logout, sessão rejeitada, Shutdown, Reboots e erros de sistema, Restore e Backup dos Bancos, Alocação de Objetos, Tentativas de acesso ao sistema operacional através do banco, estatísticas de uso de disco, tabelas bloqueadas, espaço disponível, memória e muito mais.

### Resultados Obtidos

- Introdução da cultura de Processo de Segurança de Dados na Empresa.
- Inibição de ações maliciosas contra as Informações Críticas da Empresa.
- Fortalecimento da Imagem do cliente junto ao governo e sociedade como uma instituição segura e confiável.
- Aumento da receita percebida pelo cliente com a diminuição de fraudes no processo de negócio.
- Atendimento facilitado das exigências de segurança requeridas pelos órgãos fiscalizadores como, por exemplo, o TCU em futuras auditorias.
- Atendimento das normas internacionais de segurança da informação como SOX, ABNT 17799 / ISO 27001, Basiléia II, PCI, HIPPA etc.
- Identificação dos pontos de vulnerabilidade da instituição para que sejam tomadas medidas de correção.

