Avaliação do Sistema Nacional de Integração de Informações de Justiça e Segurança Pública – Infoseg

Carlos Renato Araujo Braga,
Harley Alves Ferreira

1. DESCRIÇÃO DO SISTEMA INFOSEG

Com base no princípio federativo da Constituição Federal do Brasil, os estados possuem autonomia na área de segurança pública, gerenciando suas próprias polícias e administrando as informações pertinentes a essa área. Essa autonomia traz como resultado a existência de diferentes sistemas de informações criminais para cada estado da Federação, para a Polícia Federal, Justiças Estaduais, Justiça Federal, etc.

Por força de dispositivos legais, coube à Secretaria Nacional de Segurança Pública do Ministério da Justiça – Senasp/MJ – o desenvolvimento e 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**), sobre armas de fogo (módulo **Armas**), sobre veículos (módulo **Veículos**) e sobre condutores (módulo **Condutores**). O sistema disponibiliza essas informações para os agentes públicos federais, estaduais, distritais e municipais cadastrados no sistema via 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, pode-se 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.

Carlos Renato Araujo Braga é servidor do Tribunal de Contas da União, graduado em Engenharia de Computação pelo Instituto Militar de Engenharia, Especialista em Contabilidade e Orçamento Público pela Universidade de Brasília e *Certified Information Systems Auditor* (CISA) pela *Information Systems Audit and Control Association* (ISACA).

Harley Alves Ferreira é servidor do Tribunal de Contas da União, graduado em Ciências da Computação pela Universidade Federal da Bahia e formado em Perícia Criminal em Informática pela Academia Nacional de Polícia.

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) , respectivamente.

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. O sistema está implementado em plataforma aberta, baseada em tecnologia *WEB Services* e utiliza protocolos padrões como HTTP, XML e LDAP. Sua arquitetura, aderente aos Padrões de Interoperabilidade do Governo Eletrônico – E-ping – seguiu os padrões do *Web Service Interoperability Organization* (WS-I), garantindo assim a sua independência de plataforma e facilidade de integração com outras tecnologias.

À época da auditoria (1º semestre de 2006), 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*. Dessa forma, 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.

2. OBJETIVOS E ESCOPO DA AUDITORIA

O objetivo da auditoria, realizada entre março e maio de 2006, foi avaliar aspectos relacionados com a segurança e a consistência das informações gerenciadas pelo Infoseg. 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 nos diversos estados, é o módulo mais complexo, cuja base (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 nos estados e o IN possuam exatamente a mesma informação num determinado instante. Dessa forma, a auditoria foi focada no módulo Indivíduos, mais especificamente nas atualizações e consultas ao Índice Nacional, visto que, à época, existiam diversos estados que não disponibilizavam as consultas detalhadas aos indivíduos.

Durante a fase de planejamento foram formuladas as seguintes questões de auditoria:

Q.1.As informações do Índice Nacional – IN – refletem as informações das bases de dados dos agentes de segurança pública?

Q.2.As Políticas de Segurança da Informação estabelecidas para o Infoseg contribuem para uma boa gestão de segurança da informação na rede Infoseg?

Q.3.O perímetro de segurança e os controles de acesso físico garantem a segurança das instalações da Senasp?

Q.4.A gerência do Infoseg possui gestão de controle de acesso para a rede Infoseg que dificulte o uso indevido das informações ?

Q.5.A estrutura de Recursos Humanos da área de TI é satisfatória para atendimento das necessidades do Infoseg?

Q.6.Os contratos de prestação de serviços contemplam requisitos de segurança?

Q.7.Os contratos de locação de mão-de-obra contemplam requisitos de segurança?

Q.8.A Senasp detém o conhecimento e controle técnico do Infoseg?

Q.9.Há um Plano de Continuidade do Negócio (PCN) compatível com as necessidades operacionais do Infoseg?

Q.10.A usabilidade do sistema é satisfatória?

3. METODOLOGIA ADOTADA

Durante o planejamento, a equipe manteve diversas reuniões com os gestores do sistema nas instalações da Senasp onde o núcleo do sistema funciona. Conforme se anotará adiante, a estrutura de pessoal que suporta o Infoseg não existe formalmente na Senasp, motivo pelo qual utilizaremos a expressão **Gerência do Infoseg** para referenciá-la.

Na fase de execução, foram visitados os estados do Ceará, de Pernambuco, do Rio Grande do Sul e do Pará, o Distrito Federal e o Departamento de Polícia Federal, entes que atualizam o IN. 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 uma extração das informações constantes de suas bases criminais para verificar a consistência em relação as constantes do IN, ponto que a equipe definiu como de maior relevância para este trabalho, visto que significava avaliar se o sistema atinge seus objetivos ou não. Para efetuar o cruzamento de dados pretendido, preliminarmente, a equipe solicitou a extração da base do IN, o que foi realizado em 02.03.2006.

Durante as visitas supracitadas, como as Secretarias de Segurança Pública Estaduais visitadas não são jurisdicionadas ao TCU, a equipe solicitou, por meio de Ofícios de Requisição à Senasp, com cópia para os gestores estaduais, 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, a equipe realizou ajustes, com apoio dos técnicos estaduais, de forma a obter os dados que estavam na base criminal em 2.3.2006, data da extração do IN. Após o ajuste supra, a equipe realizou o cruzamento dos dados, com apoio do software ACL, apurando as inconsistências relatadas adiante.

Ainda durante as visitas, a equipe validou, juntamente com os técnicos estaduais, a existência das inconsistências, por meio de consultas ao Infoseg e aos sistemas criminais estaduais, entregando-lhes os arquivos que evidenciaram as inconsistências detectadas.

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, a equipe buscou 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.

Visando conhecer a opinião dos usuários da rede Infoseg, a equipe elaborou um questionário eletrônico contendo dezessete perguntas sobre sua satisfação na utilização dos quatro módulos de consulta da Rede. O questionário pôde ser respondido entre os dias 10.4.2006 e 3.5.2006 e obteve o resultado bruto de 4.238 respostas.Após a exclusão de algumas respostas repetidas chegou-se ao número final de 3.717 respostas válidas que 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, utilizaram-se como critérios de auditoria os controles previstos na norma NBR ISO/IEC 17799:2005 e no COBIT – ***C**ontrol **OB**jectives for **I**nformation and related **T**echnology* (versões 3.0 e 4.0).

4. PRINCIPAIS ACHADOS

4.1 INSUFICIÊNCIA DE LEGISLAÇÃO APLICÁVEL

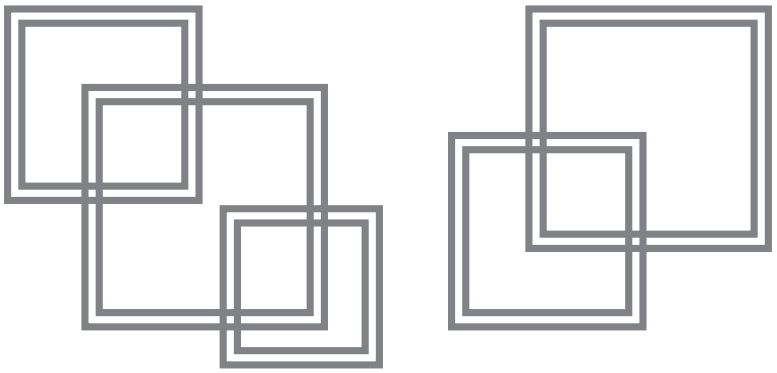
O Índice Nacional, núcleo do Infoseg, é composto por informações oriundas de diversos órgãos de segurança pública, citados no art. 144 da Constituição Federal (polícia federal, polícia rodoviária federal, polícias civis e militares estaduais e distritais), bem como de órgãos do Poder Judiciário (STJ,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

Durante a auditoria ficou 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. A equipe de auditoria constatou 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.

As informações constantes do Índice Nacional são provenientes de órgãos de diferentes Poderes (Executivo e Judiciário) e de diferentes esferas de governo (federal, estadual, distrital). 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 hoje.

A título de exemplo, registre-se que nos sistemas Renach e Renavam os entes participantes são de diversas esferas de governo e que são institucionalizados por lei federal, no caso, o Código Brasileiro de Trânsito (CBT) - Lei nº 9.503/1997. Observa-se que o Sistema Nacional de Trânsito, sendo instituído por lei (CBT), pôde estabelecer atribuições e responsabilidades (inclusive quanto à regulamentação) aos entes participantes do sistema sem prejudicar o princípio federativo, o que não ocorre com o Sistema Único de Segurança Pública (SUSP), sistema onde o Infoseg se insere.

Considerando a falta de legislação, entendemos que devem ser comunicadas as Casas Legislativas Federais, por intermédio das suas comissões temáticas, e a Casa Civil da Presidência da República, a cerca da necessidade institucionalizar o Infoseg por meio de lei federal com conteúdo nacional prevista no §7º do art. 144 da Constituição Federal.



Considera-se ainda que, ante a lacuna deixada pela ausência de lei institucionalizando o Infoseg, a Senasp deve criar dispositivos que regulamentem o Infoseg por meio do aperfeiçoamento dos termos de convênio firmados no âmbito do Fundo Único de Segurança Pública (FUSP), ainda que esta seja uma forma precária.

4.2 INCONSISTÊNCIAS ENTRE AS BASES DE DADOS CRIMINAIS E O ÍNDICE NACIONAL

Durante os trabalhos de campo, a equipe de auditoria realizou visita a seis dos vinte e nove entes que atualizam informações no Índice Nacional. Em todos eles, a equipe de auditoria constatou inconsistências entre as informações constantes em suas bases e a base do IN. Considerando a existência de inconsistência nas informações sobre mandados de prisão em aberto, as notificações supra foram encaminhadas tanto ao Secretário Nacional de Segurança Pública quanto ao interlocutor do ente visitado (normalmente o coordenador-administrativo do Infoseg) de forma a permitir maior agilidade nas eventuais correções. Registre-se que todos os entes visitados já realizaram, pelo menos uma vez, a operação de recarga da base, onde 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 (item 12.2.2, da NBR ISO/IEC 17799:2005) e podemos dividi-las 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.

As informações do IN sobre mandados de prisão e processos, originadas nos Tribunais de Justiça dos estados, chega à Senasp encaminhada pelo órgão 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. Em atenção ao princípio da eficiência, as informações originadas nos tribunais de justiça das unidades da federação deveriam ser enviadas em meio magnético diretamente ao Infoseg.

Por fim, registre-se que até o fim dos trabalhos desta equipe, nenhum tipo de auditoria na consistência dos dados do Índice Nacional havia sido empreendida, em desconformidade com o preconizado na diretriz d, do item 12.2.2, da NBR ISO/IEC 17799:2005.

As possíveis causas para este achado são falhas nas soluções de integração dos entes que alimentam o sistema e o fato de que os dados que se originam nos Tribunais de Justiça dos estados não são enviados eletrônica e diretamente para o Infoseg. Os efeitos reais e potenciais da desconformidade anotada são a utilização de informação incorreta na tomada de decisão pelos agentes de segurança pública, como por exemplo, um cidadão inocente ser preso indevidamente ou um criminoso ser parado pela polícia e deixar de ser preso.

Conclui-se que devem ser implementados mecanismos que garantam a consistência das informações entre as bases de dados criminais dos entes participantes do Infoseg e a base do Índice Nacional, e as soluções adotadas devem ser auditadas periodicamente.

Há ainda necessidade de integrar diretamente os Tribunais de Justiça das Unidades da Federação à rede Infoseg para que as informações que lá se originam (processos e mandados de prisão) sejam encaminhadas diretamente ao Infoseg por meio eletrônico.

Para avaliar a gravidade das inconsistências anotadas, registre-se que, em pesquisa realizada por meio de questionário eletrônico, acessado a partir da página do Infoseg, buscou-se conhecer o quanto os usuários confiam nas informações constantes do Índice Nacional, perguntando o quanto eles concordam com a seguinte afirmação: Confio nas informações recebidas para tomar decisões. O resultado da pesquisa registrou que 77,1% dos usuários tomariam decisões com base em informações da base indivíduos.

Outro ponto a considerar em nossa análise é a sensibilidade das informações constantes do Índice Nacional, como a existência ou não de mandados de prisão em aberto, que podem levar o agente de segurança pública a decidir prender ou não um indivíduo consultado no Infoseg.

Considerando as inconsistências entre as bases de dados dos entes que alimentam o Infoseg e o Índice Nacional evidenciadas nos trabalhos de campo que, segundo a pesquisa realizada durante a auditoria, um percentual expressivo dos agentes de segurança pública que utilizam o Infoseg tomam decisões com base na informação constante do Índice Nacional, e a sensibilidade das informações constantes do Índice Nacional que podem levar, por exemplo, a prisão ou não de um indivíduo considera-se que esta impropriedade é gravíssima, necessitando de providências urgentes a fim de evitar as situações descritas como efeitos reais e potenciais anotadas neste subitem.

4.3 INEXISTÊNCIA DE POLÍTICAS FORMALMENTE DEFINIDAS

Com relação às políticas de Segurança da Informação que deveriam estar estabelecidas para o Infoseg, evidenciou-se o descrito a seguir.

a) Ainda que haja uma PSI formalmente definida para o Ministério da Justiça (MJ), como nem todos os usuários do Infoseg estão na estrutura do MJ, a PSI do MJ não é instrumento hábil para o Infoseg, de forma que há desconformidade com a recomendação do item 5.1.1 da NBR ISO/IEC 17799:2005 (Documento da política de segurança da informação).

b) A Política de Controle de Acesso (PCA) para usuários Web existente no âmbito do Infoseg não contempla itens importantes recomendados pela NBR ISO/IEC 17799:2005, pois:

b.1) Não abrange todas as categorias de usuários – usuários host de atualização (usados pelas aplicações que executam nos módulos remotos e que atualizam o Índice Nacional) e os usuários da rede interna da gerência do Infoseg (item 11.1.1);

b.2) não é formalmente institucionalizada;

b.3) não contempla uma análise crítica periódica dos direitos de acesso dos usuários (item 11.2.4), pois não é previsto, por exemplo, o procedimento para cancelamento de contas de usuários.

c) Não há uma Metodologia de Desenvolvimento de Sistemas (MDS) formalmente aprovada para utilização no âmbito do Infoseg, em desconformidade com o previsto no item PO 8.3 do COBIT 4.0 (Padrões para desenvolvimento e aquisição), fato agravado pelo grande número de terceirizados da equipe (subitem 4.6).

d) Diante da insuficiência de normatização aplicável, não se pode identificar a responsabilidade quanto aos assuntos de segurança da informação no âmbito do Infoseg (item 6.1.3 da NBR ISO/IEC 17799:2005).

Podemos identificar como possíveis causas do registrado a falta de comprometimento quanto às questões de segurança da informação e a falta de responsabilidades formalmente definidas quanto à matéria. Como efeitos reais e potenciais temos existência de procedimentos não padronizados, deficiência nos controles internos, dificuldade ou impossibilidade de responsabilização quanto às questões de segurança, falta de cultura dos usuários da rede Infoseg sobre segurança da informação e a possibilidade de exposição de dados e informações a acessos não autorizados.

Conclui-se que as Políticas de Segurança da Informação estabelecidas pelo MJ não contribuem para uma boa gestão de segurança da informação na rede Infoseg, de forma que a Senasp deve adotar providências de forma a reverter esta situação.

4.4 INEXISTÊNCIA DE PLANO DE CONTINUIDADE DO NEGÓCIO

Evidenciou-se a inexistência, no âmbito da gerência do Infoseg, de um Plano de Continuidade do Negócio (PCN) ou procedimentos definidos que garantam, em caso de falhas ou desastres naturais significativos, a retomada em tempo hábil das atividades do sistema, protegendo os processos críticos.

Atualmente, 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. Esta 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. Há a necessidade da elaboração e aprovação formal de um PCN específico para o Infoseg, que deverá ser testado e atualizado periodicamente, e ser divulgado a todos os envolvidos, de acordo com os itens 14.1.4 e 14.1.5, da NBR ISO/IEC 17799:2005.

4.5 ESTRUTURA INSATISFATÓRIA DE RECURSOS HUMANOS

A estrutura organizacional do Ministério da Justiça, definida pelo Decreto nº 5.535, de 13.09.2005, demonstra que a gerência do Infoseg não está formalmente definida como unidade integrante do Ministério. 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 12 terceirizados. Esse número de funcionários é insuficiente para manter a produção e atender às demandas corretivas e evolutivas do sistema. 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. É difícil até mesmo encontrar substitutos dentro da própria equipe no caso de férias e outros afastamentos. A gerência do Infoseg fez um estudo e estimou em 36 o número ideal de pessoas para compor sua equipe.

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 ainda por cima com contrato temporário) é impossível que funções estratégicas de TI não sejam exercidas por prestadores de serviços, como as atividades de administrador da rede, de administrador de banco de dados e de gerente de desenvolvimento. As conseqüências diretas dessa desproporção entre o número de servidores efetivos e de prestadores de serviço 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.

O relatado encontra-se em desconformidade com o recomendado nos itens PO4.6 (Papéis e responsabilidades de TI) e PO4.12 (Assessoria de TI) do COBIT 4.0.

A Senasp necessita aumentar o número de servidores efetivos de forma que atividades estratégicas e sensíveis passem a ser exercidas por servidores públicos, tornando, assim, os ambientes de desenvolvimento e de produção do sistema mais estáveis e minimizando o risco de descontinuidade do Infoseg.

4.6 USABILIDADE DO SISTEMA INSATISFATÓRIA

Visando conhecer a opinião dos usuários da rede Infoseg, a equipe elaborou um questionário eletrônico contendo dezessete perguntas sobre a satisfação dos usuários na utilização dos quatro módulos de consulta da Rede. Os resultados finais da pesquisa (resumidos na Tabela 1) 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, devido à potencial desmotivação dos usuários para continuar consultando a rede Infoseg.

TABELA 1 - 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%	

Conclui-se que a gerência do Infoseg deve analisar as sugestões enviadas pelos usuários no questionário e estudar quais alterações são necessárias para melhorar os pontos fracos apontados.

5. CONSIDERAÇÕES FINAIS

A auditoria do TCU identificou no Infoseg graves impropriedades, sobretudo no que concerne à sua gestão, que indicam a necessidade imperiosa de aperfeiçoamento, dentre as quais registrou-se neste trabalho: insuficiência de regulamentação, inconsistências entre as bases de dados criminais e o IN, a inexistência de política de segurança de informação formalmente definida, inexistência de plano de continuidade do negócio, estrutura de recursos humanos e usabilidade do sistema insatisfatória.

Os benefícios potenciais estimados decorrentes da auditoria consistem no aperfeiçoamento do Infoseg e da sua gestão, de forma que o sistema possa evoluir para que os agentes de segurança pública possam tomar decisões com base em informações confiáveis. Os benefícios serão buscados por meio de determinações e recomendações que visam à criação de mecanismos que garantam a consistência entre as bases de dados dos estados e do Índice Nacional, à criação de arcabouço legal necessário à institucionalização e à melhoria da segurança do sistema atual, trazendo qualidade e confiabilidade às informações disponibilizadas pelo Infoseg.

Por fim, porém não menos importante, registre-se que as impropriedades relativas a segurança da informação registradas pela auditoria não são as únicas a comprometer a segurança do Infoseg. A segurança da informação no Infoseg depende também da segurança da informação nos entes que acessam o sistema (Secretarias de Justiça das UF, Tribunais de Justiça, Departamento de Polícia Federal, etc.), pois uma falha de segurança nesses entes afetará diretamente a credibilidade do sistema.

REFERÊNCIAS

1. ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT NBR ISO/IEC 17799:2005*: tecnologia da informação, técnicas de segurança, código de prática para a gestão da segurança da informação. 2. ed. Rio de Janeiro: ABNT, 2005.
2. BRASIL. *Constituição* (1988). Brasília, 1988. Disponível em: <http://www.planalto.gob.br/ccivil_03/Constituicao/Contituição.htm>. Acesso em: 19 out. 2007.
3. _____. Tribunal de Contas da União. Acírdão nº 71/2007, Plenário. Relator: Min. Augusto Sherman Cavalcanti. Brasília, 31 de janeiro de 2007. Ata 04/2007, Plenário. *Diário Oficial da União*, Brasília, 02 de fevereiro de 2007. Seção 1.
4. _____. _____. *Roteiro de auditoria de conformidade*. Brasília: TCU, Secretaria Adjunta de Fiscalização, 2003.
5. INFORMATION TECHNOLOGY GOVERNANCE INSTITUTE. *Control objectives for information and related technology*. Versão 3.0. 2000.
6. _____. _____. Versão 4.0. 2005.