



AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL
SCS, Quadra 09, Lote C, Torre A - 6º Andar, Edifício Parque Cidade Corporate - Bairro Setor Comercial
Sul, Brasília/DF, CEP 70308-200
- www.anac.gov.br

Relatório de Auditoria Interna nº 20/2019/AUD-ANAC

RELATÓRIO DE AUTOAVALIAÇÃO DE CONTROLES

Relatório..... : 2019/020

Unidade da Avaliação..... : STI

1. PROCESSO DE NEGÓCIO: GERIR A CONFIGURAÇÃO E OS ATIVOS DE TI

1.1. Em cumprimento ao Plano Anual de Atividades de Auditoria Interna para o exercício de 2019, aprovado pela Diretoria Colegiada, em 28 de novembro de 2018, e de acordo com a Portaria nº 1.956, de 26 de junho de 2019, publicada no Boletim de Pessoal e Serviço – V.14 nº 26, de 28 de junho de 2019, apresentamos o Relatório relativo ao trabalho de autoavaliação realizado na Superintendência de Tecnologia da Informação (STI), no período de 01.07.2019 a 12.08.2019.

1.2. A Auditoria Interna atuou como facilitadora e coordenadora dessa Autoavaliação de Controles – AAC, com a finalidade de oferecer à unidade a oportunidade de avaliar e de melhorar, se necessário, os controles adotados para o alcance dos objetivos de negócio sob a sua responsabilidade.

1.3. Ressalta-se que os resultados dessa AAC estão apoiados em princípios de controle apregoados pela IN Conjunta MP/CGU nº 01/2016, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal, e pela publicação Controle Interno – Estrutura Integrada do COSO (*The Comitee of Sponsoring Organizations*), de maio de 2013.

1.4. Consoante o art. 3º da referida IN Conjunta, a definição e a operacionalização dos controles internos devem levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos das organizações públicas. Assim, neste trabalho, preliminarmente, identificou-se, no processo avaliado, o objetivo e seus requisitos.

2. OBJETIVO DO PROCESSO DE NEGÓCIO OBJETO DA AUTOAVALIAÇÃO

2.1. O objetivo do processo objeto da autoavaliação é auxiliar na adequada disponibilidade dos serviços de TI e no uso eficiente de ativos tecnológicos, mantendo as soluções de TI estáveis e íntegras, durante o seu ciclo de vida, viabilizando o alcance dos objetivos da ANAC. Para abordagem completa deste objetivo foram definidos os seguintes requisitos:

- *eficácia*: Manter atualizada uma base de informações que possibilite o controle dos ativos de TI, de versões e de mudanças referentes aos itens de configuração de TI.
- *eficiência*: Estruturar as informações sobre os ativos de TI e itens de configuração de maneira tempestiva e com custo-benefício adequado.
- *efetividade*: Auxiliar na manutenção da disponibilidade e na integridade dos sistemas e dos serviços de TI dentro das expectativas das unidades organizacionais da ANAC com a adequada relação de custo-

benefício no uso, configuração e aquisição dos ativos de TI.

- *informação*: Obter informações precisas, confiáveis e suficientes sobre os ativos de TI e itens de configuração; manter as informações restritas aos agentes responsáveis pela sua manutenção; e divulgar as informações às partes interessadas e autorizadas sempre que necessário.
- *conformidade*: Atuar em conformidade com as melhores práticas de gestão e configuração de ativos de TI.

3. IDENTIFICAÇÃO E AVALIAÇÃO DOS RISCOS

3.1. Com base nos requisitos do objetivo, identificou-se, no processo, os eventos de risco e suas respectivas causas que poderiam impactar adversamente o alcance de objetivos da Agência. Eventos, suas causas e consequências são os componentes do risco inerente, que é o nível de risco antes da consideração de qualquer ação de mitigação; incluindo, dentre elas, os controles internos da ANAC.

3.2. Nesse contexto, os eventos de riscos identificados foram avaliados e classificados sob a perspectiva de probabilidade (chance de algo acontecer) e impacto no alcance dos objetivos, levando-se em conta os seus componentes de causas e consequências. Também foram definidos os objetivos de controle necessário para tratar as vulnerabilidades relacionadas a estes eventos.

3.3. Com vista à otimização das análises, bem como compatibilizar o escopo com os recursos disponíveis para a realização deste trabalho, priorizou-se o universo de análise aos controles internos dos eventos com riscos inerentes definidos, em parceria com a unidade auditada, como *Muito Alto*, *Alto* e *Médio*, sem prejuízo, ressalte-se, de avaliação dos demais eventos em auditorias futuras.

3.4. Para cada evento priorizado, conforme os resultados das avaliações dos riscos inerentes, foram identificados e avaliados os controles existentes na unidade auditada para tratar as vulnerabilidades detectadas. Cabe informar que estes controles foram avaliados de acordo com o nível de eficácia constante do anexo II - *Classificação da Eficácia do Controle*.

3.5. A matriz, a seguir, representa a avaliação do risco residual, que resultou da relação entre a avaliação dos riscos inerentes e a classificação da eficácia das atividades de controle existentes. Acrescenta-se que o resultado do risco residual demonstra a qualidade do sistema de controle interno estruturado para cumprir os requisitos de eficácia, de eficiência, de efetividade, de informação e de conformidade necessários para o bom desempenho do processo e da Agência.

Matriz de Riscos Residuais

Matriz de Riscos Residuais do Processo							
RISCO INERENTE	Muito Alto	5					
	Alto	4	R-6 R-7		R-1 R-5 R-8 R-10 R-17		
	Médio	3			R-13	R-2 R-3 R-9	
	Baixo	2					
	Muito Baixo	1					
			5	4	3	2	1
			Fraco	Bom	Mediano	Fraco	Inexiste
			CONTROLE				

LEGENDA	
Sigla	Descrição
R-1	Ausência de informações sobre os ativos de TI e os itens de configuração devido à (ao) indisponibilidade de um repositório com todas as informações relevantes do ambiente de TI.
R-2	Informações sobre os ativos de TI e itens de configuração obtidos de forma intempestiva, devido à (ao) Evolução contínua do ambiente de TI.
R-3	Custo-benefício inadequado na obtenção das informações sobre os ativos de TI e itens de configuração, devido à (ao) grande volume de dados sobre os ativos de TI ou itens de configuração existentes no ambiente de TI.
R-4	Custo-benefício inadequado na obtenção das informações sobre os ativos de TI e itens de configuração, devido à (ao) manutenção de informações desnecessárias sobre os itens de TI. (Risco residual não avaliado)
R-5	Aquisição de ativos de TI além ou aquém do necessário para atender aos objetivos do negócio, devido à (ao) ausência de visão dos gestores e da área TI da real necessidade de ativos de TI para atender aos requisitos de negócio.
R-6	Aquisição de ativos de TI além ou aquém do necessário para atender aos objetivos do negócio, devido à (ao) conflito entre os interesses da organização e o agente responsável pela aquisição de ativos de TI.
R-7	Aquisição de ativos de TI além ou aquém do necessário para atender aos objetivos do negócio, devido à (ao) falta de planejamento das unidades organizacionais sobre suas necessidades de TI.
R-8	Indisponibilidade de sistemas de informação ou de serviços de TI acima do tolerado pela ANAC, devido à (ao) depreciação de ativos de TI com o tempo.
R-9	Indisponibilidade de sistemas de informação ou de serviços de TI acima do tolerado pela ANAC, devido à (ao) perda da integridade ou confiabilidade no repositório com todas as informações relevantes do ambiente de TI.
R-10	Indisponibilidade de sistemas de informação ou de serviços de TI acima do tolerado pela ANAC, devido à (ao) serviço contratado de suporte de TI com profissionais (analista de TI) em quantidade insuficiente, ou capacidade técnica inadequada.
R-11	Informações sobre os ativos de TI e itens de configuração imprecisas ou insuficientes, devido à (ao) perfil conservador ou liberal do agente responsável pela definição dos dados e das informações a serem entregues pelo repositório com as informações do ambiente de TI. (Risco residual não avaliado)
R-12	Informações sobre os ativos de TI e itens de configuração imprecisas ou insuficientes, devido à (ao) dados de ativos de TI e de itens de configuração serem excessivamente pulverizados pelo ambiente de TI. (Risco residual não avaliado)
R-13	Acesso ou manipulação das informações de ativos de TI e itens de configuração por pessoas não autorizadas, devido à (ao) dados armazenados no repositório apresentarem informações sensíveis da infraestrutura de TI à pessoas com interesses escusos.
R-14	Informações sobre ativos de TI e itens de configuração não disponibilizadas às partes interessadas (pessoas ou processos), devido à (ao) perda dos dados do repositório de ativos de TI e de itens de configuração. (Risco residual não avaliado)
R-15	Informações sobre ativos de TI e itens de configuração não disponibilizadas às partes interessadas (pessoas ou processos), devido à (ao) desinteresse dos gestores em tomarem conhecimento sobre as informações dos ativos de TI e dos itens de configuração. (Risco residual não avaliado)
R-16	Gestão dos ativos de TI executada de forma ad hoc, pontual, sem consideração às melhores práticas, devido à (ao) desconhecimento sobre os ganhos que a adoção das boas práticas de gerir ativos de TI e configuração podem trazer para a área de TI e a organização. (Risco residual não avaliado)
R-17	Disponibilização de ativos de TI (softwares) sem a observância do licenciamento adequado, devido à (ao) indisponibilidade de um repositório com informações sobre licenciamento dos ativos de TI.

4. RESULTADO DA AVALIAÇÃO

4.1. Os resultados da avaliação das atividades de controle, conforme as técnicas e os procedimentos utilizados, visam contribuir para o aperfeiçoamento da governança, da gestão de riscos e do sistema de controle. Ressalta-se que foram identificados riscos merecedores de atenção. Esta atenção será dada no sentido de aperfeiçoar ou de retificar atividades de controle, por meio de ações corretivas.

4.2. Acrescenta-se, também, que as informações constantes do presente relatório foram obtidas com base em entrevistas realizadas ou declarações dos responsáveis pelo alcance dos objetivos. Cabe observar que o auditor-facilitador, seguindo a metodologia de autoavaliação de controles, não realizou testes e nem levantamento de evidências para confirmar a presença e o funcionamento das atividades de controle analisadas.

Resumo do resultado da avaliação da eficácia do controle interno dos eventos de risco priorizados

Objetivos	Riscos	Objetivos de Controle	Nível Impacto	Nível Probabilidade	Risco Inerente	Nível Controle	Risco Residual
Manter atualizada uma base de informações que possibilite o controle dos ativos de TI, de versões e de mudanças referentes aos itens de configuração de TI.	R-1 Ausência de informações sobre os ativos de TI e os itens de configuração devido à (ao) indisponibilidade de um repositório com todas as informações relevantes do ambiente de TI.	Manter atualizado repositório central para conter todas as informações relevantes sobre os ativos de TI e itens de configuração e de suas versões.	Alto	Alto	Alto	Mediano	Médio
Estruturar as informações sobre os ativos de TI e itens de configuração de maneira tempestiva e com custo-benefício adequado.	R-2 Informações sobre os ativos de TI e itens de configuração obtidos de forma intertemporal, devido à (ao) Evolução contínua do ambiente de TI.	Registrar no melhor tempo as alterações no repositório de ativos de TI e de configurações.	Baixo	Alto	Médio	Inexistente	Alto
	R-3 Custo-benefício inadequado na obtenção das informações sobre os ativos de TI e itens de configuração, devido à (ao) grande volume de dados sobre os ativos de TI ou itens de configuração existentes no ambiente de TI.	Identificar e manter dados suficientes para suportar a tomada de decisão sobre mudanças, incidentes e problemas nos ativos de TI e nos itens de configuração.	Baixo	Alto	Médio	Inexistente	Alto
	R-4 Custo-benefício inadequado na obtenção das informações sobre os ativos de TI e itens de configuração, devido à (ao) manutenção de informações desnecessárias sobre os itens de TI.	Manter as informações estritamente necessárias para a execução do processo.	Baixo	Médio	Baixo		
Auxiliar na manutenção da disponibilidade e na integridade dos sistemas e dos serviços de TI dentro das expectativas das unidades organizacionais da ANAC com a adequada relação de custo-benefício no uso, configuração e aquisição dos ativos de TI.	R-5 Aquisição de ativos de TI além ou aquém do necessário para atender aos objetivos do negócio, devido à (ao) ausência de visão dos gestores e da área TI da real necessidade de ativos de TI para atender aos requisitos de negócio.	Reportar e possibilitar o gerenciamento de ativos de TI conforme os requisitos de negócio.	Muito Alto	Baixo	Alto	Mediano	Médio
	R-6 Aquisição de ativos de TI além ou aquém do necessário para atender aos objetivos do negócio, devido à (ao) conflito entre os interesses da organização e o agente responsável pela aquisição de ativos de TI.	Assegurar a aquisição de ativos de TI que atendam aos interesses da organização.	Muito Alto	Baixo	Alto	Forte	Baixo
	R-7 Aquisição de ativos de TI além ou aquém do necessário para atender aos objetivos do negócio, devido à (ao) falta de planejamento das unidades organizacionais sobre suas necessidades de TI.	Incentivar o planejamento das unidades organizacionais acerca das necessidades de TI.	Muito Alto	Baixo	Alto	Forte	Baixo
	R-8 Indisponibilidade de sistemas de informação ou de serviços de TI acima do tolerado pela ANAC, devido à (ao) depreciação de ativos de TI com o tempo.	Manter o ativo de TI apto para atender ao nível de disponibilidade exigido da TI pelo negócio.	Alto	Alto	Alto	Mediano	Médio
	R-9 Indisponibilidade de sistemas de informação ou de serviços de TI acima do tolerado nela	Assegurar a integridade e a					

	do tolerado pela ANAC, devido à (ao) serviço contratado de suporte de TI com profissionais (analista de TI) em quantidade insuficiente, ou capacidade técnica inadequada.	Realizar planejamento adequado dos recursos humanos necessários.	Alto	Médio	Alto	Mediano	Médio
Obter informações precisas, confiáveis e suficientes sobre os ativos de TI e itens de configuração; manter as informações restritas aos agentes responsáveis pela sua manutenção; e divulgar as informações às partes interessadas e autorizadas sempre que necessário.	R-11 Informações sobre os ativos de TI e itens de configuração imprecisas ou insuficientes, devido à (ao) perfil conservador ou liberal do agente responsável pela definição dos dados e das informações a serem entregues pelo repositório com as informações do ambiente de TI.	Definir institucionalmente os dados e as informações do repositório com as informações do ambiente de TI	Baixo	Médio	Baixo		
	R-12 Informações sobre os ativos de TI e itens de configuração imprecisas ou insuficientes, devido à (ao) dados de ativos de TI e de itens de configuração serem excessivamente pulverizados pelo ambiente de TI.	Manter o nível de granularidade de informações necessárias para o repositório de ativos de TI e de configuração.	Baixo	Alto	Médio		
	R-13 Acesso ou manipulação das informações de ativos de TI e itens de configuração por pessoas não autorizadas, devido à (ao) dados armazenados no repositório apresentarem informações sensíveis da infraestrutura de TI à pessoas com interesses escusos.	Restringir o acesso às informações relevantes do ambiente de TI do repositório.	Médio	Médio	Médio	Mediano	Médio
	R-14 Informações sobre ativos de TI e itens de configuração não disponibilizadas às partes interessadas (pessoas ou processos), devido à (ao) perda dos dados do repositório de ativos de TI e de itens de configuração.	Manter disponível os dados do repositório de ativos de TI e de itens de configuração.	Baixo	Médio	Baixo		
	R-15 Informações sobre ativos de TI e itens de configuração não disponibilizadas às partes interessadas (pessoas ou processos), devido à (ao) desinteresse dos gestores em tomarem conhecimento sobre as informações dos ativos de TI e dos itens de configuração.	Manter o interesse dos gestores nas informações dos ativos de TI e dos itens de configuração.	Baixo	Médio	Baixo		
Atuar em conformidade com as melhores práticas de gestão e configuração de ativos de TI.	R-16 Gestão dos ativos de TI executada de forma ad hoc, pontual, sem consideração às melhores práticas, devido à (ao) desconhecimento sobre os ganhos que a adoção das boas práticas de gerir ativos de TI e configuração podem trazer para a área de TI e a organização.	Disseminação das melhores práticas para a gestão de ativos e itens de configuração.	Baixo	Médio	Baixo		
	R-17 Disponibilização de ativos de TI						

Fonte: Sistema de Identificação e Avaliação de Riscos da AUD - SiRIS

5. AÇÃO CORRETIVA

5.1. Diante dos resultados da avaliação, identificou-se a necessidade de corrigir falhas de controle para mitigar os riscos residuais classificados como *Médio e Alto*. Para isso, serão realizadas as seguintes ações corretivas detalhadas a seguir:

C01 - Manter atualizado repositório central para conter todas as informações relevantes sobre os ativos de TI e itens de configuração e de suas versões.		
1) Ação corretiva	Criticidade	Prazo
a. Identificar todos os ativos em um repositório em que conste a situação atualizada do ativo, o repositório deve estar alinhado com os processos de gerenciamento de mudanças e gerenciamento de configuração.	Média	31/03/2020
b. Manter um repositório atualizado de itens de configuração, revisando as alterações propostas para os ICs em relação a linha de base.	Média	31/03/2020
2) Benefício esperado	Tipo	Dimensão
a. Obtenção da informação, de forma imediata e confiável, sobre o status dos ativos e itens de configuração de TI, possibilitando a tomada de decisões alinhadas com as diretrizes de negócio.	Não Financeiro	Objetivo - Estratégico

C02 - Registrar no melhor tempo as alterações no repositório de ativos de TI e de configurações.		
1) Ação corretiva	Criticidade	Prazo
a. Estabelecer e manter um repositório de configuração de referência, mantendo linhas de base de configuração controladas.	Média	31/03/2020
b. Identificar regularmente todas as mudanças dos itens de configuração.	Média	31/03/2020
2) Benefício esperado	Tipo	Dimensão
a. Possibilitar a implementação de um processo de gestão de ativos e itens de configuração eficiente e padronizado.	Não Financeiro	Processo - Estratégico

C03 - Identificar e manter dados suficientes para suportar a tomada de decisão sobre mudanças, incidentes e problemas nos ativos de TI e nos itens de configuração.		
1) Ação corretiva	Criticidade	Prazo
a. Definir e chegar a um acordo sobre o escopo e o nível de detalhe para o gerenciamento da configuração.	Média	24/09/2020
2) Benefício esperado	Tipo	Dimensão
a. Ter claro o nível de profundidade da análise e obtenção de informação dos ativos e itens de configuração de TI.	Não Financeiro	Processo - Estratégico

C05 - Reportar e possibilitar o gerenciamento de ativos de TI conforme os requisitos de negócio.		
1) Ação corretiva	Criticidade	Prazo
a. Verificar se os recursos de TI são adequados à finalidade, determinando regularmente se cada ativo continua a fornecer valor, estimando a vida útil do item.	Média	24/09/2020
2) Benefício esperado	Tipo	Dimensão
b. Compreensão da adequação ao uso dos ativos de TI, possibilitando a substituição por equipamentos de melhor custo-benefício.	Não Financeiro	Processo - Estratégico

C06 - Assegurar a aquisição de ativos de TI que atendam aos interesses da organização.		
1) Ação corretiva	Criticidade	Prazo
Não serão sugeridas ações corretivas para este risco, tendo em vista que, conforme a matriz de riscos residuais, a sua criticidade é classificada como baixa.	Baixa	-

C07 - Incentivar o planejamento das unidades organizacionais acerca das necessidades de TI.		
1) Ação corretiva	Criticidade	Prazo
Não serão sugeridas ações corretivas para este risco, tendo em vista que, conforme a matriz de riscos residuais, a sua criticidade está classificada como baixa.	Baixa	-

C08 - Manter o ativo de TI apto para atender ao nível de disponibilidade exigido da TI pelo negócio.		
1) Ação corretiva	Criticidade	Prazo
a. Gerenciar ativos críticos, considerando regularmente o risco de falha e a necessidade de substituição.	Média	31/03/2020
b. Estabelecer um plano de manutenção preventiva para todo o hardware, considerando análise custo-benefício, as recomendações do fornecedor, risco de interrupção e pessoal qualificado.	Média	31/03/2020

2) Benefício esperado	Tipo	Dimensão
a. Diminuição da probabilidade de indisponibilidade de ativos de rede importantes e consequente paralisação de serviços críticos da Agência.	Não Financeiro	Objetivo - Estratégico

C09 - Assegurar a integridade e a confiabilidade do repositório de ativos de TI e de configuração.		
1) Ação corretiva	Criticidade	Prazo
a. Verificar periodicamente os itens de configuração e ativos, comparando configurações físicas e lógicas, usando ferramentas de descoberta apropriadas.	Média	30/04/2020
b. Definir e revisar periodicamente a meta para a integralidade do repositório de configuração conforme a necessidade do negócio.	Média	30/04/2020
2) Benefício esperado	Tipo	Dimensão
a. Aumento do nível de confiança das informações armazenadas na base de ativos e itens de configuração.	Não Financeiro	Processo - Estratégico

C10 - Realizar planejamento adequado dos recursos humanos necessários.		
1) Ação corretiva	Criticidade	Prazo
A ação corretiva relacionada a este objetivo de controle já é objeto da AAC-2019/009 sob a responsabilidade da STI.	Média	

C13 - Restringir o acesso às informações relevantes do ambiente de TI do repositório.		
1) Ação corretiva	Criticidade	Prazo
a. Descartar ativos quando eles não mais servirem a nenhum propósito útil, eliminando-os de forma segura, considerando a exclusão permanente de quaisquer dados gravados.	Média	31/03/2020
b. Certificar-se de que os serviços de acesso remoto e perfis de usuário (ou outros meios utilizados para a manutenção ou diagnóstico) sejam ativos somente quando necessário.	Média	31/03/2020
2) Benefício esperado	Tipo	Dimensão
a. Resguardar a segurança da informação.	Não Financeiro	Objetivo - Estratégico

C17 - Manter um repositório com informações acerca do licenciamento de ativos de TI, incluindo todos os tipos de softwares.		
1) Ação corretiva	Criticidade	Prazo
a. Manter um registro de todas as licenças de software adquiridas, bem como acordos e licenciamentos associados.	Média	30/04/2020

b. Conduzir auditorias regulares para identificar todas as instâncias dos softwares licenciados instalados, comparando o número de instâncias com o número de licenças detidas.	Média	30/04/2020
2) Benefício esperado	Tipo	Dimensão
a. Prover conformidade com a legislação referente a propriedade intelectual.	Não Financeiro	Objetivo - Transversal

ANEXO I – DETALHAMENTO DO PLANO DE AÇÃO CORRETIVA

C01 - Manter atualizado repositório central para conter todas as informações relevantes sobre os ativos de TI e itens de configuração e de suas versões.			
C02 - Registrar no melhor tempo as alterações no repositório de ativos de TI e de configurações.			
Produto a ser entregue			
Repositório de ativos de TI e itens de configuração de referência, contendo todos os atributos previstos em seus respectivos processos, com linhas de base definidas.			
Passo	Etapa	Responsável	Prazo Final
1	Avaliar e definir a ferramenta de repositório de ativos de TI. Critérios de avaliação: Discovery automático; criação e atualização de linha de base (serviços); mapas gráficos.	STI	20/10/2019
2	Implementar Discovery automático.	STI	31/03/2020
3	Criação e atualização das linhas de base de acordo com as mudanças; definindo os tempos de atualização.	STI	31/03/2020

C02 - Registrar no melhor tempo as alterações no repositório de ativos de TI e de configurações.			
C03 - Identificar e manter dados suficientes para suportar a tomada de decisão sobre mudanças, incidentes e problemas nos ativos de TI e nos itens de configuração.			
C05 - Reportar e possibilitar o gerenciamento de ativos de TI conforme os requisitos de negócio.			
Produto a ser entregue			
Processo de gestão de configuração onde conste a necessidade do registro das mudanças ocorridas nos itens de configuração e ativos e o nível de detalhe do gerenciamento de configuração. O processo também deverá prever a necessidade de verificação da vida útil dos ativos de TI.			
Passo	Etapa	Responsável	Prazo Final
1	Revisar o processo de gestão de mudança e gestão de configuração.	STI	20/01/2020
2	Implantar o processo de gestão de mudança e gestão de configuração (treinamento, criação de procedimentos e customizações necessárias).	STI	24/09/2020

C08 - Manter o ativo de TI apto para atender ao nível de disponibilidade exigido da TI pelo negócio.			
Produto a ser entregue			
Plano de manutenção preventiva dos ativos críticos de TI.			
Passo	Etapa	Responsável	Prazo Final

1	Verificar atendimento junto às ordens de serviço rotineiras e/o contratos de manutenção e suporte a fim de implementar o plano de manutenção corretiva. (conforme Termo de Referência)	STI	31/07/2020
---	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----	------------

C09 - Assegurar a integridade e a confiabilidade do repositório de ativos de TI e de configuração.			
C17 - Manter um repositório com informações acerca do licenciamento de ativos de TI, incluindo todos os tipos de softwares.			
Produto a ser entregue			
Definição de rotinas periódicas de verificação do inventário de ativos (incluindo licenças de software) e itens de configuração conforme nível de integridade (percentual de conformidade) a ser definido.			
Passo	Etapa	Responsável	Prazo Final
1	Executar as atividades referentes a inventário de ativos definidas no processo de gerenciamento de configuração: Software de Data Center (GEIT)	STI/GEIT	30/04/2020
2	Executar as atividades referentes a inventário de ativos definidas no processo de gerenciamento de configuração: Software de Desktop (GTPP)	STI/GTPP	30/04/2020

C13 - Restringir o acesso às informações relevantes do ambiente de TI do repositório.			
Produto a ser entregue			
Definição de rotina para descarte de equipamentos de informática prevendo a destruição de todos os dados contidos no equipamento.			
Passo	Etapa	Responsável	Prazo Final
1	Elaboração do plano de descarte de equipamentos (verificar o documento de gestão de ativos).	STI/GEIT/GTPP	31/03/2020

ANEXO II - RÉGUA DE AVALIAÇÃO DE EFICÁCIA DOS CONTROLES

Classificação da Eficácia do Controle		
Nota	Nível de Eficácia	Descrição
0-1	Inexistente	Ausência completa de controle
1-2	Fraco	Controle depositado na esfera de conhecimento pessoal dos operadores do processo, em geral realizado individualmente. Há um elevado grau de confiança no conhecimento das pessoas e, conseqüentemente, maior probabilidade de erros
2-3	Regular	Controle pode falhar por não contemplar todos os aspectos relevantes do risco, pois embora a atividade de controle implementada mitigue nuances do risco associado, não o faz apropriadamente, seja por não contemplar todos os seus aspectos relevantes ou por ser ineficiente em seu desenho técnico ou nas ferramentas utilizadas
3-4	Bom	Controle normatizado e executado. Embora passível de aperfeiçoamento, está sustentado por ferramentas adequadas e mitiga o risco razoavelmente

4-5	Forte	Controle mitiga o risco associado em todos os aspectos relevantes, podendo ser enquadrado num nível de “melhor prática”
-----	-------	-------------------------------------------------------------------------------------------------------------------------



Documento assinado eletronicamente por **Gustavo Sanches, Superintendente de Tecnologia da Informação**, em 01/10/2019, às 18:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **Woshington Rodrigues da Silva, Analista Administrativo**, em 02/10/2019, às 07:08, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



Documento assinado eletronicamente por **COSME LEANDRO DO PATROCINIO, Auditor-Geral**, em 07/10/2019, às 08:28, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site <https://sei.anac.gov.br/sei/autenticidade>, informando o código verificador **3187444** e o código CRC **E6439B5C**.