RELATÓRIO DE AUDITORIA

Agência Nacional de Aviação Civil

Superintendência de Tecnologia da Informação – STI

Nome do Sistema	Versão	Nome do Fornecedor
Auditores		

SEGURANÇA DO SISTEMA OU SOLUÇÃO UTILIZADA				
No tocante aos requisitos de segurança, a solução planejada deverá implementar minimamente:				
Item Auditado				
1) A solução possui criptografia digital assimétrica?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Documento do fabricante informando que a solução possui criptografia digital assimétrica em suas funcionalidades.			
No tocante aos requisitos de segurança, a solução planejada deverá implementar minimamente:				
Item Auditado				
2) A solução possui assinatura digital e eletrônica?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Documento do fabricante informando que a solução possui assinatura digital e eletrônica.			
No tocante aos requisitos de segurança, a solução planejada deverá implementar minimamente:				
Item Auditado				
3) A solução implementa hashing?	**Conforme**		**Não Conforme**	**X**
Evidências				
Resultados Esperados	Documento do fabricante informando que implementa *hashing.*			
ASSINATURA ELETRÔNICA				

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:				
Item Auditado				
4) A solução possui singularidade?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Uma assinatura eletrônica só é válida se for exclusiva ao signatário individual.			

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:				
Item Auditado				
5) A solução possui controle?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Uma assinatura eletrônica válida deve estar sob o exclusivo controle do signatário e exigir que o signatário use um nome de usuário e uma senha únicos para acessar o sistema e afixar a assinatura.			

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:				
Item Auditado				
6) A solução possui notificação?	**Conforme**		**Não Conforme**	**X**
Evidências				
Resultados Esperados	O sistema deve notificar o signatário de que a assinatura foi afixada.			

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:				
Item Auditado				
7) O signatário é solicitado antes que sua assinatura seja afixada?	**Conforme**	**X**	**Não Conforme**	
Evidências				

Resultados Esperados	Deve haver uma palavra ou declaração de intenção que transmite definitivamente a intenção do signatário de afixar sua assinatura.				
O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:					
Item Auditado					
8) O signatário toma ações deliberadas e reconhecíveis para afixar sua assinatura?		**Conforme**	**X**	**Não Conforme**	
Evidências					
Resultados Esperados	Fica claro ao signatário o que está sendo assinado, inclusive permitindo revisar ou modificar o conteúdo a ser assinado?				
O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:					
Item Auditado					
9) A solução possui associação da assinatura?		**Conforme**	**X**	**Não Conforme**	
Evidências					
Resultados Esperados	Uma assinatura deve ser anexada, ou logicamente associada, ao registro ou documento que está sendo assinado, caso contrário, tal registro ou documento não será considerado legalmente válido.				
O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:					
Item Auditado					
10) A solução é rastreável e recuperável?		**Conforme**		**Não Conforme**	**X**
Evidências					
Resultados Esperados	O usuário deve ser capaz de identificar e recuperar os documentos aos quais sua assinatura eletrônica foi aplicada.				
O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:					
Item Auditado					
11) A solução implementa rastreabilidade positiva ao indivíduo que assinou um registro, ou qualquer outro documento, sobre a sua assinatura?		**Conforme**	**X**	**Não Conforme**	
Evidências					

Resultados Esperados	Um processo de assinatura eletrônica deve ser seguro e deve impedir o acesso não autorizado ao sistema que afixa a assinatura aos documentos ou registros pretendidos.

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:

Item Auditado				
12) A solução é permanente e inalterável?	**Conforme**	**X**	**Não Conforme**	

Evidências	
Resultados Esperados	Uma assinatura eletrônica válida deve ser uma parte permanente do registro ou documento ao qual foi afixada. As informações contidas no registro ou documento devem ser inalteráveis sem uma nova assinatura para validar a alteração.

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:

Item Auditado				
13) A solução possui identificação e autenticação?	**Conforme**	**X**	**Não Conforme**	

Evidências	
Resultados Esperados	O software de assinatura eletrônica deve ter capacidades de autenticação que podem identificar uma assinatura como pertencente apenas a um determinado signatário. Um indivíduo que use uma assinatura eletrônica deve ser obrigado a usar um método de autenticação que identifique positivamente o indivíduo dentro do sistema de assinatura eletrônica.

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:

Item Auditado				
14) A solução é corrigível?	**Conforme**	**X**	**Não Conforme**	

Evidências	
Resultados Esperados	Um processo de assinatura eletrônica deve incluir um meio para que um detentor de certificado corrija registros ou documentos que foram assinados eletronicamente por erro, bem como os documentos em que uma assinatura está corretamente adotada, mas as informações ou dados estão em erro. Uma assinatura eletrônica deve ser invalidada sempre que uma entrada substitutiva for feita para corrigir o registro ou documento. As informações ou assinaturas que estão sendo corrigidas devem ser anuladas, mas permanecerem no lugar. A nova informação e / ou assinatura devem ser facilmente identificáveis.

O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:

Item Auditado

15) A solução possui um meio de arquivar os documentos assinados eletronicamente de forma segura?	**Conforme**		**Não Conforme**	**X**
Evidências				
Resultados Esperados	Deve haver um meio para que os documentos assinados eletronicamente sejam arquivados de forma segura			
O processo de assinatura eletrônica dos registros e/ou documentos deverá descrever, conter ou endereçar, minimamente, os seguintes aspectos:				
Item Auditado				
16) A solução garante que a assinatura não pode ser negada (repudiada) pelo responsável pela assinatura?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Um processo de assinatura eletrônica deve conter procedimentos e controles que assegurem a autenticidade da assinatura e impeça que o responsável pela assinatura negue ter afixado sua assinatura a um registro, documento ou dado específico.			
O sistema a ser utilizado deverá possuir e seguir políticas e procedimentos para assegurar a segurança e integridade das informações nele registradas seguindo minimamente os seguintes				
Item Auditado				
17) A solução possui processo de auditoria?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Políticas e procedimentos de assinatura eletrônica deverão incluir um processo de auditoria para garantir que todos os requisitos para assinaturas eletrônicas continuem a ser atendidos. O processo deve incluir o reconhecimento não autorizado de eventos, que inclui ações a serem tomadas pelo titular do certificado após a descoberta de uma tentativa de um indivíduo não autorizado de usar uma assinatura eletrônica.			
O sistema a ser utilizado deverá possuir e seguir políticas e procedimentos para assegurar a segurança e integridade das informações nele registradas seguindo minimamente os seguintes				
Item Auditado				
18) A solução possui alteração de processos?	**Conforme**		**Não Conforme**	**X**
Evidências				

Resultados Esperados	As políticas e os procedimentos do processo de assinatura eletrônica de um detentor de certificado devem abordar como o detentor do certificado enviará alterações ao processo de assinatura eletrônica para ANAC.				
O sistema a ser utilizado deverá possuir e seguir políticas e procedimentos para assegurar a segurança e integridade das informações nele registradas seguindo minimamente os seguintes					
Item Auditado					
19) A solução possui backup e preservação de Dados?		**Conforme**	**X**	**Não Conforme**	
Evidências					
Resultados Esperados	A política e os procedimentos devem abordar como os dados de backup e preservação dos dados serão realizados.				
O sistema a ser utilizado deverá possuir e seguir políticas e procedimentos para assegurar a segurança e integridade das informações nele registradas seguindo minimamente os seguintes					
Item Auditado					
20) A solução possui treinamento e usabilidade?		**Conforme**	**X**	**Não Conforme**	
Evidências					
Resultados Esperados	As políticas e os procedimentos de um detentor de certificado devem incluir qualquer treinamento e instruções necessárias para garantir que usuários autorizados compreendam como acessar e aplicar corretamente o processo de assinatura eletrônica.				
INTEGRIDADE E CONFIABILIDADE DA INFORMAÇÃO					
Visando a integridade e confiabilidade da informação, o sistema deverá, comprovadamente, demonstrar:					
Item Auditado					
21) O sistema demonstra como o processo de assinatura eletrônica previne que pessoas não autorizadas assinem um documento ou registro?		**Conforme**		**Não Conforme**	**X**
Evidências					
Resultados Esperados	Processos aplicados/processo de assinatura eletrônica previnem que alguém além do signatário/pessoas não autorizadas consigam assinar o registro ou documento.				
Visando a integridade e confiabilidade da informação, o sistema deverá, comprovadamente, demonstrar:					
Item Auditado					
22) Como as modificações em um documento assinado são evitadas sem uma nova assinatura?		**Conforme**	**X**	**Não Conforme**	
Evidências					

Resultados Esperados	Evidências de como as modificações em um documento assinado são evitadas sem uma nova assinatura.

Visando a integridade e confiabilidade da informação, o sistema deverá, comprovadamente, demonstrar:

Item Auditado				
23) Como a assinatura é afixada de forma permanente ao documento ou registro a ser assinado?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Evidências de como a assinatura é afixada de forma permanente ao documento ou registro a ser assinado.			

Os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

Item Auditado				
24) O sistema protege informações confidenciais?	**Conforme**		**Não Conforme**	**X**
Evidências				
Resultados Esperados	Evidências de como o sistema protege informações confidenciais?			

Os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

Item Auditado				
25) O sistema garante que a informação em um registro eletrônico não seja alterada de forma não autorizada?	**Conforme**	**X**	**Não Conforme**	
Evidências				
Resultados Esperados	Evidências de como o sistema garante que a informação em um registro eletrônico não seja alterada de forma não autorizada.			

Os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

Item Auditado				
26) O sistema providencia acesso seguro e conter garantias contra acesso não autorizado?	**Conforme**	**X**	**Não Conforme**	

Evidências	
Resultados Esperados	Evidências de como o sistema providencia acesso seguro e conter garantias contra acesso não autorizado

Os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

Item Auditado				
27) O detentor de sistema certificado fornece seus registros em um formato aceitável pela Agência?	**Conforme**		**Não Conforme**	**X**

Evidências	
Resultados Esperados	Evidências do compartilhamento de informações do sistema sendo compatível com os requisitos da ANAC.

Os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

Item Auditado				
28) O sistema possui procedimentos para auditoria periódica de forma a garantir a qualidade, integridade e precisão do sistema?	**Conforme**		**Não Conforme**	**X**

Evidências	
Resultados Esperados	Um registro da auditoria deverá ser preenchido e mantido em arquivo.

Os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

Item Auditado				
29) O sistema inclui procedimentos de manutenção e suporte que incluem provisões para interrupções de sistema eletrônico (hardware, software, rede de aplicativos etc) e o protege contra a perda de dados de registro?	**Conforme**	**X**	**Não Conforme**	

Evidências	
Resultados Esperados	O sistema deverá incluir medidas de backup para manter e fornecer acesso aos registros em caso de falha do sistema. O sistema de backup poderá ser um sistema eletrônico separado, um servidor de backup ou uma unidade de backup. O backup também poderá incluir mídia como impressão ou CD-ROM, unidade externa ou outra mídia aceitável pela ANAC.

Os sistemas de manutenção e registro eletrônico de logs e dados devem incluir os seguintes elementos:

Item Auditado

30) O sistema possui um método para garantir a continuidade dos dados durante a transição de um sistema de legado (cópia) para um novo sistema eletrônico?	**Conforme**	**X**	**Não Conforme**	
Evidências					
Resultados Esperados	Evidências de método para garantir a continuidade dos dados durante a transição de um sistema de legado (cópia) para um novo sistema eletrônico.				
DISPONIBILIDADE PARA FISCALIZAÇÃO					
Todas as informações armazenadas em sistemas informatizados deverão estar disponíveis para fins de fiscalização ou eventual transmissão de dados, na forma e periodicidade definida em normativo específico para cada escopo.					
Item Auditado					
31) As informações estavam disponíveis no momento da solicitação?	**Conforme**	**X**	**Não Conforme**	
Evidências					
Resultados Esperados	Todas as informações armazenadas em sistemas informatizados deverão estar disponíveis para fins de fiscalização ou eventual transmissão de dados, na forma e periodicidade definida em normativo específico para cada escopo.				