

## Caroline Luchtenberg Ribeiro

---

**De:** BERNARDES Fabio [fabio.bernardes@thalesgroup.com]  
**Enviado em:** sexta-feira, 27 de abril de 2018 17:09  
**Para:** ADM Afis  
**Assunto:** Audiência Pública 01/2018 - recomendação técnica  
**Anexos:** image001.jpg  
  
**Prioridade:** Alta

Prezados Senhores,  
em atenção ao disposto na Ata de Audiência Pública 01/2018, referente ao Projeto de Modernização do sistema ABIS da Polícia Federal, temos a contribuir com as seguintes sugestões:

- No item 6.1.10 – “Módulo de Monitoramento”, sugerimos alterar o título para “6.1.10 – Módulo de Monitoramento e Proteção de Dados Sensíveis (cybersegurança)”.
- No item 6.1.10, incluir especificação técnica que trate da proteção dos dados biométricos e biográficos armazenados nos sistema ABIS, baseado na justificativa abaixo:

Tomamos a liberdade de propor uma solução de criptografia e controle dos acessos à tal informação, face a experiência da Thales em projetos de similar ou ainda maior complexidade, por exemplo proteção de transações bancárias, mercado onde a Thales é líder mundial. Nossa expectativa é apresentar um controle eficiente para proteção dos dados biométricos e biográficos (“dados sensíveis”) do sistema ABIS, garantindo o uso dos mesmos dentro dos procedimentos autorizados pela DPF e evitar assim o seu uso indevido, dentro de um valor de investimento relativamente superficial em relação ao investimento total esperado para o Projeto. Atualmente, os custos associados ao vazamento de informações sensíveis são muito altos, tanto os tangíveis (sistemas sequestrados fora de operação, restauração de ambientes e de bases de dados, gastos com processos civis e criminais, ...) quanto os intangíveis (imagem da organização,...).  
Desta forma, seguem nossas recomendações:

**= sugerimos incluir como segundo parágrafo no item 6.1.10**

*“- A solução proposta deve incluir componente para proteção de dados sensíveis – biométricos e biográficos, contemplando quaisquer dados armazenados no Sistema Operacional das estações/sítios relacionados diretamente ao Sistema ABIS, através de uma abordagem de criptografia transparente, com o objetivo de introduzir um controle eficiente para a proteção dos dados biométricos e biográficos e garantir o uso dos mesmos dentro dos procedimentos autorizados pela DPF e evitar seu uso indevido como o vazamento e manipulação dos mesmos”.*

**= Como “Requisitos técnicos e funcionais”, sugerimos incluir no item 6.1.10:**

*“Proteção de Dados Sensíveis:*

*Um agente de software deve ser adicionado ao Sistema Operacional de cada estação para monitorar todas as chamadas de E/S no sistema de arquivos, autorizando somente as operações previamente configuradas para realização por um usuário e aplicação específicos. Em outras palavras, somente a aplicação autorizada poderá escrever nas pastas designadas para armazenar os arquivos (de vídeo, texto, etc.), com as credenciais do usuário autorizado, podendo ser um usuário de sistema (nem mesmo superusuários, como administradores, poderão contornar este controle).*

*Para consulta pelo sistema central, as operações de leitura podem ser designadas para uma outra aplicação, com credenciais de outro usuário, controlando e monitorando o acesso aos arquivos.  
Tentativas de acesso não autorizados são reportados através de protocolo syslog para sistemas do tipo SIEM usado pela DPF.*

A implementação deve ser realizada através de “configuração” e “parametrização”, sem necessidade de nenhuma customização das aplicações em nível de código e sem comprometimento dos níveis de serviço de performance e disponibilidade definidos nesta especificação.

Módulos mínimos a serem incluídos na solução de proteção de dados sensíveis:

**- Módulo Gerenciador de Segurança**

Sistema que centraliza as funções de gerenciamento de chaves criptográficas (key management) em harmonia com as melhores práticas do mercado para segurança de chaves criptográficas (FIPS 140-2 L3). Concentra também as configurações dos parâmetros operacionais para os agentes de criptografia transparente, incluindo mapeamento das pastas protegidas, identificação dos programas e usuários autorizados, além dos tipos de operação autorizada para cada usuário nas pastas e arquivos protegidos.

Especificações técnicas:

- Interface administrativa: Secure Web, CLI, SOAP, REST
- Suporte API: PKCS #11, Microsoft Extensible Key Management (EKM), SOAP, REST
- Autenticação de Segurança: Username/Password, RSA multi-factor authentication (opcional)
- Suporte a plataforma de virtualização: VMWare, Hyper-V e ‘bare metal’ via IBM SoftLayer
- Gestão de redes: SNMP, NTP, Syslog-TCP
- Formato Syslog: CEF, LEEF, RFC 5424.
- Certificações e validações: FIPS 140-2 Level 3
- Suporte Multi-tenancy

**- Módulo de Criptografia Transparente**

Agente de software a ser adicionado ao Sistema Operacional de cada estação/sítio, para monitoramento das operações de E/S ao sistema de arquivos. Este agente receberá as chaves de operação (“working Keys”) do Módulo Gerenciador de Segurança, bem como as regras de operação e políticas de controle de acesso. Tentativas de acesso não autorizado serão identificadas por este agente e enviadas ao Módulo Gerenciador de Segurança, para repasse ao sistema SIEM.

Especificações técnicas:

- Plataformas suportadas: Microsoft Windows Server 2008, 2012 e 2016, Red Hat Enterprise Linux (RHEL), SuSE Linux Enterprise Server & Ubuntu
- Bancos de dados suportados: Microsoft SQL Server, MySQL, NoSQL, Oracle, Sybase.
- Suporte a Containers: Docker, Red Hat Open Shift
- Certificações e Validações: FIPS 140-2 Level 1
- Suporte a chaves criptográficas: AES128, AES256, ARIA128, ARIA256, and 3DES
- Autenticação via Lightweight Directory Access Protocol (LDAP) e Active Directory (AD)”

Sem mais, ficamos a disposição de V.Sas. para realizar uma reunião de detalhamento de nossa visão e sugestão sobre a implementação desta tecnologia de proteção de dados sensíveis, atualmente em uso por organizações bancárias em todo o mundo e por outras sujeitas à regulações fortes como as do mercado norte americano e europeu (ex. GDPR).

Atenciosamente,

**Fabio Bernardes**

**KAM/Sales Manager, Security Market**

Mobile: +55 (11) 9.6486-0589

e-mail: [fabio.bernardes@thalesgroup.com](mailto:fabio.bernardes@thalesgroup.com)  
[www.thalesgroup.com](http://www.thalesgroup.com)

**THALES**