PROGRAMA DE AUDITORIA DO SISTEMA DE TECNOLOGIA DA INFORMAÇÃO

I - SISTEMA

Rede de Tecnologia da Informação da CONAB (Rede Local).

II - CONCEITUAÇÃO

Constitui-se dos procedimentos relacionados com a área de Tecnologia da Informação, que visam garantir o funcionamento, manutenção e segurança da rede de comunicação de dados da Companhia Nacional de Abastecimento - CONAB.

III – ÁREAS ENVOLVIDAS

- DIRETORIA DE GESTÃO E LOGÍSTICA EMPRESARIAL - DIGEM

- SUPERINTENDÊNCIA DE MODERNIZAÇÃO EMPRESARIAL - SUMEP

- GERÊNCIA DE SISTEMAS DE INFORMAÇÃO - GESIN

- GERÊNCIA DE INFRA-ESTRUTURA TECNOLÓGICA - GETEC

IV – PERÍODO DE AUDITORIA

De / /2006 a / /2006.

V - OBJETIVOS

1. GERAIS

Segurança: certificar-se de que o sistema dá proteção adequada aos recursos da Rede e às informações armazenadas e transmitidas.

Desempenho: assegurar que a Rede esteja atendendo aos usuários, em termos de *performance* e disponibilidade.

Efetividade: avaliar se a Rede está atendendo à finalidade para que foi implantada,

se atende à Companhia Nacional de Abastecimento – Conab e está dentro das normas/políticas.

Administração de Recursos: avaliar se a administração dos recursos humanos, a terceirização e contratação de serviços estão dentro das leis/normas vigentes e se existe definição clara das funções de cada área.

2. ESPECÍFICOS

Segurança

- segurança lógica
- manutenções
- política de armazenamento
- trilha de auditoria
- documentação
- política de instalação e manutenção de produtos (*softwares*)
- política de combate a vírus
- segurança física

Desempenho

- gerência de *performance*
- consumo de recursos
- disponibilidade da rede
- monitoração

Efetividade

- desempenho para o usuário
- qualidade do suporte
- evolução da rede
- orientação ao usuário

Administração de Recursos

- gestão de pessoas
- gestão de contratos e terceirizações
- definição das funções dos órgãos envolvidos

VI - IDENTIFICAÇÃO DE RISCOS E LIMITAÇÕES

A auditoria será focada na rede local instalada em Brasília e nas Superintendências Regionais da Conab.
Não serão avaliados os *softwares* adquiridos no mercado e os desenvolvidos internamente, que dão suporte à rede.

VII – CRONOGRAMA

Etapas	Início	Fim
Pré-auditoria/Planejamento	xx/xx/2006	xx/xx/2006
Execução da Auditoria	xx/xx/2006	xx/xx/2006
Encerramento da Auditoria	xx/xx/2006	xx/xx/2006

VIII - EQUIPE DE AUDITORES

Será definida oportunamente.

IX - CUSTOS

AUDITORES	R$ 9.999,99
DIÁRIAS	R$ 9.999,99
PASSAGEM AÉREA	R$ 9.999,99
EMBARQUE/DESEMBARQUE	R$ 9.999,99
TOTAL	**R$ 9.999,99**

Brasília (DF), 10 de outubro de 2006.

X – PROCEDIMENTOS DE AUDITORIA

NA UNIDADE DE AUDITORIA	Tempo Previsto	Tempo Gasto
Levantamento prévio das particularidades do sistema a ser auditado		
1. Verifique a organização administrativa da Unidade a ser auditada		
2. Pesquise as competências e estrutura da Unidade a ser auditada.		
3. Pesquise e leia a legislação pertinente ao sistema a ser auditado.		
4. Estude o sistema, manuais, dossiê referente a última auditoria nesse sistema (se houver).		
5. Solicite à área tecnológica uma palestra sobre as funcionalidades e características do sistema.		
6. Solicite uma reunião com a área gestora do sistema, onde serão apresentados os objetivos do sistema.		
7. Elabore o fluxograma do sistema.		
8. Aplique o Questionário de Avaliação do Controle Interno.		
9. Solicite a carta de apresentação ao Chefe da Unidade de Auditoria		
10. Apresente-se ao Chefe da Unidade auditada, solicitando disponibilização de acesso aos dados da atividade, bem como aos servidores da área envolvida.		
Plano Diretor de Informática		
11. Verifique a existência e uso de planejamento ou política de longo prazo para a área tecnológica (Plano Diretor de Informática)		
12. Verifique a existência de previsão de investimentos a serem feitos em informática para o período abrangido e a definição das prioridades de atendimento.		
13. Verifique se o planejamento é adequado às necessidades da entidade, que tenha descrição clara das atividades, atribuições, prioridades e prazos de implementação, e que seja acompanhado e revisado periodicamente.		
Utilização e adequabilidade dos recursos computacionais e tecnológicos, e qualidade da gestão da rede.		
15. Verifique se foram estabelecidos padrões de uso dos recursos computacionais e do acompanhamento e controle do nível de uso dos equipamentos.		
16. Verifique se existem rotinas de acompanhamento sistemático do nível de uso dos recursos.		
17. Verifique a existência e efetividade da proteção anti-vírus.		
18. Verifique se há rotinas de acompanhamento de performance da rede e de observância do nível de obsolescência dos equipamentos.		
19. Verifique a efetividade do controle da saída de informações sigilosas.		
Gestão de recursos humanos		
20. Verifique se há clara definição e atribuição dos cargos e funções.		
21. Verifique se ocorre de fato segregação de funções – se as funções de análise,		

programação, teste e transferência de módulos para a produção são executadas por pessoas diferentes.		
22. Verifique a existência e cumprimento de política de treinamento, inclusive treinamento para situações de contingência .		
23. Verifique a existência de programa de conscientização da importância da segurança no ambiente de CPD.		
24. Verifique a existência e cumprimento de política de avaliação de desempenho e da produtividade dos analistas.		
25. Verifique se os sistemas não são proprietários de um analista, ou seja, não são dependentes do conhecimento específico de uma pessoa ou um pequeno grupo de pessoas.		
26. Verifique se a documentação referente aos sistemas é completa o bastante para garantir a sua manutenção.		
Custo da Área Tecnológica		
27. Verifique se as soluções implementadas são economicamente viáveis para a instituição e o custo total da área se justifica pelos seus produtos.		
Instalações Físicas		
28. Verifique a localização do CPD, se está fora de área de risco como estação repetidora de eletricidade, depósitos de papel ou material explosivo, etc..		
29. Verifique a efetividade do controle de acesso físico aos diversos ambientes da área.		
30. Verifique a qualidade e segurança das instalações elétricas e hidráulicas, se não existe risco de infiltração na sala do computador e na fitoteca, se estão preparadas para situações de contingência, existência de tubulação individual para a rede elétrica e lógica e outros.		
31. Verifique a existência e adequação de sistema de alarme e se é feita revisão e teste periódico do mesmo.		
Plano de Contingência		
32. Verifique a existência, adequação, teste periódico e revisão do plano de contingência.		
33. Verifique se o pessoal de segurança e corpo de bombeiros estão aptos a agirem em caso de sinistro.		
34. Verifique se o treinamento/orientação dados são suficientes para garantir que, em situação de emergência, essas pessoas não provocarão danos acima do esperado.		
35. Verifique a existência e confiabilidade do CPD back-up, se são feitos testes para garantir que os sistemas de informação serão processados em casos inesperados, e a definição de quais os sistemas ou suas funções são prioritários para o processamento.		
36. Verifique a existência e adequação de rotinas para reconstrução de arquivos magnéticos.		
37. Verifique a existência de inventário atualizado das chaves de todos os ambientes da área tecnológica.		
38. Verifique a existência de relação atualizada – nome e telefones de contato – das pessoas autorizadas a circular no ambiente dos computadores.		

Política de Segurança		
39. Verifique a existência, adequação e cumprimento das normas de segurança de acesso físico e lógico.		
40. Verifique a existência e cumprimento dos regulamentos e penalidades atribuídas contra a violação das normas de segurança, monitoração e controle dos acessos, principalmente a dados sensíveis.		
41. Verifique a existência e revisão periódica dos planos de seguro do CPD – tanto das máquinas e equipamentos, quanto das instalações físicas.		
42. Verifique a existência, adequação e cumprimento de contratos de manutenção, e se atendem aos requisitos definidos pelos fabricantes.		
43. Verifique a existência de fitoteca de segurança fora do CPD e adequação e segurança do transporte das fitas (são embaladas e mantidas em temperatura adequada, são protegidas contra calor e umidade)		
Normas Técnico-operacionais		
44. Verifique a existência e utilização de normas técnico-operacionais (padrões e procedimentos) para desenvolvimento, manutenção, teste, homologação, preparação e operação de sistemas, para transferência de módulos para a produção, para a concessão de acesso aos arquivos de produção e à biblioteca de desenvolvimento, para catalogação de programas nas bibliotecas de desenvolvimento e produção, para geração, transporte, armazenamento e teste dos arquivos back-up.		
45. Verifique a existência, adequação, cumprimento e revisões periódicas das normas, visando manter sua atualidade em relação às necessidades das atividades.		
Normas e Padrões para Aquisição de Produtos e Equipamentos de Tecnologia		
46. Verifique a adequação das normas ao cumprimento de leis vigentes para aquisições de softwares e hardwares.		
47. Verifique existência, adequação e cumprimento de normas para contratações de serviços no desenvolvimento e manutenção de sistemas – se essas normas contemplam, inclusive, a avaliação do serviço prestado, como por exemplo a efetividade das consultorias contratadas pela área tecnológica.		
Conclusão		
48. Elabore a conclusão do trabalho, relacionando os pontos passíveis de discussão e citação no relatório.		
Elabore minuta de relatório destacando as ocorrências identificadas e as recomendações efetuadas.		
49. Discuta com o supervisor o resultado do trabalho.		
50. Atualize o programa de auditoria, se for o caso, adequando-o para os futuros trabalhos.		
51. Referencie os papéis de trabalho, com a finalidade de constituição do dossiê da auditoria.		
52. Elabore o Relatório de Auditoria e encaminhe o processo ao chefe imediato.		

Elaborado por:	**Revisado por:**	**Data:**
		/ /

Num.	Questionário de Avaliação dos Controles Internos 1	ATENDE			Obs.
	Segurança	Sim	Não	Prej.	
	1 Segurança – Diretrizes				
1.a	A área de segurança da Conab participou das definições dos pontos concernentes à segurança da Rede?				
	1.1 Segurança Lógica				
1.1.a	**Acessos**				
1.1.a.1	São utilizadas senhas individualizadas para a administração da rede?				
1.1.a.2	O esquema previsto para concessão de acesso permite um controle adequado dos níveis de privilégio?				
1.1.a.3	A formatação/composição das senhas está atendendo às necessidades da Política de Segurança da entidade?				
1.1.a.4	A periodicidade de mudança de senha atende às necessidades da Política de Segurança?				
1.1.a.5	Existem autorizações formais dos administradores das diversas unidades para acesso fora do perfil pré-definido?				
1.1.a.6	Existe cancelamento/revogação de senhas por tentativas de acesso não concluídas? O controle está adequado?				
1.1.a.7	As contas do grupo Administrador estão sendo usadas de forma controlada?				
1.1.a.8	A *password* da conta Administrador está adequadamente protegida?				
1.1.a.9	As pessoas envolvidas na administração da rede possuem privilégios compatíveis com as atividades que executam?				
1.1.a.10	Os procedimentos de criação, alteração e manutenção de contas estão normatizados e essas normas são cumpridas?				
1.1.a.11	Os direitos dos diversos grupos de usuários estão corretamente setados?				
1.1.a.12	As senhas, em especial as de contas com acesso aos servidores, obedecem cuidados especiais para evitar violação?				
1.1.a.13	As sessões abertas são desconectadas automaticamente quando inativas por um longo período?				
1.1.a.14	Contas-modelo usadas para criação de outras contas estão desativadas?				
1.1.a.15	As contas *guest* estão inibidas em todos os servidores?				
1.1.a.16	Os administradores/operadores estão treinados para as tarefas de criação/manutenção de contas?				
1.1.a.17	Os administradores/operadores conhecem os controles de segurança necessários para a criação/manutenção de contas?				
1.1.a.18	Os recursos acessados por usuários e grupos estão de acordo com o especificado na Política de Segurança?				
1.1.a.19	Em casos de concessões especiais de acesso a recursos, estas são formalmente solicitadas e documentadas?				
1.1.a.20	Existem contas para os auditores com autoridade suficiente para permitir auditoria na rede?				
1.1.b	**Mecanismos de Proteção aos Dados**				
1.1.b.1	Os dados sensíveis (senhas, informações restritas etc.) que são armazenados ou que trafegam na Rede são criptografados?				
1.1.b.2	Os usuários estão orientados sobre os procedimentos necessários para protegerem seus diretórios e arquivos?				
1.1.b.3	As facilidades que permitem ver o tráfego na rede têm seu uso				

	controlado?				
1.1.b.4	Estão documentadas e analisadas as fragilidades que os aplicativos em funcionamento na Rede podem causar a ela?				
1.1.b.5	Caso existam *gateways* entre a rede e *mainframes,* esses possuem mecanismos de segurança implementados?				
1.1.b.6	É obrigatória a utilização de *password* para arquivos tipo BAT nas estações?				
1.1.b.7	Os mecanismos utilizados para proteção dos arquivos críticos estão adequados e atendem às necessidades das Unidades?				
1.1.c	**Acessos Remotos/Conexões Externas**				
1.1.c.1	Está adequado o critério de controle dos acessos remotos à Rede?				
1.1.c.2	Estão claros os critérios para concessão desse tipo de acesso?				
1.1.c.3	Estão sendo usadas as opções de segurança para as ligações *dial-up*?				
1.1.c.4	O número dos *modems* em funcionamento é de conhecimento restrito daqueles que necessitam do acesso remoto?				
1.1.c.5	Os *modems* oferecem segurança adicional, como senha e criptografia?				
1.1.c.6	Existe controle sobre os usuários que se conectam simultaneamente à Rede local e redes externas?				
	1.2 Manutenções				
1.2.1	São registrados regularmente os problemas da Rede, inclusive aqueles causados por usuários e aplicações?				
1.2.2	Existem orientações para os operadores sobre como registrar e solucionar os problemas?				
1.2.3	O registro dos problemas é analisado periodicamente para verificar deficiências no SW, no HW e no treinamento de usuários?				
1.2.4	Existe controle sobre o tempo de solução de problemas?				
1.2.5	As ocorrências relevantes são reportadas tempestivamente aos órgãos responsáveis pelo suporte técnico e administrativo?				
1.2.6	O controle das ocorrências da Rede em cada turno de operação e a passagem das mesmas para o turno seguinte são efetivos?				
1.2.7	Os encarregados da administração da Rede possuem conhecimentos suficientes do sistema operacional?				
1.2.8	As mudanças no sistema são autorizadas, testadas, documentadas, comunicadas e controladas?				
1.2.9	O contrato de manutenções preventivas para os equipamentos da sala de servidores da Rede é suficiente e está atendendo às necessidades?				
1.2.10	São observados todos os requisitos do fabricante previstos no contrato?				
	1.3 Política de Armazenamento				
	1.3.a Cópias de Segurança				
1.3.a.1	Está adequado o processo de *back-up* dos servidores?				
1.3.a.2	A estratégia de *back-up* (completo, diferencial, incremental etc.) atende às necessidades dos usuários?				
1.3.a.3	O processo de *back-up* está automatizado?				
1.3.a.4	Está sendo gravado *log* das ocorrências do processamento do *back-up* e esse *log* é examinado?				
1.3.a.5	São adequados a periodicidade e os prazos de retenção dos *back-ups* da Rede, inclusive dos *logs*?				
1.3.a.6	As fitas geradas no *back-up* são adequadamente identificadas, para evitar perda acidental ou sua não localização?				

1.3.a.7	As fitas de *back-up* contêm o nome do proprietário e estão setadas para que apenas ele tenha acesso aos dados?				
1.3.a.8	É utilizada a opção "Verificar após *back-up*", para comparar o resultado do *back-up* com o conteúdo do disco rígido?				
1.3.a.9	Os *back-ups* funcionam e é possível restaurá-los?				
1.3.a.10	Existe rotina de inventário periódico das fitas de *back-up* e essa rotina é cumprida?				
	1.3.b Recuperação de desastre				
1.3.b.1	Existe plano completo e claro de recuperação de acidentes e este é conhecido por todos os administradores/operadores?				
1.3.b.2	O plano foi testado e provou sua eficácia?				
1.3.b.3	As orientações para situações de emergência e os manuais estão disponíveis para todos os operadores?				
1.3.b.4	A equipe de administração da Rede conhece os mecanismos de inicialização do sistema e principais causas de problemas?				
1.3.b.5	Existem discos de inicialização do sistema, contendo os principais arquivos necessários?				
1.3.b.6	Existem discos de Reparação de Emergência para cada máquina?				
1.3.b.7	Os Discos de Reparação de Emergência são regerados sempre que se faz uma alteração na máquina?				
1.3.b.8	Existem discos contendo as informações sobre as partições dos discos de cada máquina?				
1.3.b.9	São anotadas as alterações feitas em cada servidor, de modo que nas ocorrências se possa descobrir as prováveis causas do erro?				
1.3.b.10	Existem meios automáticos de eliminação de arquivos sem uso, quando da sobrecarga dos discos?				
	1.4 Trilha de Auditoria				
1.4.1	É gravado, em *log* de segurança, as atividades dos administradores da Rede?				
1.4.2	É gravado, em *log* de segurança, os acessos a arquivos e diretórios sensíveis/críticos da Rede?				
1.4.3	São monitorados e registrados em *log* os processos que possam causar danos à Rede?				
1.4.4	O acesso aos *logs* está restrito às pessoas que devem examiná-los?				
1.4.5	É feita a análise periódica desses *logs* pelo responsável geral da Rede ou seu preposto?				
1.4.6	Estão adequados os processos definidos para preenchimento do *log* de auditoria e descarte das entradas, se o *log* estiver cheio?				
	1.5 Documentação				
1.5.1	A documentação da Rede está completa, atualizada e em ordem?				
1.5.2	Existem esquemas e diagramas que permitem aos administradores da Rede uma visão completa da mesma?				
1.5.3	As instruções para operação e monitoração da Rede estão completas e em ordem?				
1.5.4	Os manuais dos *softwares* utilizados estão disponíveis para a equipe que administra a Rede?				
1.5.5	Os nós da Rede estão devidamente mapeados?				
1.5.6	Os documentos e manuais são mantidos em local seguro e acessível para os componentes da equipe?				
1.5.7	Existe um catálogo dessa documentação e é feito o controle entre inventário e existência física da mesma?				
1.5.8	Os documentos indispensáveis à operação da Rede possuem cópias guardadas em local separado?				

	1.6 Política de Instalação e Manutenção de Produtos (Software)				
1.6.1	Existe catálogo completo e atualizado dos produtos utilizados na Rede?				
1.6.2	Os *softwares* e aplicativos utilizados na Rede foram devidamente testados e homologados?				
1.6.3	Os *softwares* utilizados na Rede estão devidamente licenciados?				
1.6.4	Existe sistema que evite a entrada de *softwares* não autorizados na Rede?				
1.6.5	É feita varredura periódica para detecção de programas piratas e material indevido na Rede?				
	1.7 Política de Combate a Vírus				
1.7.1	Estão definidos os procedimentos para se evitar contaminação de arquivos?				
1.7.2	São utilizados *softwares* anti-vírus na Rede e suas versões são atualizadas tempestivamente?				
1.7.3	É adequado o processo de instalação e atualização dos anti-vírus nos equipamentos (servidores e estações) da Rede?				
1.7.4	Existe sistema que detecta e elimina arquivos estranhos à Rede?				
1.7.5	Os mecanismos de prevenção abrangem todas as máquinas da Rede?				
1.7.6	Existe processo de conscientização dos usuários sobre os procedimentos para evitar a instalação de vírus na Rede?				
1.7.7	São monitoradas e documentadas as ocorrências de contágio?				
1.7.8	A Política de Segurança define normas para se evitar a contaminação da Rede e prevê sanções/penalidades para quem as infringe?				
	1.8 Segurança Física				
	1.8.a Equipamentos				
1.8.a.1	A sala dos servidores e equipamentos da Rede localiza-se longe de áreas de risco?				
1.8.a.2	A sala dos servidores e equipamentos da Rede está protegida contra poluição, infiltrações, umidade e calor excessivos?				
1.8.a.3	Estão sendo usadas *passwords* para ligar/ativar os servidores, para evitar que pessoas não autorizadas inicializem o sistema?				
1.8.a.4	Existem mecanismos de segurança contra acesso nos próprios servidores?				
1.8.a.5	O inventário dos *hardwares* utilizados na Rede, como servidores, impressoras, *modems* etc., está completo e atualizado?				
1.8.a.6	Os procedimentos de compra e manutenção de *hardware* e *software* estão adequados?				
1.8.a.7	Os computadores estão protegidos contra a incidência de raios solares?				
1.8.a.8	Os servidores estão protegidos contra problemas de alimentação por UPS/condicionadores de voltagem?				
1.8.a.9	As estações estão protegidas por condicionador de voltagem?				
	1.8.b Ambiente				
1.8.b.1	O acesso de pessoas à sala dos servidores e equipamentos da Rede está devidamente controlado?				
1.8.b.2	Existe controle de entrada e saída de pacotes da sala de servidores?				
1.8.b.3	A sala dos servidores e equipamentos da Rede encontra-se protegida de riscos de desastres com as tubulações físicas?				
1.8.b.4	Existem regras de conduta para os operadores sobre o ingresso de cigarros acesos, comida ou bebida na sala dos servidores?				

1.8.b.4	Existe controle sobre o cumprimento rigoroso dessas regras de conduta?				
1.8.b.5	É evitado o armazenamento de papel, listagens, fitas, materiais de limpeza, acessórios e outros materiais na sala dos servidores?				
1.8.b.6	A limpeza da sala dos servidores é adequada?				
1.8.b.7	A sala dos servidores possui mecanismos de prevenção contra incêndio?				
1.8.b.8	São realizados testes periódicos de funcionamento desses mecanismos?				
1.8.b.9	Existem sensores de temperatura e emissão de gases na sala dos servidores e equipamentos da Rede?				
1.8.b.10	Existe rede elétrica específica para os equipamentos servidores?				
1.8.b.11	Os servidores estão ligados a tomadas com carga elétrica adequada?				
1.8.b.12	São realizados testes para verificação do adequado dimensionamento e qualidade do conjunto de energia alternativa?				
1.8.b.13	Existe aterramento para o prédio onde se encontram os servidores da Rede?				
1.8.b.14	Os dutos para cabos lógicos estão separados dos dutos de cabos de eletricidade?				
1.8.b.15	Os cabos lógicos estão devidamente identificados e protegidos contra possíveis avarias?				
1.8.b.16	Existem interruptores de emergência próximos às saídas da sala dos servidores?				
	1.8.c *Back-ups*				
1.8.c.1	As fitas de *back-up* estão armazenadas em local seguro e em prédio diferente de onde ficam os servidores?				
1.8.c.2	O acesso físico à sala de armazenamento das fitas de *back-up* é controlado?				
1.8.c.3	As fitas de *back-up* são protegidas contra efeitos de campos magnéticos?				
	1.8.d Preparação do Pessoal				
1.8.d.1	O pessoal responsável recebe treinamento para prevenção e combate a incêndios?				
1.8.d.2	O pessoal está preparado para agir em caso de sinistro?				
1.8.d.3	São realizados testes periódicos de combate a incêndio com o pessoal responsável pela Rede?				
1.8.d.4	O pessoal está treinado para executar os procedimentos necessários à manutenção da segurança?				
1.8.d.5	Existe esquema formal de plantão para atendimento das necessidades dos usuários e este é acompanhado?				
	1.8.e Contingência				
1.8.e.1	A segurança na sala dos servidores funciona 24 horas por dia?				
1.8.e.2	São realizadas rondas por vigias no andar onde se encontra a sala dos servidores?				
1.8.e.3	Existe registro atualizado das principais chaves da sala dos servidores da Rede?				
1.8.e.4	Existe lista atualizada e acessível, contendo os principais nomes e telefones a serem chamados em caso de emergência?				
1.8.e.5	Os equipamentos da sala de servidores estão cobertos por seguro?				
1.8.e.6	Os equipamentos da sala de servidores são alimentados por mecanismos de fornecimento ininterrupto de energia elétrica?				
1.8.e.7	Tais mecanismos são suficientes para suportar a necessidade dos equipamentos da sala de servidores?				

1.8.e.8	Tais equipamentos são testados periodicamente?				
1.8.e.9	É realizada manutenção preventiva desses equipamentos?				

Num.	Questionário de Avaliação dos Controles Internos 2	ATENDE			Obs.
	Desempenho	Sim	Não	Prej.	
	2.1 Gerência de *Perfomance*				
	2.1.a Performance Atual				
2.1.a.1	Existe monitor para acompanhamento da Rede e este está atendendo às necessidades da Rede?				
2.1.a.2	Está adequado o tempo de resposta da Rede?				
2.1.a.3	Os operadores receberam treinamento sobre como monitorar a Rede e melhorar seu desempenho?				
2.1.a.4	Todos os procedimentos passíveis de automação estão automatizados?				
2.1.a.5	Os administradores sabem onde os *softwares* são executados e onde os dados são guardados?				
2.1.a.6	Na definição dos domínios da Rede foram analisadas as diversas opções de configuração possíveis?				
2.1.a.7	A Rede está programada para emitir automaticamente alertas em caso de problemas?				
	2.1.b Performance Desejada				
2.1.b.1	Existe definição de qual seria o padrão de performance desejado para a Rede?				
2.1.b.2	Esse documento contempla todos os itens da Rede?				
2.1.b.3	Existem ações visando atingir tal padrão?				
	2.1.c Prospecção para Melhorias				
2.1.c.1	Existem trabalhos ou planos de prospecção de novas soluções para atualização e melhoria da Rede?				
2.1.c.2	Esses trabalhos são permanentes e estão atendendo às necessidades de evolução da Rede?				
2.1.c.3	Estão definidos os pontos a serem mais valorizados na prospecção e estes atendem às necessidades da entidade?				
	2.1.d Análise de Uso - Vales e Picos				
2.1.d.1	Existem ações de acompanhamento para verificar períodos de maior uso da Rede?				
2.1.d.2	Durante os períodos de pico é feito acompanhamento para otimização dos recursos da Rede?				
2.1.d.3	Tem sido feita análise dos períodos de menor uso, com vistas a adequação dos horários de *back-up* da Rede?				
	2.1.e Situação de Contingência				
2.1.e.1	Está definido o mínimo de *performance* da Rede, em caso de contingência?				
2.1.e.2	A *performance* mínima tem sido atendida quando da ocorrência de contingência?				
2.1.e.3	Têm sido tomadas ações para adequação dos parâmetros mínimos definidos, quando não atendidos?				
	2.2 Consumo de Recursos				
2.2.1	O consumo dos recursos da Rede está dentro dos limites estabelecidos?				
2.2.2	Existe processo sistemático de acompanhamento do uso dos recursos da Rede - discos, meio de transmissão etc.?				

2.2.3	Existe trabalho de acompanhamento preventivo para evitar sobrecarga da Rede e garantir performance nas operações?				
	2.3 Disponibilidade da Rede				
	2.3.a Situação Normal				
2.3.a.1	É adequada a disponibilidade da Rede para os usuários?				
2.3.a.2	Os horários de funcionamento definidos para a Rede estão sendo cumpridos?				
2.3.a.3	Tais horários atendem às necessidades dos usuários?				
	2.3.b Situação de Contingência				
2.3.b.1	Estão definidos os períodos mínimos e máximo de acessos a recursos da Rede, em caso de contingência?				
2.3.b.2	Estão definidos os grupos de usuários prioritários na Rede, em caso de contingência?				
2.3.b.3	Estão definidos os produtos que ficarão disponíveis para acesso via Rede, em caso de contingência?				
2.3.b.4	Tem sido tomadas ações para adequação dos parâmetros mínimos definidos, quando não atendidos?				
	2.4 Monitoração				
	2.4.a Uso de Recursos para Prevenir Manutenções				
2.4.a.1	Está sendo usada alguma ferramenta para acompanhamento das manutenções corretivas e preventivas por equipamento da Rede?				
2.4.a.2	A ferramenta está atendendo às necessidades de acompanhamento?				
2.4.a.3	Existe algum trabalho de análise para verificar os equipamentos que apresentam maior número de ocorrências?				
2.4.a.4	É feito algum trabalho para melhoria na disponibilidade de equipamentos com grande número de ocorrência de chamados?				
	2.4.b Distribuição Adequada dos Recursos				
2.4.b.1	Existem mecanismos suficientes e adequados para monitorar os acessos e usos da Rede?				
2.4.b.2	É monitorada regularmente a *performance* da Rede, para verificar problemas de sobrecarga?				
2.4.b.3	É monitorado regularmente o uso da Rede no que diz respeito a abusos?				
Num.	**Questionário de Avaliação dos Controles Internos 3**	**ATENDE**			**Obs.**
	Efetividade	**Sim**	**Não**	**Prej.**	
	3.1 Desempenho				
	3.1.a Tempo de Resposta				
3.1.a.1	Na visão do usuário, o tempo de resposta da Rede está atendendo às suas necessidades?				
3.1.a.2	Existem intervalos nos quais o tempo de resposta da Rede fica lento?				
	3.1.b Disponibilidade da Rede				
3.1.b.1	O tempo (período) em que a Rede está disponível para uso atende às necessidades dos usuários?				
3.1.b.2	O número de pontos de rede instalados nas Unidades são suficientes para atendimento das necessidades dos usuários?				
3.1.b.3	Os recursos disponibilizados, como espaço em disco para arquivamento, atende às necessidades dos usuários?				
	3.1.c Desempenho dos Recursos Disponíveis/Alocados				

3.1.c.1	A Rede está contribuindo para melhorar a qualidade ou facilitar a execução dos serviços por parte dos usuários?				
3.1.c.2	Os equipamentos disponibilizados em cada Unidade estão adequados às suas necessidades?				
3.1.c.3	Os equipamentos, na visão dos usuários, funcionam a contento para atender as suas necessidades?				
	3.2 Qualidade do Suporte				
	3.2.a Atendimento				
3.2.a.1	Está sistematizado o processo de acolhimento de sugestões e reclamações dos usuários?				
3.2.a.2	Os usuários estão satisfeitos com a qualidade do atendimento aos pedidos de recuperação de arquivos?				
3.2.a.3	O atendimento às dúvidas sobre a Rede é satisfatório?				
3.2.a.4	Os usuários estão satisfeitos com o atendimento aos pedidos de manutenção e novas instalações?				
3.2.a.5	A qualificação técnica do pessoal de suporte à Rede atende às expectativas dos usuários?				
3.2.a.6	Os usuários estão satisfeitos com a atenção dispensada pelo pessoal de suporte à Rede?				
3.2.a.7	Os mecanismos usados para garantir integridade aos arquivos contra vírus e deleções indevidas atende às expectativas dos usuários?				
3.2.a.8	As mensagens de alerta são claras e completas para os usuários?				
	3.2.b Resolução de Problemas				
3.2.b.1	O atendimento aos pedidos de solução de erros e problemas está adequado às necessidades dos usuários?				
3.2.b.2	É dado tratamento adequado às reclamações sobre a falta de tempestividade na solução de problemas da Rede?				
3.2.b.3	Em casos de paradas ou problemas na Rede, caso seja possível, são enviados alertas e informações on-line aos usuários?				
3.2.b.4	É dado retorno aos usuários da análise sobre as sugestões encaminhadas?				
	3.3 Evolução da Rede				
	3.3.a Novos Produtos				
3.3.a.1	A agilidade na implementação de novos produtos, especialmente quando solicitada, atende às expectativas dos usuários?				
3.3.a.2	Existe processo sistematizado para acolhimento de sugestões para análise de novos produtos, especialmente quando específicos para determinadas funções?				
3.3.a.3	Tais sugestões, quando analisadas, sua conclusão é devidamente informada ao seu proponente?				
	3.3.b Implementação de Melhorias				
3.3.b.1	É feito trabalho permanente de implementação de melhoria na Rede?				
3.3.b.2	Esse trabalho satisfaz as expectativas e necessidades dos usuários?				
	3.4 Orientação ao usuário				
	3.4.a Sobre a Rede				
3.4.a.1	Existe programa de orientação e conscientização dos usuários para				

	utilização da Rede de maneira adequada?				
3.4.a.2	Existe orientação completa, disponibilizada permanentemente aos usuários, sobre os produtos instalados (*softwares*) na Rede?				
3.4.a.3	É feito trabalho permanente para divulgação de orientações de apoio ao uso da Rede?				
	3.4.b Disseminação da Política de Segurança				
3.4.b.1	Existe programa de divulgação e conscientização da Política de Segurança da Instituição?				
3.4.b.2	Os usuários conhecem o conteúdo da Política de Segurança, especialmente as normas que se aplicam à segurança da Rede?				
3.4.b.3	Na visão dos usuários, o conteúdo da Política, referente à segurança da Rede, está completo, objetivo e claro?				
3.4.b.4	Os usuários consideram o conteúdo da Política de Segurança adequado às necessidades de segurança da Rede?				
3.4.b.5	Os usuários são conscientizados dos riscos sobre o uso de programas piratas e *shareware*?				
3.4.b.6	Existe trabalho de conscientização dos usuários sobre riscos de armazenamento de material indevido na Rede?				
3.4.b.7	As transgressões às normas são tratadas conforme definição da Política de Segurança?				
	3.4.c Para Novos Produtos				
3.4.c.1	Os novos produtos, tão logo instalados na Rede, são procurados/utilizados pelos usuários?				
3.4.c.2	Existe programa de orientação aos usuários previamente à implantação de novos produtos (*software*)?				
3.4.c.3	As orientações prévias têm atendido às necessidades dos usuários?				

Num.	Questionário de Avaliação dos Controles Internos 4	ATENDE			Obs.
	Administração de Recursos	**Sim**	**Não**	**Prej.**	
	4.1 Gestão de Pessoas				
4.1.1	Estão claramente definidas as responsabilidades dos administradores da Rede e elas são por eles conhecidas?				
4.1.2	A equipe constituída está adequada para o atendimento das necessidades dos usuários?				
4.1.3	A distribuição das tarefas é feita formalmente e leva em consideração a capacitação dos funcionários?				
4.1.4	Existe programa de treinamento contínuo para o pessoal da Rede?				
4.1.5	Existe esquema formal de rodízio do pessoal, para evitar dependência na execução de determinada atividade?				
4.1.6	Foram estabelecidas as regras para acompanhamento e avaliação do desempenho e produtividade individual e da equipe?				
4.1.7	Tem sido feito acompanhamento das tarefa distribuídas e da produtividade acordada?				
4.1.8	A motivação e o relacionamento entre os participantes da equipe têm sido bons?				
4.1.9	É feita apuração de responsabilidade pelos prejuízos decorrentes de falhas na administração da Rede?				
	4.2 Gestão de Contratos e Terceirizações				
4.2.1	Os recursos terceirizados foram formalmente contratados?				
4.2.2	Nas admissões são adotadas precauções para checagem dos antecedentes dos contratados e seus conhecimentos?				
4.2.3	Nas admissões, os contratados recebem informação e treinamento				

	sobre a Política de Segurança da entidade e sobre a Rede?				
4.2.4	Nas dispensas, são adotados os procedimentos de segurança necessários, como exclusão imediata de privilégios de acessos?				
4.2.5	A qualidade dos serviços prestados pela contratada tem estado dentro dos padrões estabelecidos?				
4.2.6	São alocadas tarefas vitais da Rede a funcionários contratados?				
4.2.7	Existe programa de treinamento contínuo para o pessoal contratado sobre prevenção e combate a incêndio?				
4.2.8	O custo dos serviços contratados tem estado dentro dos parâmetros utilizados pelos demais serviços?				
4.2.9	Os recursos estão sendo alocados de acordo com o estabelecido no contrato?				
4.2.10	Estão previstos procedimentos de emergência em caso de greves?				
4.2.11	É feito o repasse de custos para a contratada, por falhas na operação da Rede, provocadas pelos contratados?				
4.2.12	Existe controle e acompanhamento efetivos, por parte do pessoal da entidade, sobre o trabalho executado pelos contratados?				
	4.3 Definição de Funções dos Órgãos envolvidos				
4.3.1	Existe definição clara das funções/atividades/tarefas de suporte, manutenção e desenvolvimento/prospecção da Rede?				
4.3.2	Está claramente definida a área responsável para cada atividade/tarefa?				
4.3.3	As áreas envolvidas com as funções da Rede estão trabalhando de forma integrada, possibilitando uma gestão coesa da mesma?				
4.3.4	As funções/atividades/tarefas foram distribuídas de acordo com a especialização e enfoque de cada área?				
4.3.5	A área tem autoridade técnica e administrativa suficiente para cumprimento dessas responsabilidades?				

QUESTIONÁRIO DE AVALIAÇÃO DE CONTROLES INTERNOS

CONCEITO DO AUDITOR

A partir dos assinalamentos dos itens do QACI, os auditores formam um conceito do sistema auditado. Esse conceito pode ser fixado a partir de uma escala padrão como, por exemplo:

CONCEITO	DESCRIÇÃO
1	Indica que os controles necessitam apenas de acompanhamento normal.
2	Os controles apresentam deficiências modestas, que podem ser corrigidas no andamento normal dos trabalhos.
3	Os controles apresentam uma combinação de deficiências e intempestividades, requerendo a tomada de ações corretivas.
4	Indica precariedade ou falhas de controle que propiciam o surgimento de problemas sérios. Exige urgentes ações corretivas.
5	Indica ausência ou total deficiência dos controles, implicando elevado risco e necessidade de imediatas ações corretivas.

Os conceitos variam de 1 a 5, onde 1 é o melhor e 5 o pior. Cada grupo de itens do QACI recebe um conceito, que orientará a avaliação geral do sistema, atribuída pelos auditores.

OBSERVAÇÕES

OBSERVAÇÕES

CONSTATAÇÕES DO AUDITOR

MATRIZ DE RISCO DAS CONSTATAÇÕES		
IMPACTO	•	•
	Baixa Probabilidade / Alto Impacto	**Alta Probabilidade / Alto Impacto**
	•	•
	Baixa Probabilidade / Baixo Impacto	**Alta Probabilidade / Baixo Impacto**
	PROBABILIDADE DE OCORRÊNCIA	

CONCEITUAÇÃO DOS CONTROLES INTERNOS		
Conceito	***Risco***	***Descrição***
A	Insignificante	Indica a conformidade dos controles com os normativos e as boas práticas desejáveis, bastando o monitoramento normal.
B	Baixo	Indica impropriedades ou disfunções modestas nos controles, que podem ser corrigidas no andamento normal dos trabalhos.
C	Moderado	Indica uma combinação de impropriedades e/ou disfunções leves, requerendo a tomada de ações corretivas.
D	Alto	Indica precariedade ou falhas de controle, que propiciam o surgimento de irregularidades. Exige urgentes ações corretivas.
E	Muito Alto	Indica ausência ou total deficiência de controles. Exige imediatas ações corretivas devido ao elevado risco de irregularidades.
CONCEITO DO AUDITOR SOBRE OS CONTROLES VERIFICADOS		

Elaborado por:	**Revisado por:**	**Data:**
		/ /