TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Auditoria no Sistema Nacional de Integração de Informações em Justiça e Segurança Pública - Infoseg

República Federativa do Brasil

Tribunal de Contas da União

Ministros

Walton Alencar Rodrigues, Presidente
Ubiratan Aguiar, Vice-Presidente
Marcos Vinicios Vilaça
Valmir Campelo
Guilherme Palmeira
Benjamin Zymler
Augusto Nardes
Aroldo Cedraz
Raimundo Carreiro

Auditores

Augusto Sherman Cavalcanti
Marcos Bemquerer Costa
André Luís de Carvalho

Ministério Público

Lucas Rocha Furtado, Procurador-Geral
Paulo Soares Bugarin, Subprocurador-Geral
Maria Alzira Ferreira, Subprocuradora-Geral
Marinus Eduardo de Vries Marsico, Procurador
Cristina Machado da Costa e Silva, Procuradora
Júlio Marcelo de Oliveira, Procurador
Sérgio Ricardo Costa Caribé, Procurador

Negócio
Controle Externo da Administração Pública
e da gestão dos recursos públicos federais

Missão
Assegurar a efetiva e regular gestão dos
recursos públicos em benefício da sociedade

Visão
Ser instituição de excelência no controle e contribuir
para o aperfeiçoamento da Administração Pública

TRIBUNAL DE CONTAS DA UNIÃO

Sumários Executivos

Auditoria no Sistema Nacional de Integração de Informações em Justiça e Segurança Pública - Infoseg

Relator
Auditor Augusto Sherman Cavalcanti

Brasília, Brasil 2007

Impresso no Brasil / Printed in Brazil
1ª Reimpressão - 2008

<www.tcu.gov.br>

Para leitura completa do Relatório, do Voto e do Acórdão nº 71/2007 - TCU – Plenário, acesse a página do TCU na Internet, no seguinte endereço:

<www.tcu.gov.br/fiscalizacaoti>

Brasil. Tribunal de Contas da União.

Auditoria no Sistema Nacional de Integração de Informações em Justiça e Segurança Pública : Infoseg / Tribunal de Contas da União; Relator Auditor Augusto Sherman Cavalcanti . – Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007.

p. 45 – (Sumários Executivos. Nova Série ; 14)

1. Segurança pública. 2. Polícia. 3. Sistema de Informação Criminal. 4. Sistema Nacional de Integração de Informações de Justiça e Segurança Pública. I. Título. II. Série.

Catalogação na fonte: Biblioteca Ministro Ruben Rosa

SUMÁRIO

APRESENTAÇÃO

Os sumários executivos da Secretaria de Fiscalização de Tecnologia da Informação (Sefti), editados pelo Tribunal de Contas da União, têm por objetivo divulgar os principais resultados das fiscalizações de Tecnologia da Informação realizadas pela Sefti. As publicações contêm, de forma resumida, aspectos importantes verificados durante auditorias, recomendações e determinações para melhorar a governança de tecnologia da informação na Administração Pública Federal, e boas práticas identificadas.

O foco das fiscalizações de Tecnologia da Informação (TI) realizadas pela Sefti é a verificação da conformidade e do desempenho das ações governamentais nessa área, a partir de análises sistemáticas de informações sobre aspectos de governança, segurança e aquisições de bens e serviços de TI, utilizando critérios fundamentados. O principal objetivo dessas fiscalizações é contribuir para o aperfeiçoamento da gestão pública, para assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

Pretende-se, com a divulgação desses trabalhos, oferecer aos parlamentares, aos órgãos governamentais, à sociedade civil e às organizações não-governamentais informações suficientes e fidedignas para que possam exercer o controle das ações de governo.

Este número traz as principais informações sobre a auditoria realizada no Sistema Nacional de Integração de Informações em Justiça e Segurança Pública - Infoseg, de responsabilidade da Secretaria Nacional de Segurança Pública do Ministério da Justiça (Senasp/MJ). Este processo (TC 003.293/2006-3) foi apreciado em sessão do Plenário de 31 de janeiro de 2007, sob a relatoria do Auditor Augusto Sherman Cavalcanti.

Walton Alencar Rodrigues
Ministro-Presidente

RESUMO

O Sistema Nacional de Integração de Informações em Justiça e Segurança Pública (Infoseg) tem por finalidade integrar e prover de informações os órgãos de segurança pública, justiça e fiscalização da União, dos Estados e do Distrito Federal.

Considerando que o tema segurança pública encontra-se presente na agenda da sociedade brasileira e que auditoria anterior do TCU havia detectado dificuldades na implantação de tão importante sistema, o Tribunal realizou essa auditoria com objetivo de avaliar aspectos relacionados com a segurança e consistência das informações gerenciadas pelo Infoseg.

O TCU constatou graves impropriedades no sistema, sobretudo no que concerne à sua gestão, tais como: insuficiência de regulamentação, inconsistências entre as bases de dados criminais das unidades da Federação e o Índice Nacional (IN), que, além de desacreditar a confiabilidade do sistema, podem provocar conseqüências sérias como a prisão indevida de um cidadão ou a não prisão de um criminoso.

Na busca do aperfeiçoamento do Infoseg, que constitui um poderoso instrumento cuja utilização poderá contribuir para a tempestividade, eficiência e eficácia das ações de fiscalização, de segurança pública e de justiça, o TCU recomendou a institucionalização do sistema por meio de lei federal. O Tribunal determinou à Secretaria Nacional de Segurança Pública (Senasp), entre outras medidas, a correção das falhas que geram as inconsistências entre as bases de dados criminais das unidades da Federação e o IN e a elaboração de políticas de segurança de informação e de controle de acesso.

SISTEMA NACIONAL DE INTEGRAÇÃO DE INFORMAÇÕES EM JUSTIÇA E SEGURANÇA PÚBLICA (INFOSEG)

De acordo com o princípio Federativo da Constituição Federal do Brasil, os estados possuem autonomia na área de segurança pública para gerir suas próprias polícias e administrar as informações a ela pertinentes. Essa autonomia traz, como resultado, a existência de diferentes sistemas de informações criminais para cada estado da Federação, para a Polícia Federal, Justiças Estaduais e Justiça Federal.

Por força de dispositivos legais, coube à Secretaria Nacional de Segurança Pública do Ministério da Justiça (Senasp/MJ) o desenvolvimento e a manutenção do Sistema Nacional de Integração de Informações de Justiça e Segurança Pública (Infoseg).

O Infoseg tem por objetivo a integração e disponibilização das informações dos órgãos de segurança pública, justiça e fiscalização da União, dos Estados e do Distrito Federal, por meio de quatro módulos de consulta que contêm dados sobre inquéritos, processos e mandados de prisão (módulo Indivíduos), armas de fogo (módulo Armas), veículos (módulo Veículos) e condutores (módulo Condutores). O sistema disponibiliza essas informações para os agentes públicos federais, estaduais, distritais e municipais cadastrados por meio de consultas à Internet.

No caso do módulo Indivíduos, o sistema utiliza um Índice Nacional (IN) que consiste em um indexador das informações básicas sobre indivíduos (existência de inquéritos, processos, mandados de prisão etc.) de todo o país. Após a pesquisa inicial no IN, é possível obter o detalhamento dessas informações por meio de um link que acessa as bases estaduais de origem ("consultas detalhadas"), mantendo a autonomia dos estados em relação às suas informações detalhadas. Dessa forma, o Infoseg concentra, em sua base de dados, apenas as informações básicas (Índice Nacional) que apontam para as fontes de dados dos estados, e estes continuam utilizando seus sistemas de informações criminais.

Os módulos de Armas, Condutores e Veículos disponibilizam o acesso ao usuário da rede Infoseg , de acordo com seu perfil, diretamente às bases do SINARM (Sistema Nacional de Armas mantido pelo Departamento de Polícia Federal – DPF), RENACH (Registro Nacional de Carteiras de Habilitação mantido pelo Departamento Nacional de Trânsito – Denatran) e RENAVAM (Registro Nacional de Veículos Automotores também mantido pelo Denatran).

A Senasp firmou convênios com outros órgãos federais para possibilitar a integração à rede Infoseg de sistemas de interesse da segurança pública, da justiça e dos órgãos de fiscalização, como ocorreu com a Receita Federal (bases CPF e CNPJ) e o Superior Tribunal de Justiça e a Justiça Federal (base Estratégia Nacional de Combate à Corrupção e a Lavagem de Dinheiro – ENCCLA).

A alimentação dos dados na base do Índice Nacional é feita por uma "solução de atualização" e, na medida que a base de dados do estado sofre uma atualização, é gerado um registro atualizado no Índice Nacional da base de Indivíduos da rede Infoseg. No primeiro semestre de 2006, época da realização da auditoria, vinte e seis estados atualizavam o IN dessa forma e o estado de São Paulo estava em processo final para implantar a atualização *on-line*. Assim, a base de dados do Índice Nacional deveria refletir a realidade das bases estaduais, integrando e disponibilizando as informações criminais para consulta via Internet, apoiando o trabalho dos profissionais de segurança pública, justiça e fiscalização em todo o país.

O que foi avaliado pelo TCU

O objetivo da auditoria do TCU foi avaliar os aspectos relacionados com a segurança e a consistência das informações gerenciadas pelo Infoseg. A segurança da informação visa protegê-las de ameaças e reduzir vulnerabilidades para garantir a continuidade das atividades da organização, minimizando os danos acidentais ou propositais. De acordo com a NBR

ISO/IEC 17799:2001[1] , para garantir a segurança da informação, é necessária a preservação de:

- confidencialidade – garantia de que a informação seja obtida somente por pessoas autorizadas;
- integridade – salvaguarda da exatidão e completeza da informação e dos métodos de processamento;
- disponibilidade – garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Dos quatro módulos do Infoseg, três são apenas consultas a bases geridas por outros entes públicos (Condutores e Veículos consultam a base do Denatran e Armas consulta a base do DPF). O módulo Indivíduos, que utiliza um índice de bases distribuídas por órgãos nas diversas Unidades da Federação (UF), é o módulo mais complexo, cuja base (Índice Nacional – IN) é de responsabilidade da Senasp. A consistência entre os dados constantes do IN e os constantes das bases dos órgãos que alimentam o sistema é um fator crítico para o sucesso do sistema, pois garante que as bases de dados dos agentes de segurança pública nas diversas UF e o IN possuam exatamente a mesma informação em um determinado instante. Por tais motivos, o foco da auditoria foi o módulo Indivíduos do Infoseg, mais especificamente as atualizações e consultas ao Índice Nacional, visto que, à época da auditoria, ainda existiam diversos estados que não disponibilizavam as consultas detalhadas aos indivíduos.

Para orientar a execução da auditoria, foram formuladas questões de auditoria contemplando a consistência das informações encontradas no Índice Nacional, a Política de Segurança da Informação estabelecida pelo Ministério da Justiça, a Política de Controle de Acesso à gerência e ao sistema Infoseg, a estrutura dos recursos humanos e os contratos de prestação de serviço para a plataforma do Infoseg, a existência de um Plano de Continuidade de Negócios compatível com as necessidades operacionais do Infoseg e a satisfação dos usuários quanto à usabilidade do sistema Infoseg.

Não foram objeto do escopo da auditoria os atos de gestão não relacionados ao sistema Infoseg, a legalidade de contratações e de convênios firmados no âmbito do Infoseg, a gestão de sistemas e de segurança da informação no âmbito dos entes que participam do Infoseg atualizando o Índice Nacional, a gestão de sistemas e de segurança da informação no âmbito da Coordenação Geral de Tecnologia da Informação do Ministério da Justiça (CGTI/MJ).

Por que foi avaliado

A Auditoria operacional[2] realizada durante o exercício de 2004 pelo TCU no programa Sistema Único de Segurança Pública (SUSP) identificou que havia problemas enfrentados pela Senasp e pelos estados na implantação do Infoseg, de forma que o Plenário desta Corte de Contas, por meio do Acórdão nº 724/2005 – TCU – Plenário, determinou a realização de auditoria naquele sistema.

Como se desenvolveu o trabalho

Durante o planejamento da auditoria, a equipe de auditoria realizou diversas reuniões com os gestores do sistema nas instalações da Secretaria Nacional de Segurança Pública (Senasp) onde o sistema funciona. A estrutura que suporta o Infoseg não existe formalmente na Senasp, motivo pelo qual será utilizada, neste documento, a expressão "gerência do Infoseg" para referí-la.

Na fase de execução da auditoria, foram visitadas instituições nos estados do Ceará, de Pernambuco, do Rio Grande do Sul e do Pará, do Distrito Federal e o Departamento de Polícia Federal. Na Região Nordeste, Pernambuco foi escolhido por manter o equipamento de redundância da base de dados do IN e o Ceará por ter tido um dos maiores avanços na sua solução de integração, segundo informações dos gerentes do Infoseg. Na região Sul, a opção pelo Rio Grande do Sul deveu-se ao fato de que foi naquele estado que o Infoseg teve sua primeira versão desenvolvida.

O estado do Pará, na região Norte, foi escolhido por apresentar número bem reduzido de registros (cerca de 16.000 em 02.03.2006) e existirem relatos dos gestores da Senasp de problemas de quedas freqüentes do serviço de conexão prestado pela Embratel. Na Região Centro-Oeste, a escolha recaiu sobre o DF e o DPF, devido à sua localização próxima ao TCU.

O estado de São Paulo, que possui o maior número de registros no IN, seria o representante natural da Região Sudeste, mas não foi escolhido por ainda não estar atualizando o Índice Nacional (IN) de forma *on-line*.

Nessas visitas, a equipe verificou o estado e as condições de uso dos equipamentos da Senasp cedidos às unidades daqueles entes que integram o Infoseg, buscou conhecer as soluções de integração desenvolvidas por eles e solicitou extração das informações constantes de suas bases criminais para verificar a consistência com as constantes do IN, ponto que a equipe definiu como de maior relevância para este trabalho, visto que significa avaliar se o sistema atinge seus objetivos ou não.

Para efetuar o cruzamento de dados foi solicitada à Senasp a extração da base do IN, a qual foi realizada em 02.03.2006. Durante as visitas citadas, como as Secretarias de Segurança Pública Estaduais visitadas não são jurisdicionadas ao TCU, foi solicitado, por meio da Senasp, acesso aos dados constantes das bases criminais que eram necessários aos cruzamentos desejados.

Como a data de extração da base criminal estadual era posterior à da extração do Índice Nacional, foram realizados ajustes, com apoio dos técnicos estaduais, de forma a obter os dados que estavam na base criminal em 02.03.2006, data da extração do IN. Após o ajuste, a equipe realizou o cruzamento dos dados, com apoio do *software* ACL, verificando a existência de inconsistências.

Ainda durante as visitas, foi validada, juntamente com os técnicos estaduais, a existência das inconsistências, por meio de consultas ao Infoseg e

aos sistemas criminais estaduais, e foram entregues aos técnicos os arquivos que evidenciavam as inconsistências detectadas. Por fim, foi comunicada formalmente a existência das inconsistências para que fossem logo adotadas as medidas corretivas.

Considerando as diferentes plataformas tecnológicas envolvidas, a diversidade de soluções encontradas (cada ente visitado implementou sua solução de integração de forma diferente) e os ajustes necessários, conforme descrito acima, os procedimentos de cruzamentos de dados não foram precisamente os mesmos, o que não traz prejuízo aos resultados obtidos, qual seja, há evidências de inconsistências entre as bases de dados analisadas, conforme registrado mais adiante.

Houve limitação aos trabalhos de cruzamento de dados do IN com as bases do estado de Pernambuco e do Departamento de Polícia Federal, devido ao atraso para entrega dos dados, o que não chegou a inviabilizar o trabalho. Nenhuma outra restrição foi imposta aos trabalhos da auditoria.

Foram solicitados ainda diversos documentos relacionados ao desenvolvimento, à manutenção e à operação do Sistema, à segurança da informação e aos usuários do Infoseg. Seguindo as boas práticas de auditoria, buscou-se certificar a veracidade das informações constantes dos documentos, por meio de entrevistas, acessos aos módulos do Sistema e visitas às instalações da Senasp e dos entes citados.

Para conhecer a opinião dos usuários do sistema Infoseg, foi elaborado um questionário eletrônico sobre a satisfação dos usuários quanto à utilização dos quatro módulos de consulta do sistema. O questionário pôde ser respondido entre os dias 10.04.2006 e 03.05.2006. As respostas tabuladas foram usadas como base para as conclusões acerca das impressões do usuário sobre o sistema.

Registre-se que, por se tratar de auditoria de sistemas, foram utilizados, como critérios de auditoria, os controles previstos na norma NBR ISO/IEC

17799:2005 e no COBIT – *Control OBjectives for Information and related Technology* (versão 4.0). A norma NBR ISO/IEC 17799:2005 é o Código de Prática para a Gestão da Segurança da Informação mais adotado em todo o mundo, foi nacionalizado pela Associação Brasileira de Normas Técnicas (ABNT) em 30.09.2001. Essa norma fornece recomendações para gestão da segurança da informação, preconizando seu uso pelos responsáveis pela implementação e manutenção da segurança em suas organizações. Tem como propósito prover uma base comum para o desenvolvimento de normas de segurança organizacional e das práticas efetivas de gestão da segurança.

O COBIT destina-se a prover um modelo de boas práticas para Governança de Tecnologia da Informação e organiza seus objetivos de controle[3] em quatro grandes grupos: Planejamento e Organização, Aquisição e Implementação, Entrega e Suporte, e Monitoração. Cabe salientar que esses modelos e padrões são amplamente reconhecidos e utilizados, no Brasil e no mundo, no âmbito da tecnologia da informação, tanto por gerentes de informática quanto por auditores de TI.

O QUE O TCU ENCONTROU

Insuficiência de legislação aplicável

O Índice Nacional (IN), núcleo do Infoseg, é composto por informações oriundas de diversos órgãos de segurança pública, citados no art. 144 da Constituição Federal (polícia federal, polícia rodoviária federal, polícias civis e militares estaduais e distritais), bem como de órgãos do Poder Judiciário (Superior Tribunal de Justiça, Tribunais de Justiça e Justiça Federal), que são entes participantes do sistema.

Apesar de as informações constantes do Índice Nacional serem provenientes de órgãos de diferentes poderes (Executivo e Judiciário) e de diferentes esferas de governo (Federal, Estadual e Distrital), não foi identificado um normativo que instituiu o Infoseg, mas somente o Decreto s/nº, de 26.09.1995, que define, para o programa, seus objetivos, seus participantes,

os cadastros que o constituirão, os recursos para o seu desenvolvimento, e dispõe o seguinte:

> "Art. 1º Fica criado, no âmbito do Ministério da Justiça, o Programa de Integração das Informações Criminais, que tem por objetivos:
>
> I - Integrar as informações criminais, por intermédio de rede informatizada;
>
> II - estreitar a cooperação com os estados.
>
> Art. 2º Participarão do Programa os órgãos de segurança federais e, mediante convênio de cooperação técnica entre a União e os estados, os demais órgãos previstos no art. 144, da Constituição , para consecução dos objetivos de que trata o artigo anterior.
>
> Art. 3º O Programa será constituído pelos Cadastros Nacionais e Estaduais de Informações Criminais, de Mandados de Prisão, de Armas de Fogo e de Veículos Roubados e Furtados.
>
> Art. 4º O Programa contará com recursos da União e apoio técnico dos órgãos públicos envolvidos diretamente com os cadastros descritos no artigo anterior."

A Portaria do Ministro da Justiça nº 1.542, de 08.12.1995, atribuiu, ao Departamento de Assuntos de Segurança Pública, da Secretaria de Planejamento de Ações Nacionais de Segurança Pública do Ministério da Justiça, a coordenação do Programa criado pelo Decreto supra, especificando ainda que sua concepção deveria ser descentralizada, respeitando a autonomia de cada ente participante, e as bases de dados de cada ente participante continuariam sob a gerência e responsabilidade do ente. A competência para desenvolver o Infoseg foi atribuída à Senasp, conforme consta do inciso X, do art. 12, do Decreto nº 5.834, de 06.07.2006 – Regimento do Ministério da Justiça.

Com relação aos convênios previstos no Decreto s/nº, de 26.09.1995, foram identificados termos de convênio firmados entre a Senasp e os 26 estados e o Distrito Federal para repasses de recursos do Fundo Nacional de Segurança Pública (FUSP), os quais prevêem a viabilização do acesso ao Infoseg por diversos entes e a obrigação de o convenente atualizar o Índice Nacional pelo menos duas vezes por mês. Não há outras cláusulas nos convênios tratando do Infoseg.

Ainda que exista normatização para o Programa de Integração das Informações Criminais, com relação ao sistema Infoseg, foram apenas identificadas a normatização da competência da Senasp para desenvolvê-lo e a obrigação de os convenentes que recebem recursos do FUSP viabilizarem o acesso ao sistema e atualizarem-no pelo menos duas vezes por mês.

Registre-se a precariedade dos escassos dispositivos existentes, visto que não é definido 'o que é o sistema Infoseg' que a Senasp deve desenvolver, o que é 'viabilizar o acesso' ao sistema e o que é considerado 'atualizar' o Índice Nacional, obrigações estabelecidas nos termos de convênio mencionados.

Destarte, fica evidente a ausência de regulamentação para o funcionamento de um sistema de grande importância para a segurança pública do país. Não existem definições formais e claras do que é o sistema Infoseg, quem deve fornecer suas informações, quem são seus usuários, tampouco o estabelecimento de atribuições e responsabilidades. Foi constatado que, devido à ausência de normatização, o sistema foi desenvolvido e encontra-se em execução por causa da cooperação, muitas vezes informal, entre a Senasp e os órgãos de segurança pública do país.

Há registros no Ministério da Justiça de que a participação de diversos estados na alimentação do Índice Nacional ocorreu apenas após a comunicação da possibilidade de suspensão do repasse de verbas do FUSP para os estados conveniados, sendo este o único mecanismo que permite ao órgão responsável pelo sistema (Senasp) cobrar responsabilidade dos entes participantes. Não há qualquer atribuição ou responsabilidade formalmente estabelecida para os órgãos do Poder Judiciário, que são detentores de informações de interesse do sistema (mandados de prisão e processo).

Considerando os princípios da Legalidade, da Federação e da Separação de Poderes, o sistema Infoseg deve ser instituído por lei, por ser esta a espécie capaz de institucionalizá-lo nos diversos entes, e não por legislação infralegal, como precariamente ocorre. A título de exemplo, registre-se que o Registro Nacional de Carteiras de Habilitação (RENACH) e o Registro

Nacional de Veículos Automotores (RENAVAM) são sistemas cujos participantes são entes de diversas esferas de governo e que são institucionalizados por lei, no caso, o Código Brasileiro de Trânsito - CBT (Lei nº 9.503/97).

Inconsistências entre as bases de dados criminais e o Índice Nacional

Durante a auditoria do sistema Infoseg, foram realizadas visitas a 6 (seis) dos 29 (vinte e nove) entes que atualizam informações no Índice Nacional (IN). O objetivo dessas visitas foi realizar o cruzamento das informações constantes das bases de dados criminais desses entes com as constantes do IN, com vistas a identificar possíveis inconsistências.

Em todos os entes visitados, foram constatadas inconsistências entre as informações constantes das bases dos entes e da base do IN. Registre-se que todos os entes visitados já haviam realizado, pelo menos uma vez, a operação de recarga da base, quando foi solicitado à Senasp que excluísse todos os registros daquele ente, para que pudessem ser incluídas informações consistentes.

As inconsistências encontradas evidenciam controles de processamento insuficientes[4] e podem ser divididas em três grupos: registros constantes do IN sem correspondência nas bases do ente, registros constantes das bases do ente sem correspondência no IN e registros constantes das bases do ente e do IN, porém com conteúdos divergentes.

A solução de atualização para o Índice Nacional que os entes visitados desenvolveram depende da plataforma que cada um deles utiliza nos seus sistemas criminais. Ainda que com diferentes tecnologias, todos os entes visitados utilizam basicamente o mesmo paradigma na solução de atualização, a qual podemos dividir em duas etapas:

1) quando ocorre no sistema criminal do ente uma operação que insere, altera ou remove uma informação que é de interesse do Infoseg, a

informação é colocada em uma tabela que genericamente é chamada de "espelho do Infoseg";
2) posteriormente, uma aplicação lê a informação da tabela "espelho do Infoseg" e realiza a atualização do IN.

Apesar de não ser possível inferir se há entes cuja solução de atualização seja melhor que a de outros, foi constatado que todas as soluções vistas apresentam falhas que geram informações de baixa confiabilidade na base do Índice Nacional, o que prejudica a qualidade da informação que é disponibilizada aos agentes de segurança pública por meio do Infoseg para tomada de decisão.

Outra possível fonte de inconsistência encontrada no Índice Nacional são as informações do IN sobre mandados de prisão e processos, originadas nos Tribunais de Justiça dos estados, que são encaminhadas à Senasp pelo ente do Poder Executivo Estadual que alimenta o Infoseg. Nas Unidades da Federação visitadas, as informações sobre mandados de prisão não chegam em meio magnético aos órgãos de segurança pública, sendo necessária a sua digitação para constar dos sistemas criminais estaduais (que por sua vez alimentam o Infoseg). Há possibilidade de falha humana na digitação, que pode ocasionar erros na identificação dos indivíduos e, ainda que não fosse causa de inconsistências, o lapso temporal entre a emissão dos mandados nos Tribunais de Justiça e sua inclusão nos sistemas criminais estaduais pode chegar a dias, prejudicando a tempestividade da ação policial.

Até o fim dos trabalhos da equipe de auditoria, nenhum tipo de auditoria na consistência dos dados do Índice Nacional havia sido empreendida pela Senasp[5].

Com objetivo de ilustrar os efeitos das inconsistências anotadas nesta seção, registram-se dois fatos noticiados na imprensa em 2003 e 2004. No primeiro[6], veiculado no Jornal do Brasil em 27.06.2004, a cidadã Vânia Abrantes foi detida indevidamente em uma delegacia policial em Copaca-

bana, no estado do Rio de Janeiro, quando tentava registrar um extravio de cheques em 14.12.2003. Segundo a reportagem, o ocorrido deveu-se a um mandado de prisão inserido pelo estado de São Paulo no Infoseg, que o estado alegou não conseguir retirar do sistema. Em procedimento de rotina, os policiais fluminenses consultaram o nome da Srª Vânia no Infoseg, onde constava um mandado de prisão em aberto, sem dados sobre a acusação nem o número do processo. A inocente passou uma noite presa e entrou com ação indenizatória contra a União, por ter seu nome no cadastro do Infoseg; contra o estado de São Paulo, por tê-lo incluído; e contra o estado do Rio de Janeiro, por tê-la prendido.

Outro caso[7], este com grande repercussão nacional, foi o ocorrido no estado do Rio Grande do Sul em 2003, onde Adriano da Silva, foragido de um presídio do estado do Paraná, teria sido preso e solto pela polícia do Rio Grande do Sul, que não teria conseguido identificá-lo no Infoseg. A reportagem da Folha *on-line* registra a informação do secretário de segurança pública do Paraná de que seu estado, em abril de 2002, já havia informado à Senasp acerca de problemas de compatibilidade para alimentar o Infoseg.

Ainda que as situações narradas acima tenham ocorrido antes da reestruturação promovida pela Senasp no Infoseg, as evidências apresentadas por esta equipe de auditoria (registros contendo inconsistências) atestam que esses fatos podem voltar a acontecer. Sem entrar no mérito de outros aspectos envolvidos nos dois casos escritos acima e sem a intenção de atribuir as ocorrências exclusivamente a falhas no sistema Infoseg, o que se busca ilustrar são algumas das possíveis conseqüências das inconsistências que se evidenciam, quais sejam, um cidadão inocente ser preso indevidamente ou um criminoso ser parado pela polícia e deixar de ser preso.

Indefinição dos significados das informações que compõem o Índice Nacional (IN)

Durante os trabalhos da auditoria, não foi identificada a definição do conteúdo das "Informações Criminais" que, de acordo com o art. 3 do

Decreto s/nº, de 26.09.1995, devem constar do Infoseg. Também não foi demonstrada a existência do dicionário de dados[8] do Índice Nacional, tampouco a existência de documento formal, estabelecido entre a Senasp e os participantes do Infoseg, definindo a semântica dos campos do IN[9]. A indefinição dos significados dos campos do IN prejudica o entendimento comum dos dados entre o setor de TI e os usuários, e, principalmente, entre os diversos usuários do Infoseg (agentes de UF diferentes entendem a informação de forma diferente). A seguir seguem-se exemplos de dúvidas dos gestores dos entes visitados com relação ao significado dos campos do IN.

Campo: NARCOTRAFICO.

Descrição[10]: Identificador de envolvimento com narcotráfico.

Dúvidas: O envolvimento é caracterizado por um inquérito, por um processo, por um mandado de prisão, por uma condenação ou por qualquer uma dessas espécies?

Campo: PROCESSO.

Descrição: Identificador de Processo.

Dúvidas: Quais são os tipos de processos que devem ser encaminhados? Todos? Só os penais? E os de pensão alimentícia que podem gerar mandados de prisão?

Campo: INQUERITO.

Descrição: Identificador de Inquérito.

Dúvidas: Quais tipos de inquéritos devem ser enviados? Em quais situações? Inquéritos em andamento ou que tenham sido encaminhados ao Ministério Público? Os inquéritos encerrados também devem ser enviados?

Campo: MANDADO_PRISAO.

Descrição: Identificador de Mandado de Prisão.

Dúvidas: Somente os mandados de prisão que estão em aberto devem constar do IN ou em qualquer outra situação (revogado, suspenso, cumprido, etc.)? O que fazer quando as informações constantes do mandado que identificam o indivíduo são insuficientes para identificá-lo na base criminal?

Inexistência de políticas formalmente definidas

Quanto às políticas de segurança no âmbito do sistema Infoseg, a equipe de auditoria procurou identificar Políticas de Segurança da Informação[11] (PSI)e Política de Controle de Acesso[12] (PCA) para o Infoseg. A equipe certificou-se da existência de uma minuta de PSI, bem como da existência de documento denominado "Controle de Acesso Usuários *Web* – Infoseg".

A minuta de Política de Segurança da Informação é datada de 23.10.2003, quando a arquitetura do sistema era bem diferente da existente à época da auditoria (p.e., o sistema funcionava em uma Intranet e à época da auditoria as consultas ocorriam pela Internet). Além de desatualizado, o documento não foi formalmente aprovado nem divulgado às partes interessadas[13]. Ainda foi identificada a existência de uma PSI para o Ministério da Justiça (MJ), instituída por meio da Portaria do Ministro nº 279, de 10.03.2006. Ocorre que, como nem todos os usuários do Infoseg estão na estrutura do MJ, a PSI do MJ não é instrumento hábil para o Infoseg.

A Política de Controle de Acesso para usuários *Web* apresentada é difundida e utilizada no âmbito do Infoseg, entretanto falha por não ser formalmente institucionalizada e não contemplar uma análise crítica periódica dos direitos de acesso dos usuários[14] (não é previsto, por exemplo, o procedimento para cancelamento de contas de usuários). Além de não ter sido aprovada formalmente, a PCA encontrada não contempla as aplicações que são executadas nos módulos remotos e que atualizam o Índice Nacional e os usuários da rede interna da gerência do Infoseg.

A auditoria também verificou a inexistência de Metodologia de Desenvolvimento de Sistemas (MDS) formalmente aprovada para utilização no âmbito do Infoseg. Tal fato pode ocasionar problemas devido ao grande número de terceirizados da equipe.

Por fim, diante da insuficiência de normatização aplicável, não se pode identificar a responsabilidade quanto aos assuntos de segurança da informação no âmbito do Infoseg[15].

Procedimento inadequado de controle de mudanças no sistema

De acordo com Senasp/MJ, não existe procedimento formal de controle sobre as solicitações de alteração ou correção do sistema[16]. Os usuários fazem as demandas diretamente à gerência do Infoseg ou aos coordenadores administrativos, via e-mail ou por telefone. Não há um processo de análise qualitativa, nem priorização dessas demandas, havendo aprovação informal do diretor do projeto Infoseg. Essas demandas vão sendo atendidas de acordo com a disponibilidade da equipe de desenvolvimento. Porém, como a equipe é bastante reduzida, tal situação tem gerado um acúmulo de demandas não atendidas ou atendidas intempestivamente.

Dessa forma, inexiste mecanismo que permita aos usuários que originam as demandas de TI acompanharem os seus pedidos, não sendo possível saber quais desses estão sendo atendidos, quais estão aguardando ainda por serem iniciados, quais estão paralisados, qual é a prioridade e a ordem de atendimento e qual o tempo e o custo previstos e executados. Assim como não existe procedimento formal de controle das demandas, não existem critérios de aceitação definidos nem procedimento formal de homologação das versões[17] implantadas do Infoseg.

Inexistência de Plano de Continuidade de Negócio (PCN)

A auditoria não identificou a existência, no âmbito da gerência do Infoseg, de um Plano de Continuidade do Negócio[18] (PCN) ou procedimentos definidos que garantam, em caso de falhas ou desastres significa-

tivos, a retomada em tempo hábil das atividades do sistema, protegendo os processos críticos. É conveniente que o PCN inclua controles para identificar e reduzir riscos, limitar as conseqüências e danos em caso de incidentes e garanta que as informações requeridas para os processos críticos do negócio sejam recuperadas a contento, devendo ser testados e atualizados periodicamente[19].

Existe apenas uma replicação da base de dados do IN em Recife. No entanto, não há nenhum tipo de redundância dos serviços de atualização e consulta dessas bases, ou seja, não há um local alternativo que garanta a continuidade do sistema caso ocorra algum problema nas instalações da gerência do Infoseg. Essa estrutura totalmente centralizada aumenta a dificuldade de restauração e recuperação da operação do sistema em caso de uma falha, tornando ainda mais preocupante a inexistência do PCN.

Gestão insatisfatória das cópias de segurança

Foi verificada a existência de documento formal que define os procedimentos de rotina para gerar cópias de segurança dos dados que possibilitem sua recuperação em um tempo aceitável no caso de perda no âmbito do sistema Infoseg. Apesar de gerar cópias de segurança periodicamente, a gerência do Infoseg não possui uma política formal de geração dessas cópias[20], de forma que não há um padrão definido sobre como e quando efetuá-las, podendo gerar dúvidas quanto a sua execução. Além disso, foi detectado que as mídias de backup são armazenadas no mesmo local físico da operação do sistema, contrariando as boas práticas em segurança da informação[21].

Deficiências na segurança física da gerência do Infoseg

No que tange à segurança física, foi verificado que o acesso às dependências da gerência do Infoseg é feito por um sistema de identificação por biometria (impressão digital e senha) para os funcionários e por identificação por meio de interfone e câmera de vídeo para as demais pessoas. O sistema

funciona bem no controle de acesso dos funcionários da gerência do Infoseg, mas não é feito nenhum registro dos acessos de visitantes que possibilite identificação futura no caso de ocorrer um incidente de segurança. Além disso, não foi estabelecido um perímetro de segurança para as instalações do Infoseg[22]. Dessa forma, a porta de acesso está em contato direto com a rua e, na parte dos fundos, onde funciona um estacionamento, há uma porta de vidro que torna a segurança vulnerável.

Indefinição dos proprietários de alguns ativos

De acordo com as boas práticas de segurança da informação, é conveniente que todos os ativos de *software* e *hardware* sejam inventariados[23], tenham um proprietário identificado e a ele seja atribuída a responsabilidade pela proteção adequada desses ativos[24]. Esse inventário deve ser constantemente atualizado para refletir a situação exata dos ativos. No caso do Infoseg, não há inventário dos ativos do sistema.

Além disso, a gerência do Infoseg disponibilizou equipamentos para os estados implementarem as soluções de integração e, até a época da execução da auditoria, ainda não havia conseguido colher assinaturas nas cautelas de custódia dos referidos equipamentos. No caso de Pernambuco, a situação é ainda mais grave, pois lá se encontram os equipamentos de redundância das bases de dados e não há nenhum documento que formalize essa situação e estabeleça cláusulas de sigilo e responsabilização pelo uso indevido dos equipamentos ou divulgação não autorizada dos dados.

Estrutura insatisfatória de recursos humanos

A gerência do Infoseg não está formalmente definida na estrutura organizacional do Ministério da Justiça, definida pelo Decreto nº 5.535, de 13 de setembro de 2005. Isso gera dificuldades na alocação de pessoal, pois não há remunerações específicas (cargos comissionados) para assumir atividades de chefia que envolvam maior responsabilidade.

A gerência do Infoseg conta com uma equipe de 13 pessoas, sendo um servidor com contrato temporário atuando como gerente de projeto e doze terceirizados, contratados pelo Ministério da Justiça e alocados ao Infoseg. Esse número de funcionários é insuficiente para manter a produção e atender às demandas corretivas e evolutivas do sistema[25]. Na realidade faltam pessoas para desempenhar papéis importantes na equipe, como o de gerente de segurança da informação e o de responsável pela elaboração e estabelecimento de normas, políticas e metodologias.

Outro aspecto importante relativo à gestão e à segurança de TI é o exercício de funções sensíveis ou estratégicas por terceirizados. Com apenas um servidor do MJ (e com contrato temporário), é impossível que funções estratégicas de TI não sejam exercidas por prestadores de serviços. As conseqüências diretas dessa desproporção entre o número de servidores efetivos e de prestadores de serviço (92,31% da equipe são terceirizados) é o risco de descontinuidade da manutenção do sistema, devido a uma possível saída dos terceirizados, e a dependência em relação à empresa contratada, uma vez que a Senasp não detém o conhecimento tecnológico do sistema.

Funcionamento inadequado do serviço de atendimento ao usuário

Os usuários do Infoseg não possuem uma central de atendimento (*help desk*) que permita o esclarecimento de dúvidas, a resolução de problemas de funcionamento e a informação de incidentes de segurança[26]. A gerência do Infoseg possui dois atendentes que "funcionam" como *help desk*, atendendo nos dias úteis das 8h às 12h e das 14h às 18h. Porém, como o sistema de segurança pública funciona 24 horas por dia, atendendo, em âmbito nacional, aproximadamente quarenta e sete mil usuários de consulta, esse serviço não atende adequadamente às necessidades dos usuários.

Falhas nos contratos de locação de mão-de-obra

A Senasp não possui quadro próprio de servidores efetivos para desempenhar as atividades relacionadas à tecnologia da informação. Dessa forma, para suprir essa deficiência, foram alocados para a gerência do Infoseg, doze prestadores de serviço, sendo dez do contrato nº 02/2003 celebrado pelo Ministério da Justiça com a empresa Politec Informática Ltda.

Apesar de não ter sido celebrado com a Senasp, esse contrato está relacionado indiretamente ao Infoseg e por isso foi avaliado para verificar se contempla os requisitos de segurança da informação estabelecidos pela NBR ISO/IEC 17799[27]. Esses aspectos tornam-se ainda mais relevantes devido ao caráter sigiloso das informações criminais constantes do IN.

De acordo com a análise do contrato, dentre os aspectos verificados podem ser destacados a aderência parcial à Política de Segurança da Informação (PSI) e à Política de Controle de Acesso (PCA), a inexistência de processo claro e definido de gestão de mudanças, a inexistência de requisitos para a continuidade dos serviços, a inexistência de normas bem definidas visando à proteção de ativos, a inexistência de acordo de nível de serviço – SLA com metas mensuráveis de desempenho e aferição de satisfação, a inexistência de regras de desligamento do sistema e a inexistência de critérios de desempenho, monitoração e registro.

Inexistência de controles compensatórios para as operações dos administradores do sistema

Quanto à utilização do banco de dados, foram identificadas duas impropriedades:

- compartilhamento de senha com privilégios absolutos de acesso às bases de dados do Infoseg pelos dois administradores de banco de dados (DBA) da Senasp[28];

- inexistência de registro dos procedimentos realizados pelos DBA[29].

Em geral, não se pode evitar que um DBA realize as operações que desejar sobre as bases de dados. Devido ao acesso completo que o administrador de banco de dados tem que ter sobre os dados da base, o controle das suas operações é dos mais complexos de serem implementados. Entretanto, ainda que não se possa impedir que o DBA modifique os dados, controles compensatórios para possibilitar o rastreamento de suas operações devem ser providos.

Falha no gerenciamento de privilégios dos usuários

Em relação aos privilégios dos usuários, foi identificado que eles possuem mais privilégios que o necessário para suas operações[30,31]. O usuário responsável por fazer as consultas ao Índice Nacional necessita apenas de privilégio para executar consultas sobre a tabela do IN, porém possui outros sete privilégios. O usuário responsável por fazer as atualizações no IN necessita apenas dos privilégios de consulta, inserção e atualização dos dados da tabela, porém possui outros cinco privilégios. Além disso, segundo os gestores, a exclusão de registros é lógica, e não física, porém há usuários com privilégios para apagar, fisicamente, registros das tabelas.

Insuficiência de trilhas de auditoria

As trilhas de auditoria existentes no Infoseg contemplam apenas as consultas realizadas pelos usuários *Web* (quem consultou o quê, e quando). Não há registros sobre a data da atualização dos registros no Índice Nacional (IN), bem como não há informações sobre os dados alterados no IN, tampouco sobre as concessões e revogações das contas de usuários que realizam atualizações na base de dados.

Observe-se que houve preocupação, por parte da equipe do Infoseg, de permitir auditoria nas consultas, mas não nas alterações realizadas no sistema. Tal fato deve-se à intenção de disponibilizar a auditoria das consultas ao

Infoseg como ferramenta para corregedorias das polícias. Conclui-se, portanto, pela insuficiência das trilhas de auditoria existentes no sistema[32].

Ausência de otimização do tráfego na rede Infoseg

A Senasp implantou uma solução para interligar os sistemas estaduais e o Infoseg, baseada em uma interface bem definida por padrões abertos, sendo que para cada informação trocada entre estes sistemas também são encaminhadas informações de controle que identificam com marcas (*tags*) os dados transportados.

Como a quantidade de informação de controle, em bytes, é bem superior à quantidade de informação sobre o indivíduo, identifica-se a oportunidade de otimização do tráfego na rede, pois a comunicação entre os componentes do Infoseg que estão sob o domínio da Senasp não necessita utilizar as informações de controle do padrão aberto utilizado, já que este elo do sistema não é heterogêneo.

Ainda que atualmente não haja gargalos no processamento nem no tráfego de rede, com o aumento da demanda do sistema esses gargalos podem surgir, e a otimização proposta poderá retardar a necessidade de aumentar os links de comunicação, bem como a capacidade de processamento na Senasp.

Usabilidade do sistema insatisfatória

Visando conhecer a opinião dos usuários da rede Infoseg, foi elaborado um questionário eletrônico contendo dezessete perguntas sobre a satisfação dos usuários na utilização dos quatro módulos de consulta da Rede (indivíduos, armas, veículos e condutores). Os principais resultados podem ser vistos na tabela a seguir. Os resultados da pesquisa demonstram que, em geral, os usuários confiam nas informações da rede Infoseg e entendem bem seu significado. Porém, um percentual, em média um pouco acima de 20%, não encontra ou não acha fácil encontrar as informações que precisa,

mostrando que há espaço para a gerência do Infoseg melhorar a efetividade do sistema. Os efeitos potenciais são a desmotivação dos usuários para continuar consultando a rede Infoseg.

Tabulação dos principais resultados da pesquisa de satisfação

		Discordo totalmente	Discordo mais que concordo	Concordo mais que discordo	Concordo totalmente
Consigo a informação de que preciso	Indivíduos	3,5%	24,1%	54,4%	18,0%
		27,6%		72,4%	
	Veículos	3,7%	17,7%	43,5%	35,1%
		21,4%		78,6%	
	Condutores	3,1%	17,1%	44,5%	35,3%
		20,2%		79,8%	
	Armas	6,5%	22,6%	43,8%	27,1%
		29,1%		70,9%	
É fácil encontrar a informação de que preciso	Indivíduos	3,4%	23,3%	46,9%	26,4%
		26,7%		73,3%	
	Veículos	3,2%	16,5%	41,0%	39,3%
		19,7%		80,3%	
	Condutores	2,7%	16,2%	41,8%	39,2%
		18,9%		81,0%	
	Armas	5,9%	22,0%	41,4%	30,7%
		27,9%		72,1%	
Confio nas informações recebidas para tomar decisões	Indivíduos	4,4%	18,4%	37,3%	39,8%
		22,8%		77,1%	
	Veículos	3,3%	13,7%	35,5%	47,6%
		17,0%		83,1%	
	Condutores	2,3%	12,7%	35,6%	49,4%
		15,0%		85,0%	
	Armas	6,0%	17,5%	36,0%	40,5%
		23,5%		76,5%	

Inexistência ou inadequação da documentação da solução de integração

Entender o funcionamento das soluções de integração com a Senasp desenvolvidas pelos entes federados foi um dos objetivos das visitas feitas aos estados. No entanto, isso não foi possível de ser devido à inexistência ou inadequação da documentação apresentada. Além disso, em alguns lugares, as pessoas diretamente responsáveis pelo desenvolvimento ou manutenção não estavam presentes e os substitutos não sabiam quase nada sobre o sistema.

Devido à falta de documentação adequada, os gestores estaduais tiveram dificuldade em apontar as possíveis causas das inconsistências encontradas entre os dados constantes do Índice Nacional (IN) e das bases estaduais, pois não sabiam descrever todo o fluxo de dados das aplicações envolvidas nas operações de atualização do Infoseg. Também foi observado alto nível de terceirização de prestadores de serviço de informática nos estados, agravando a falta da documentação, devido à grande rotatividade dos contratados.

Desenvolvimento, manutenção e operação de sistema sem supervisão

O Anexo I ao Decreto nº 5.834, de 06.07.2006, que define a Estrutura Regimental do Ministério da Justiça, prescreve que:

> "Art. 4º À Secretaria-Executiva compete:
>
> ...
>
> II - supervisionar e coordenar as atividades de organização e modernização administrativa, bem como as relacionadas com os sistemas federais de planejamento e de orçamento, de contabilidade, de administração financeira, de administração dos recursos de informação e informática, de recursos humanos e de serviços gerais, no âmbito do Ministério; e
>
> ...
>
> Art. 5º À Subsecretaria de Planejamento, Orçamento e Administração compete:

> I - planejar, coordenar e supervisionar a execução das atividades relativas à organização e modernização administrativa, assim como as relacionadas com os sistemas federais de planejamento e de orçamento, de contabilidade e de administração financeira, de administração de recursos de informação e informática, de recursos humanos e de serviços gerais, no âmbito do Ministério;"

Apesar de não constar do Regimento Interno do Ministério da Justiça, o órgão executor das atividades de tecnologia da informação no Ministério é a Coordenação-Geral de Tecnologia da Informação (CGTI), subordinada à Subsecretaria de Planejamento, Orçamento e Administração. O Infoseg, sistema de extrema relevância para uma das atividades-fim do Ministério da Justiça, foi desenvolvido, é mantido e operado pela Senasp, portanto, fora da CGTI/MJ, com estrutura própria de equipamentos, contratos de prestação de serviço e pessoal (terceirizados). A auditoria não evidenciou qualquer supervisão ou coordenação das atividades de tecnologia da informação desenvolvidas pela Senasp no que diz respeito ao Infoseg.

A descentralização da execução das atividades ligadas à tecnologia da informação dentro de um órgão, por si só, não representa impropriedade, mas uma faculdade do administrador. Entretanto, a ausência de supervisão e coordenação dessas atividades executadas de forma descentralizada pode gerar problemas na alocação de recursos (humanos, financeiros e outros) e problemas nos controles relativos à segurança da informação, além de disputas políticas internas. Registre-se, por oportuno, que vários dos achados desta auditoria consistem na ausência ou deficiência de controles fora do sistema (políticas, metodologias, normas) que deveriam ser estabelecidos pelo principal órgão executor das atividades de tecnologia da informação do Ministério.

Em que pese o Infoseg estar implantado e com utilização crescente, conforme demonstrativos de números de usuários e de acessos, o fato de sua implantação, manutenção e operação ocorrerem sem supervisão ou coordenação sugere a existência de problemas na gestão das atividades de tecnologia da informação no Ministério.

Boas práticas identificadas

Dentre as boas práticas adotadas pela gerência do Infoseg, destaca-se a manutenção de soluções estaduais na integração da solução. A rede Infoseg é composta pela integração de um conjunto de bases de dados distribuídas pelos estados da Federação e por órgãos do governo federal. Porém, como cada unidade da federação trabalha com soluções tecnológicas diferentes, ficou a cargo dos estados desenvolverem módulos de integração com a base da Senasp. A solução de atualização para o Índice Nacional que os entes desenvolveram é função da plataforma que cada um deles utiliza nos seus sistemas criminais, não sendo necessário modificar suas bases originais nem adquirir novas tecnologias.

Para permitir a integração de tantas tecnologias diferentes com sua base de dados, a arquitetura adotada pela Senasp atende aos padrões de interoperabilidade do governo eletrônico federal (*E-ping*[33]) e visa à difusão do acesso aos dados por meio de outros dispositivos, tais como viaturas policiais, palmtops e celulares. A possibilidade de cada ente desenvolver sua solução de integração com a Senasp sem precisar modificar suas bases nem alterar sua plataforma tecnológica foi uma boa iniciativa da Senasp, sendo fator crítico de sucesso para a implantação do projeto.

Outra boa prática identificada foi a motivação dos gestores estaduais. Como a rede Infoseg não foi instituída por lei, que seria o único instrumento legal capaz de institucionalizá-la em órgãos de diferentes poderes e de diferentes esferas de governo, chega-se à conclusão que os entes envolvidos não têm obrigação legal de alimentar o sistema.

No entanto, a equipe de gestores do Infoseg efetua um excelente trabalho de conscientização dos entes federados sobre a importância de alimentarem o sistema, pois em todos os locais visitados a postura da gerência do Infoseg foi elogiada. O clima de cooperação e confiança observado foi apontado por todos como um dos principais fatores de sucesso da implantação da rede Infoseg.

O QUE PODE SER FEITO PARA MELHORAR O DESEMPENHO DO SISTEMA

Em relação à institucionalização do sistema Infoseg, o TCU recomendou que a Senasp apresente à Casa Civil da Presidência da República um anteprojeto de lei que institucionalize o Infoseg, de forma a permitir o estabelecimento de atribuições e responsabilidades para os entes participantes do sistema.

As determinações do TCU quanto aos problemas de consistência de informações encontradas entre o Índice Nacional e as bases de dados estaduais visam à adoção de providências necessárias para a correção das inconsistências. Além disso, o TCU determinou a instituição de mecanismos que garantam a consistência entre o IN e as bases de dados dos entes que alimentam o Índice Nacional, com verificação periódica da eficácia da solução implementada.

Quanto aos aspectos de segurança do Infoseg, as determinações do Tribunal visam à definição formal de uma Política de Segurança da Informação (PSI), com ampla divulgação do documento para todos os usuários, que orientará e apoiará a segurança da informação da rede. Da mesma forma, o TCU determinou que uma Política de Controle de Acesso (PCA) seja formalmente definida e contemple todos os tipos de usuários do Infoseg, estabelecendo a análise crítica dos direitos dos usuários do Infoseg.

O Tribunal determinou que a Senasp defina, formalmente, um Plano de Continuidade do Negócio (PCN) específico para o Infoseg que garanta, em caso de falhas ou desastre natural significativo, a retomada em tempo hábil das atividades do sistema. No mesmo sentido, determinou que seja formalizada política de geração de cópias de segurança para o Infoseg e que as mídias contendo essas cópias sejam armazenadas em local diverso da operação do sistema.

Em referência ao controle de mudanças do sistema Infoseg, o TCU determinou que sejam estabelecidos procedimentos formais de controle

de demandas e de mudanças no Infoseg, bem como sejam determinados critérios formais para homologação e aceitação de atualizações e novas versões do Infoseg. O Tribunal determinou ainda a definição formal de padrões para desenvolvimento de sistemas no âmbito do Infoseg.

Quanto à estrutura insatisfatória de recursos humanos encontrada na auditoria, o Tribunal determinou que sejam envidados esforços no sentido de dotar a gerência do Infoseg de recursos humanos especializados e treinados, necessários à garantia da continuação do desenvolvimento, manutenção e operação do sistema. Além disso, a Senasp deve avaliar a situação de terceirização de pessoal na gerência do Infoseg, de modo a dotar aquela gerência de servidores ocupantes de cargos efetivos suficientes, capacitados e treinados. Dessa forma, a dependência de recursos humanos externos ao Senasp será mitigada.

Em relação ao acesso à base de dados do Índice Nacional, o TCU determinou a implementação de controles compensatórios para as operações dos administradores de banco de dados do Infoseg, permitindo o registro e rastreamento das operações com privilégios realizadas na base de dados. Determinou ainda a utilização de identificadores de usuários únicos para o Infoseg, sem compartilhamento de senha, atribuindo-se a responsabilidade de cada usuário, inclusive para os usuários com privilégios de administração. O estabelecimento de procedimentos formais para a execução de operações diretamente sobre as bases de dados do Infoseg, bem como a atribuição a cada usuário do banco de dados do Infoseg somente dos privilégios mínimos necessários ao desempenho de suas funções, são outras medidas determinadas pelo Tribunal para que haja rígido controle do acesso ao banco de dados.

Para que os usuários do sistema Infoseg possam ter dúvidas esclarecidas e problemas de funcionamento resolvidos de forma ágil, o TCU recomendou que seja implementado um serviço de atendimento ao usuário do Infoseg (*help desk*) adequado às suas necessidades, avaliando-se a conveniência de implantá-lo em regime ininterrupto (24 horas por dia e 7 dias por semana).

Por fim, o TCU recomendou que Senasp analise as sugestões enviadas pelos usuários no questionário eletrônico e estude quais alterações são necessárias para melhorar os pontos fracos apontados.

BENEFÍCIOS DA IMPLEMENTAÇÃO DAS RECOMENDAÇÕES E DETERMINAÇÕES DO TCU PARA O SISTEMA INFOSEG

O Tribunal de Contas da União pôde contribuir para o aperfeiçoamento do sistema Infoseg com um conjunto de recomendações a serem adotadas pela Secretaria Nacional de Segurança Pública do Ministério da Justiça (Senasp/MJ), tornando o ambiente do sistema Infoseg mais confiável, estável e seguro. A implementação das recomendações e determinações é de grande relevância para que o Infoseg tenha sua importância estratégica ampliada no cenário da segurança pública, tornando-se uma ferramenta útil e ágil para os entes participantes.

ACÓRDÃO Nº 71/2007 – TCU – PLENÁRIO

1. Processo nº TC-003.293/2006-3

2. Grupo I, Classe de Assunto: V – Relatório de Auditoria

3. Entidade: Secretaria Nacional de Segurança Pública - Senasp/MJ

4. Responsável: Luiz Fernando Corrêa, CPF: não informado

5. Relator: Ministro-Substituto Augusto Sherman Cavalcanti

6. Representante do Ministério Público: não atuou

7. Unidade Técnica: Secretaria Adjunta de Fiscalização – Adfis

8. Advogado constituído nos autos: não há

9. Acórdão:

VISTOS, relatados e discutidos estes autos de Relatório de Auditoria realizada na Secretaria Nacional de Segurança Pública do Ministério da Justiça – Senasp/MJ com o objetivo de avaliar aspectos relacionados com a segurança e a consistência das informações gerenciadas pelo sistema Infoseg (Sistema Nacional de Integração de Informações em Justiça e Segurança Pública), em cumprimento ao disposto no item 9.4 do Acórdão 724/2005-TCU-Plenário,

ACORDAM os Ministros do Tribunal de Contas da União, reunidos em sessão do Plenário, diante das razões expostas pelo Relator, em:

9.1. recomendar, com fulcro no art. 43, inciso I, da Lei 8.443/92 c/c o art. 250, inciso III, do Regimento Interno do TCU, à Secretaria Nacional de Segurança Pública do Ministério da Justiça - Senasp/MJ que:

9.1.1. em atenção ao Princípio da Legalidade, constante do art. 37, caput, da Constituição Federal, estude a viabilidade de apresentar à Casa Civil da Presidência da República anteprojeto de lei que regulamente o § 7º, do art. 144, da Constituição Federal, de forma a institucionalizar o sistema Infoseg, contendo, entre outros, dispositivos que contemplem atribuições e responsabilidades para os entes que detêm as informações de interesse do sistema;

9.1.2. estude, em atenção ao Princípio da Eficiência contido no caput, do art. 37, da Constituição Federal, a viabilidade de virem a integrar diretamente à rede Infoseg todos os órgãos que possam fornecer informações ao Índice Nacional, em especial os Tribunais de Justiça das unidades da federação, órgãos responsáveis pelas informações sobre mandados de prisão e andamento de processos;

9.1.3. implemente serviço de atendimento ao usuário do Infoseg (*help desk*) adequado às suas necessidades, em conformidade com o previsto no item 13.1.1 da NBR ISO/IEC 17799:2005 e à semelhança das orientações contidas no DS8.1 do COBIT 4.0, avaliando a conveniência de implantá-lo em regime ininterrupto (24 horas por dia e 7 dias por semana);

9.1.4. estude a viabilidade de trafegar os dados pela rede Infoseg em formato mais compacto que o formato XML usado atualmente, como por exemplo no formato TXT, em atendimento ao Princípio da Eficiência constante do art. 37, caput, da Constituição Federal;

9.1.5. em atenção ao Princípio da Eficiência contido no caput, do art. 37, da Constituição Federal, avalie os resultados da pesquisa realizada com os usuários do Infoseg no curso deste trabalho (CD-ROM em anexo), visando a implementar melhorias no sistema que minimizem os pontos frágeis apontados, em especial quanto à facilidade de busca das informações;

9.2. determinar, com fulcro no art. 43, inciso I, da Lei 8.443/92 c/c o art. 250, inciso II, do Regimento Interno do TCU, à Secretaria Nacional de Segurança Pública do Ministério da Justiça - Senasp/MJ que:

9.2.1. em atenção ao princípio da legalidade constante do art. 37, caput, da Constituição Federal, crie dispositivos que melhor regulamentem o Infoseg, estabelecendo atribuições e responsabilidades para os entes participantes do sistema, ainda que por meio do aperfeiçoamento dos termos de convênio firmados no âmbito do Fundo Único de Segurança Pública - FUSP;

9.2.2. adote as providências necessárias para resolver as inconsistências entre as bases de dados estaduais e o Índice Nacional, constantes dos arquivos do CD-ROM em anexo;

9.2.3. institua mecanismos que garantam a consistência entre o Índice Nacional - IN - e as bases dos entes que alimentam o IN, verificando periodicamente a eficácia dos mecanismos implementados, de acordo com o previsto no item 12.2.2, da NBR ISO/IEC 17799:2005;

9.2.4. defina formalmente junto a todos os entes que alimentam o Infoseg o significado preciso de todas as informações e termos que compõe o IN, à semelhança das orientações contidas no item PO2.2 do COBIT 4.0, de modo a evitar ambigüidades de entendimento acerca deles;

9.2.5. estabeleça e identifique formalmente responsabilidades relativas às questões de segurança das informações do Infoseg, de acordo com o previsto no item 6.1.3 da NBR ISO/IEC 17799:2005;

9.2.6. defina formalmente uma Política de Segurança da Informação – PSI – para o Infoseg, que forneça orientação e apoio para a segurança da informação da rede, promovendo-se ampla divulgação do documento para todos os usuários, de acordo com o previsto no item 5.1.1 da NBR ISO/IEC 17799:2005;

9.2.7. defina formalmente uma Política de Controle de Acesso – PCA – para o Infoseg, contemplando usuários *Web*, "*host* de atualização" e da rede interna da gerência do Infoseg, de acordo com o previsto no item 11.1.1 da NBR ISO/IEC 17799:2005;

9.2.8. conduza, a intervalos regulares, a análise crítica dos direitos de acesso dos usuários do Infoseg, por meio de um processo formal, de acordo com o previsto no item 11.2.4 da NBR ISO/IEC 17799:2005;

9.2.9. defina formalmente padrões para desenvolvimento de sistemas no âmbito do Infoseg, à semelhança das orientações contidas no item PO8.3 do COBIT 4.0;

9.2.10. crie mecanismos para que as políticas e normas se tornem conhecidas, acessíveis e observadas por todos os usuários e gestores do Infoseg, de acordo com o previsto no item 5.1.1 da NBR ISO/IEC 17799:2005;

9.2.11. implemente os procedimentos informatizados, ou não, necessários no sentido de ajudar a garantir a observância dos itens 9.2.6 a 9.2.9 acima;

9.2.12.estabeleça procedimentos formais de controle de demandas e de mudanças no Infoseg, de acordo com o previsto no item 12.5.1 da NBR ISO/IEC 17799:2005 e à semelhança das orientações contidas no item AI6.2 do COBIT 4.0;

9.2.13. estabeleça critérios formais para homologação e aceitação de atualizações e novas versões do Infoseg, de acordo com o previsto no item 10.3.2 da NBR ISO/IEC 17799:2005;

9.2.14. defina formalmente um Plano de Continuidade do Negócio – PCN – específico para o Infoseg, que garanta em caso de falhas ou desastre natural significativo, a retomada em tempo hábil das atividades do sistema, protegendo os processos críticos, de acordo com o previsto nos itens 14.1.4 e 14.1.5 da NBR ISO/IEC 17799:2005;

9.2.15. formalize política de geração de cópias de segurança para o Infoseg, de acordo com o previsto no item 10.5.1 da NBR ISO/IEC 17799:2005;

9.2.16. armazene as mídias contendo cópias de segurança do Infoseg em local diverso da operação do sistema, de acordo com a diretriz "d" do item 10.5.1 da NBR ISO/IEC 17799:2005;

9.2.17. estabeleça um perímetro de segurança nas instalações da gerência do Infoseg (barreiras tais como paredes, portões de entrada controlados por cartão ou balcão com recepcionista), em conformidade com o item 9.1.1 da NBR ISO/IEC 17799:2005;

9.2.18. realize as obras necessárias de forma que se constituam barreiras físicas suficientes nas instalações da gerência do Infoseg que impeçam o acesso de pessoas não autorizadas, em conformidade com a diretriz "b" do item 9.1.1 da NBR ISO/IEC 17799:2005;

9.2.19. formalize o inventário dos ativos do Infoseg, em conformidade com o previsto no item 7.1.1 da NBR ISO/IEC 17799:2005;

9.2.20 defina formalmente o proprietário de cada ativo constante do inventário acima, em conformidade com o item 7.1.2 da NBR ISO/IEC 17799:2005, atentando para a assinatura das cautelas que se fizerem necessárias;

9.2.21. formalize, junto à Agência Estadual de Tecnologia da Informação do Estado de Pernambuco – ATI –, um termo de compromisso que contemple de maneira específica a cópia das bases de dados do Infoseg que se encontra naquelas instalações, estabelecendo nele cláusulas de sigilo e responsabilização pelo uso indevido dos equipamentos ou divulgação não autorizada dos dados;

9.2.22. envide esforços no sentido de dotar a gerência do Infoseg dos recursos humanos especializados e treinados, necessários à garantia da continuação do desenvolvimento, manutenção e operação do sistema, à semelhança das orientações contidas no item PO 4.12 do COBIT 4.0;

9.2.23. avalie a situação de terceirização de pessoal na gerência do Infoseg, de modo a dotar aquela gerência de servidores ocupantes de cargos efetivos suficientes, capacitados e treinados para exercer as atividades estratégicas e sensíveis, sobretudo as de gestão do sistema (planejamento, coordenação, organização, supervisão e controle);

9.2.24. implemente controles compensatórios (autorização formal, registro e monitoramento das alterações) para as operações dos administradores de banco de dados do Infoseg de forma a permitir o registro e rastreamento das operações realizadas na base de dados com privilégios, em conformidade com o previsto no item 10.10.4 da NBR ISO/IEC 17799:2005;

9.2.25. utilize identificadores de usuários únicos para o Infoseg (senha única não compartilhada) de forma fixar a responsabilidade de cada usuário, inclusive para os usuários com privilégios de administração, em conformidade com o previsto no item 11.2.1 da NBR ISO/IEC 17799:2005;

9.2.26. estabeleça procedimentos formais para a execução de operações diretamente sobre as bases de dados do Infoseg com a utilização de utilitários, documentando os procedimentos realizados, em conformidade com o previsto no item 11.5.4 da NBR ISO/IEC 17799:2005;

9.2.27. atribua a cada usuário do banco de dados do Infoseg somente os privilégios mínimos necessários ao desempenho de suas funções, conforme previsto no item 11.2.2 da NBR ISO/IEC 17799:2005;

9.2.28. implemente trilhas de auditoria para as atualizações no Índice Nacional do Infoseg, em conformidade com o previsto no item 10.10.1 da NBR ISO/IEC 17799:2005, contendo, no mínimo, a data-hora da alteração, o dado alterado e a identificação do responsável pela alteração;

9.2.29. implemente trilhas de auditoria para as concessões e revogações das contas de HOST do Infoseg, em conformidade com o previsto no item 10.10.1 da NBR ISO/IEC 17799:2005;

9.3. recomendar, com fulcro no art. 43, inciso I, da Lei 8.443/92 c/c o art. 250, inciso III, do Regimento Interno do TCU, ao Ministério da Justiça que defina formalmente a estrutura organizacional da gerência do Infoseg, definindo suas competências e responsabilidades, à semelhança das orientações contidas nos itens PO4.5 e PO4.6 do COBIT 4.0;

9.4. determinar, com fulcro no art. 43, inciso I, da Lei 8.443/92 c/c o art. 250, inciso II, do Regimento Interno do TCU, à Coordenação-Geral de Logística do Ministério da Justiça - CGL/MJ que nos contratos de serviços relativos à área de TI, defina claramente, tanto nos editais de licitação como nos contratos, cláusulas contemplando requisitos de segurança da informação como os previstos no item 6.2.3 da NBR ISO/IEC 17799:2005;

9.5. encaminhar cópia da presente deliberação, bem como do relatório e voto que o fundamentam: à Subcomissão Permanente de Segurança Pública, da Comissão de Constituição, Justiça e Cidadania do Senado Federal - CCJSSP; à Comissão de Segurança Pública e Combate ao Crime Organizado da Câmara dos Deputados – CSPCCO; à Casa Civil da Presidência da República; e ao Gabinete de Segurança Institucional – GSI – da Presidência da República;

9.6. determinar à Adfis que, no prazo de 180 dias, promova monitoramento, de modo a verificar o cumprimento das recomendações e determinações constantes deste acórdão.

10. Ata nº4/2007 – Plenário

11. Data da Sessão 31/01/2007 – Ordinária

12. Código eletrônico para localização na página do TCU na internet: AC-0071-04/07-P

13. Especificação do quórum:

13.1. Ministros presentes: Walton Alencar Rodrigues (Presidente), Marcos Vinicios Vilaça, Ubiratan Aguiar, Benjamin Zymler, Augusto Nardes e Aroldo Cedraz.

13.2. Auditores convocados: Augusto Sherman Cavalcanti (Relator) e Marcos Bemquerer Costa.

Walton Alencar Rodrigues
Presidente

Augusto Sherman Cavalcanti
Relator

NOTAS

[1] NBR ISO/IEC 17799:2001 - Código de Prática para a Gestão da Segurança da Informação

[2] Processo TC 011.659/2004-1

[3] COBIT 4.0 - "Um objetivo de controle é uma declaração de um propósito ou resultado a ser alcançado, por meio da implementação de controles em determinada atividade de TI." (tradução livre).

[4] NBR 17799:2005, item 12.2.2: Controle do processamento interno - "Convém que sejam incorporadas, nas aplicações, checagens de validação com o objetivo de detectar qualquer corrupção de informações, por erros ou por ações deliberadas".

[5] NBR 17799:2005, item 12.2.2, diretriz "d": "verificações de integridade, autenticidade ou qualquer outra característica de segurança, dados ou *softwares* transferidos ou atualizados entre computadores centrais e remotos".

[6] http://www.clippingexpress.com.br/noticias_justiça.php?id=16762, acessado em 17.05.2006

[7] http://clipping.planejamento.gov.br/Noticias.asp?NOTCod=99206, acessado em 17.05.2006

[8] Dicionário de dados - Repositório organizado de informações acerca da sintaxe e semântica dos dados dispostos em banco de dados.

[9] COBIT 4.0, item PO2.2: Dicionário de dados corporativos e regras de sintaxe dos dados - **"Mantenha um dicionário de dados corporativo que contenha as regras sintáticas para os dados da organização. Este dicionário possibilita o compartilhamento dos elementos de dados entre aplicações e sistemas, promovendo um entendimento comum dos dados entre o setor de TI e os usuários, e previne a criação de elementos de dados incompatíveis."** (tradução livre) (grifamos).

[10] Descrição apresentada pela Senasp.

[11] NBR 17799:2005, item 5.1 - Política de Segurança da Informação: "Objetivo: Prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos de negócio e com as leis e regulamentações relevantes. Convém que a direção estabeleça uma política clara, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização".

[12] NBR 17799:2005, item 11.1.1 - Política de Controle de Acesso: "Convém que as regras de controle de acesso e direitos para cada usuário ou grupo de usuários sejam expressas claramente na política de controle de acesso".

[13] NBR 17799:2005, item 5.1.1 - Documento da política de segurança da informação: "Convém que um documento da política de segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes".

[14] NBR17799:2005, item 11.2.4 - Análise crítica dos direitos de acesso de usuário: "Convém que o gestor conduza a intervalos regulares a análise crítica dos direitos de acesso dos usuários, por meio de um processo formal."

[15] NBR 17799:2005, item 6.1.3 - Atribuição de responsabilidades para a segurança da informação: "Convém que todas as responsabilidades pela segurança da informação sejam claramente definidas".

[16] NBR 17799:2005, item 12.5.1 (Procedimentos para controle de mudanças) – "Convém que a implementação de mudanças seja controlada utilizando procedimentos formais de controle de mudanças".

[17] NBR 17799:2005, item 10.3.2 (Aceitação de Sistemas) – "Convém que sejam estabelecidos critérios de aceitação para novos sistemas, atualizações e novas versões, e que sejam efetuados testes apropriados do(s) sistema(s) durante seu desenvolvimento e antes da sua aceitação".

[18] NBR 17799:2005, item 14.1.4 (Estrutura do plano de continuidade do negócio) – "Convém que uma estrutura básica dos planos de continuidade do negócio seja mantida para assegurar que todos os planos são consistentes, para contemplar os requisitos de segurança da informação e para identificar prioridades para testes e manutenção".

[19] NBR 17799:2005, item 14.1.5: Testes, manutenção e reavaliação dos planos de continuidade do negócio – "Convém que os planos de continuidade do negócio sejam testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade".

[20] NBR 17799:2005, item 10.5.1: Cópias de segurança das informações – "Convém que as cópias de segurança das informações e dos *softwares* sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida".

[21] NBR ISO/IEC 17799:2005, item 10.5.1, diretriz "d" – "as cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no local principal".

[22] NBR 17799:2005, Item 9.1.1: Perímetro de segurança física – "Convém que sejam utilizados perímetros de segurança (barreiras tais como paredes, portões de entrada controlados por cartão ou balcões de recepção com recepcionistas) para proteger as áreas que contenham informações e instalações de processamento da informação".

[23] NBR 17799:2005, item 7.1.1: Inventário dos ativos – "Convém que todos os ativos sejam claramente identificados e um inventário de todos os ativos importantes seja estruturado e mantido".

[24] NBR ISO/IEC 17799:2005, item 7.1.2: Proprietário dos ativos – "Convém que todas as informações e ativos associados com os recursos de processamento da informação tenham um proprietário designado por uma parte definida da organização".

[25] COBIT 4.0, item PO4.12: "Assessoria de IT - Avalie as necessidades de pessoal periodicamente para garantir que as funções de TI tenham pessoal com qualificação e em quantidade suficientes" (tradução livre).

[26] COBIT 4.0, item DS 8.1: Atendimento ao usuário - "Estabeleça uma função de atendimento ao usuário, que funcione como interface dos usuários com a TI, para registrar, comunicar, encaminhar e analisar todas as chamadas, relatar incidentes, requisitar serviços e informações." (tradução livre).

[27] NBR ISO/IEC 17799:2005, item 6.2.3: Identificando segurança da informação nos acordos com terceiros – "Convém que os acordos com terceiros envolvendo o acesso, processamento, comunicação ou gerenciamento dos recursos de processamento da informação ou da informação da organização, ou o acréscimo de produtos ou serviços aos recursos de processamento da informação cubram todos os requisitos de segurança da informação relevantes".

[28] NBR 17799:2005, item 11.2.1: Registro de usuário (diretriz a) - "a) utilizar identificadores de usuário (ID de usuário) único para assegurar a responsabilidade de cada usuário por suas ações ..."

[29] NBR 17799:2005, item 10.10.4: Registros (log) de administrador e operador - "Convém que os recursos e informações de registros (log) sejam protegidos contra falsificação e acesso não autorizado".

[30] NBR 17799:2005, item 11.2.2: Gerenciamento de privilégios - "Convém que a concessão e uso de privilégios sejam restritos e controlados".

[31] NBR 17799:2005, item 11.2.2, diretriz b - "os privilégios sejam concedidos a usuários conforme a necessidade de uso e com base em eventos alinhados com a política de controle de acesso (ver 11.1.1), por exemplo, requisitos mínimos para sua função somente quando necessários;"

[32] NBR 17799:2005, item 10.10.1: Registros de auditoria - "Convém que registros (log) de auditoria contendo atividades dos usuários, exceções e outros eventos de segurança da informação sejam produzidos e mantidos por um período de tempo acordado para auxiliar em futuras investigações e monitoramento do controle de acesso".

[33] www.eping.e.gov.br

TRIBUNAL DE CONTAS DA UNIÃO
SAFS Quadra 4 lote 1
70042-900 Brasília-DF
<http://www.tcu.gov.br>

Responsabilidade Editorial

Secretário-Geral de Controle Externo
Jorge Pereira de Macedo

Secretário de Fiscalização de Tecnologia da Informação
Cláudio Souza Castello Branco

Equipe de Auditoria
Carlos Renato Araujo Braga (coordenador)
Harley Alves Ferreira
Roberta Ribeiro de Queiroz Martins (supervisora)

Capa e Editoração

Secretaria-Geral da Presidência
Instituto Serzedello Corrêa
Centro de Documentação
Editora do TCU

Revisão de Texto
Nancy Alves Martinez

Impresso pela Sesap/Segedam

TRIBUNAL DE CONTAS DA UNIÃO

Endereço para contato, solicitação de exemplares e consulta na Internet

TRIBUNAL DE CONTAS DA UNIÃO
Secretaria de Fiscalização de
Tecnologia da Informação (Sefti)
SAFS, Quadra 4, Lote 1
Anexo II, Sala 311
70042-900 – Brasília-DF
Fone: (61) 3316.5371/7396
Fax: (61) 3316.5372
http://www.tcu.gov.br/fiscalizacaoti
sefti@tcu.gov.br

Secretaria de Fiscalização de Tecnologia da Informação

Negócio

Controle externo da governança de tecnologia da informação na Administração Pública Federal.

Missão

Assegurar que a tecnologia da informação agregue valor ao negócio da Administração Pública Federal em benefício da sociedade.

Visão

Ser unidade de excelência no controle e no aperfeiçoamento da governança de tecnologia da informação.