Número da Norma Complementar	Revisão	Emissão	Folha
06/IN06/DTI/IFAP	00	18/JUN/18	1/10

INSTITUTO FEDERAL DE EDUCAÇÃO,
CIÊNCIA TECNOLOGIA DO AMAPÁ
Diretoria de Tecnologia da Informação

NORMATIZA O BACKUP, TESTE E RECUPERAÇÃO DE DADOS NO ÂMBITO DO IFAP

Fls. 02
03/08/18

ORIGEM

Diretoria de Tecnologia da Informação
Coordenação de Segurança da Informação

REFERÊNCIA NORMATIVA

Lei n° 7.232, de 29 de outubro de 1984, que dispõe sobre a Politica Nacional de Informática;
Lei n° 8.027, de 12 de abril de 1990, que dispõe sobre as normas de conduta a serem observadas pelos servidores públicos civis da União, das Autarquias e das Fundações Públicas;
Decreto n° 1.048, de 21 de janeiro de 1994, que trata do Sistema de Administração dos Recursos de Informação e Informática da Administração Púbica Federal;
Decreto n° 3.505, de 13 de junho de 2000, que institui a Politica de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
Decreto n° 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos materiais sigilosos de interesse da segurança da sociedade e do Estado no âmbito da Administração Pública Federal;
Norma ABNT NBR ISO n° 17799:2005: Código de Práticas para a Gestão da Segurança da Informação;
Instrução Normativa n° 01 – GSI/PR, de 13 de junho de 2008, que Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.
Instrução Normativa n° 01 – DTI/IFAP, de 26 de fevereiro de 2013, que dispõe sobre as regras e diretrizes de Tecnologia da Informação e Segurança da Informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP.

CAMPO DE APLICAÇÃO

Esta Norma Complementar se aplica no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP.

SUMÁRIO

INSTITUTO FEDERAL DE EDUCAÇÃO,
CIÊNCIA TECNOLOGIA DO AMAPÁ
Diretoria de Tecnologia da Informação

NORMATIZA O BACKUP, TESTE E RECUPERAÇÃO DE DADOS NO ÂMBITO DO IFAP

Fls. 03
03/08/18

INFORMAÇÕES ADICIONAIS
Não há

ÉVERTON DE SOUSA VIEIRA
Coordenador da Coordenadoria de Segurança da Informação
Portaria n° 294/2015/GR/IFAP

APROVAÇÃO

Marco Rogério da Silva Pantoja
Diretor da Diretoria de Tecnologia da Informação
Portaria n° 1063/2016/GR/IFAP

Ciente:

Portaria 2231/2018/GR/IFAP

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA TECNOLOGIA DO AMAPÁ
Diretoria de Tecnologia da Informação

NORMATIZA O BACKUP, TESTE E RECUPERAÇÃO DE DADOS NO ÂMBITO DO IFAP

Fls. 04
03/08/18

1 OBJETIVO

Normatizar e dar publicidade aos procedimentos de backup, testes e recuperação de dados realizados pelo Instituto Federal de Educação, Ciência e Tecnologia do Amapá – IFAP, provendo uma base comum para elaboração de procedimentos para garantir a disponibilidade das informações relevantes as atividades da Instituição.

As normas descritas no decorrer não constituem uma relação exaustiva e podem ser atualizadas a qualquer tempo, sendo verificada a necessidade.

2 CONSIDERAÇÕES INICIAIS

Esta é uma norma complementar à Política de Segurança de Informação e Comunicação (POSIC), a qual foi elaborada pela Diretoria de Tecnologia de Informação – DTI e aprovada/instituída pela resolução nº 15 de 03 de Julho de 2012.

O IFAP adotará ações em consonância com as suas regulamentações, as leis federais, estaduais, municipais e às normas internas, para identificar e estabelecer mecanismos técnicos e procedimentos que garantam a funcionalidade, segurança e robustez do ambiente dos recursos de TIC.

3 FUNDAMENTO LEGAL DA NORMA COMPLEMENTAR

Conforme disposto no inciso II do art. 3º da Instrução Normativa nº 01, de 13 de Junho de 2008, do Gabinete de Segurança Institucional, compete ao Departamento de Segurança da Informação e Comunicações – DSIC, estabelecer normas definindo os requisitos metodológicos para implementação da Gestão de Segurança da Informação e Comunicações pelos órgãos e entidades da Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008.

Norma Técnica ABNT NBR ISO/IEC 27001:2013, que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro da organização.

Norma Técnica ABNT NBR ISO/IEC 27002:2013, que fornece diretrizes para práticas de gestão de segurança da informação

4 CONCEITOS E DEFINIÇÕES

Para os fins desta Norma Complementar devem ser adotadas as seguintes definições:

4.1 Dado: Qualquer elemento identificado em sua forma bruta e que, por si só, não conduz a uma compreensão de um fato ou situação.

4.2 Acesso: permissão, privilégio ou capacidade de ler, registrar, atualizar, gerenciar ou administrar a consulta e/ou a manipulação do acervo de dados e informações do IFAP.

4.3 Dado de uso corporativo ou institucional: todos os dados capturados e utilizados nas operações de serviço e administrativas do IFAP.

4.4 Agente: qualquer pessoa ou conjunto de pessoas autorizadas pelo IFAP para o acesso e/ou tratamento dos dados corporativos: docentes, funcionários, discentes e terceirizados.

4.5 *Backup*: consiste na cópia de dados específicos, por questão de redundância, para que possam ser restaurados no caso de perda dos dados originais.

4.6 *Restore*: Restauração dos backups realizados.

4.7 Retenção: tempo de guarda dos arquivos de backup até que sejam sobrescritos ou apagados do sistema de backup.

4.8 RPO: *Recovery Point Objective*, é o período de tempo máximo durante o qual as alterações feitas aos dados podem ser perdidas com o processo de recuperação de dados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA TECNOLOGIA DO AMAPÁ
Diretoria de Tecnologia da Informação

NORMATIZA O BACKUP, TESTE E RECUPERAÇÃO DE DADOS NO ÂMBITO DO IFAP

Fls. 05
03/08/18

4.7 RTO: *Recovery Time Objective*, é a quantidade de tempo que as operações levam para voltar ao normal, após uma parada.
4.8 GFS: *Grandfather-father-son*, é um esquema de rotacionamento de mídias de backup. Consiste em um método básico que cria três conjuntos de backup, sendo um diário, um semanal e outro mensal. Os backups diários (son) ou "filhos" são rotacionados a cada dia com um semanal (ou pai-*father*) a cada semana.
4.9 Backup Completo (backup full): é uma cópia completa de todos os arquivos "marcados" para backup, independente se os arquivos foram alterados ou não, também chamado de *backup full*. Geralmente é realizado quando é feito o backup de um dado pela primeira vez, ou no início de cada ciclo de backup.
4.10 Backup Diferencial: Consiste em realizar o backup apenas dos arquivos que foram alterados a partir do último backup completo. É executado após o último backup full. Este tipo de backup requer menor capacidade de armazenamento e é mais rápido de ser realizado. Em sua restauração sempre será necessário dois volumes de backup, um completo e o último backup diferencial.
4.11 Backup Incremental: realiza backup apenas dos últimos arquivos alterados a partir do último backup diferencial. Este tipo de backup é mais rápido, porém sua restauração é bem mais complexa, já que será necessário vários volumes, o backup completo e todos os demais incrementais.
4.12 *Snapshot*: ponto de restauração de máquinas virtuais que permite o retorno a um estado anterior.
4.13 *Disaster recovery:* consiste em estratégias e procedimentos que serão realizados para recuperar a infraestrutura e/ou sistemas de TI, que ficaram inoperantes devido a uma falha ou catástrofe, seja ela natural ou provocada.
4.14 TXT: extensão de arquivo para arquivos texto sem formatação.
4.15 XML: eXtensible Markup Language, linguagem recomendada para compartilhamento de informações, capaz de descrever diversos tipos de dados.
4.16 JSON: acrônimo de *JavaScript Object Notation*, formato de padrão aberto que utiliza texto legível a humanos.
4.17 IEC: *International Electrotechnical Commission.*
4.18 ISO: *International Organization for Standardization*.
4.20 NBR: Norma Brasileira, que são regras, diretrizes, características ou orientações sobre determinado material, produto, processo ou serviço, aprovada pela Associação Brasileira de Normas Técnicas - ABNT
4.21 Responsáveis pelos dados: usuário dos serviços de TIC, com autoridade para determinar a restauração de dados antigos de um serviço sobre bases atuais, ou ainda, usuário com autoridade sobre quaisquer arquivos digitais armazenados nos computadores servidores, que venha a requisitar a recuperação dos mesmos.
4.22 Administrador de serviço: administradores de serviços de TIC ofertados ou hospedados pelo IFAP, que também podem requisitar a restauração de backup dos serviços por eles gerenciados em caso de desastre.
4.23 Administrador de backup: são os técnicos responsáveis e qualificados para as tarefas de configuração dos serviços de backup e também da restauração em casos de desastre ou solicitação de responsáveis pelos dados ou administradores de serviço.
4.24 Mídias: Meios difundidos de cópias de segurança incluem CD-ROM, DVD, disco rígido

Fls. 06
03/08/18

externo, fitas magnéticas, flash de memória, entre outros que porventura surjam com o avanço tecnológico.

5 ORIENTAÇÕES GERAIS

5.1 Antes da realização de modificações impactantes nos dados, cópia de segurança total das informações e configurações devem ser feitas, a fim de preservar os dados originais, caso ocorram falhas no processo de modificação.

5.2 As unidades de TIC dos Campi deverão ser responsáveis pelos dados sob sua custódia e executar procedimentos de Backup e Restauração segundo as orientações desta normativa.

5.3 A operacionalização do software, particularidades dos dispositivos de Backup, definição dos arquivos dos diversos Servidores a serem copiados, os locais onde são executadas estas tarefas e demais informações relevantes, deverão estar detalhadas em documento específico de cada unidade de TI (DITI e unidades de TI dos campi), denominado Plano de Backup (Modelo anexo)

5.4 A necessidade de parada nos serviços de Tecnologia da Informação para execução das rotinas de Backup e restauração deve ser observada e programada.

5.5 Cada unidade do IFAP deverá ser responsável por fornecer a infraestrutura e insumos necessários para operacionalização dos procedimentos desta normativa.

5.6 Esta normativa tem como diretrizes:

5.6.1 Assegurar o acesso contínuo às informações definidas por esta política, através de procedimentos para Backup e restauração que observem criteriosamente o modo e a periodicidade de cada cópia dos dados.

5.6.2 Definir e informar aos usuários do IFAP quais tipos de informações são relevantes e pertinentes de salvamento em dispositivos secundários.

5.6.3 Definir os procedimentos formais de solicitação por parte do usuário acerca da restauração de arquivos ou informações eventualmente perdidas.

5.6.4 Definir os procedimentos de armazenamento e descarte da mídia utilizada no processo de Backup, bem como o período de tempo em que essas mídias permanecerão guardadas até serem reutilizadas.

5.6.5 Definir a periodicidade e os procedimentos para realização de testes de restauração e validação dos backups gerados, inclusive gerando evidências, status e documentação, garantindo assim a confiabilidade do backup.

6 PROCEDIMENTOS

6.1 Fazem parte do Esquema de Backup os dados classificados nas seguintes categorias: Banco de dados, sistemas corporativos, servidores físicos, máquinas virtuais, arquivos de usuários, arquivos de configuração de ativos.

6.2 Preferencialmente deve-se optar por procedimentos automatizados para realização dos Backups.

6.3 Não estão incluídos nessa normativa, os serviços armazenados em nuvem (Ex: Todos os serviços do Google, incluindo e-mail e Google Drive).

6.4 Deverá ser mantido um registro diário de acompanhamento da execução do Backup. Esse registro, deve conter, no mínimo, os seguintes requisitos: Informações de periodicidade, tipo de Backup, número da mídia, conteúdo da cópia, data/hora de execução, erros em procedimentos de cópia e local onde deverá ser armazenado o Backup.

6.5 Banco de Dados

Fls. 07
03/08/18

6.5.1 Para a manutenção dos Procedimentos de Backup dos Bancos de Dados deverão ser executadas as seguintes atividades:
6.5.1.1 Identificar a plataforma de hardware, o sistema operacional do servidor, o meio de armazenamento externo disponível para aquele servidor e o software do banco de dados ali instalado.
6.5.1.2 Estimar a quantidade de objetos de banco e sua adequação ao limite de espaço do meio de armazenamento.
6.5.1.3 Estudar a melhor política ou a mais recomendada pelo fabricante do banco de dados e analisar a sua adequação à situação presente.
6.5.1.4 Escrever script de teste para mensurar tempo de execução.
6.5.1.5 Avaliar o melhor horário e períodos de execução do procedimento, seja ele manual ou automático.
6.5.2 É recomendável a exportação dos dados em formato portável, como por exemplo os formatos JSON, XML ou TXT, que possibilitem a leitura dos dados sem a necessidade de aquisição de software específico. Esta medida manterá a interoperabilidade dos dados ao longo do tempo.
6.6 Sistemas Corporativos
6.6.1 O código-fonte dos sistemas corporativos deverá seguir as mesmas orientações dos Arquivos de Usuários. Caso utilizem algum gerenciador de repositório de software, deve-se avaliar a melhor estratégia de acordo com a solução adotada.
6.6.2 Para garantir a continuidade, segurança e evitar mudanças não registradas e autorizadas em sistemas de informação, os acessos aos backups dos códigos-fonte devem ser restritos e controlado.
6.7 Servidores Físicos
6.7.1 O backup dos arquivos dos servidores físicos será realizado nas seguintes condições:
6.7.1.1 Backups dos arquivos de configuração: a cada atualização de segurança realizada ou em caso de alterações sensíveis no sistema, a pedido do responsável.
6.7.1.1.1 No caso de inexistência de software de gerenciamento de configuração, o uso de gerenciadores de versionamento para estes arquivos é uma prática recomendada.
6.7.1.2 O tempo de retenção será até se criar nova demanda por backup, permitindo sempre existir cópia funcional para os dados. Serão mantidas minimamente 02 (duas) instâncias funcionais de backup.
6.7.1.3 O backup do conteúdo dos arquivos de cada servidor seguirá a mesma estratégia dos arquivos de usuários.
6.8 Máquinas Virtuais
6.8.1 As Máquinas Virtuais terão o mesmo tratamento dispensado a máquinas físicas.
6.8.2 O backup das máquinas virtuais como imagem - *"snapshots"* (adequado para fins de *"disaster recovery"*), será feito na seguinte periodicidade:
6.8.2.1 Backups completos: a cada atualização de segurança realizada ou em caso de alterações sensíveis no sistema, a pedido do responsável pelo serviço.
6.9 Arquivos de Usuários
6.9.1 Para que toda e qualquer informação relevante às atividades do IFAP façam parte dessa norma, cabe a cada usuário, o devido arquivamento das informações por ele manipuladas em uma das unidades de armazenamento remoto do servidor de arquivo;
6.9.2 Só poderão ser armazenados nos servidores do IFAP arquivos relacionados a execução

Fls. 08
03/08/18

institucional.

6.9.2.1 É vedado o armazenamento de arquivos particulares ou que não tenham relação com a área atuação profissional do setor.

6.9.3 Os dados armazenados em disco rígido local (estações de trabalho) não são considerados pertinentes de Backup, por se tratar de armazenamento descentralizado, que impossibilitaria o backup diário, ocasionando tráfego de rede excessivo.

6.9.3.1 Estes discos rígidos, portanto, estão passíveis de serem substituídos por outros em caso de pane ou atualização, sem nenhum comunicado prévio ao usuário, uma vez que todas as informações neles contidas são consideradas genéricas e passíveis de descarte.

6.10 Arquivos de Configuração de ativos

6.10.1 Os arquivos de configuração dos ativos de redes seguirão as mesmas orientações destinadas aos arquivos de configuração dos servidores físicos.

6.11 Necessidades especiais de Backup

6.11.1 Qualquer outro dado que necessite de backup e que não esteja contemplado nesta normativa, deverá ser descrito no Plano de backup (ANEXO I).

7 JANELA DE BACKUP

7.1 Consiste no período de tempo adequado e necessário para a realização do backup dos dados.

7.2 A fim de que a disponibilidade dos sistemas não sejam afetadas, e considerando que os sistemas do IFAP tem um funcionamento 24x7, os períodos de realização de backup deverão ser escolhidos com determinado critério.

7.3 A janela de backup deverá ser realizada, preferencialmente, nos período em que os sistemas tiverem menos fluxo, de forma a evitar interferência no seu funcionamento.

7.4 Para que seja evitado ao máximo a perda de informação, deverá ser estabelecida no mínimo duas janelas diárias.

8 NOMENCLATURA DAS MÍDIAS

8.1 As mídias de backup devem obrigatoriamente ser identificadas.

8.2 A identificação deve conter, no mínimo, a data da cópia de segurança da informação e o código da mídia.

8.3 O padrão de nomenclatura das mídias deverá ser especificado no Plano de Backup.

9 RESTAURAÇÃO DOS DADOS

9.1 As solicitações de restauração de arquivos e a interlocução com os administradores de backup, relativas as normas aqui apresentadas, deverão sempre partir do responsável pelos dados ou administrador de serviço, utilizando a central de serviço para registrar tal solicitação.

9.2 Caso uma área não proprietária de uma informação solicite a restauração da mesma, o proprietário da informação deverá ser notificado para ciência e autorização do procedimento.

9.3 O serviço de backup deve ser orientado para a restauração das informações no menor tempo possível, principalmente havendo indisponibilidade de serviços que dependam dessa operação.

9.4 O tempo máximo de restauração dos serviços ofertados e hospedados será definido no Plano de Backup juntamente com os administradores e responsáveis pelos dados.

9.5 Problemas técnicos devidamente justificados pela Equipe de TI responsável pelo Backup poderão atrasar o prazo de restauração e serão devidamente justificados.

9.6 A restauração deverá ocorrer em local diferente do ambiente original, sempre que possível, de modo a evitar falhas no processo.

Fls. 09
03/08/18

9.7 Deverá ser mantido registro de todos os arquivos cuja restauração foi solicitada, juntamente com as informações relativas ao solicitante, nome do arquivo, data da versão restaurada e data e hora da solicitação.
9.8 A restauração dos arquivos de usuários somente será possível nos casos em que o arquivo tenha sido contemplado por esta normativa e de acordo com a estratégia definida no Plano de Backup, ou seja, os arquivos criados e eventualmente apagados ou alterados no período de tempo inferior ao definido no Plano, não serão passíveis de recuperação.

10 TESTES DE VALIDAÇÃO

10.1 Periodicamente deverão ser realizados testes de recuperação de dados nas mídias de backup.
10.1.1 Os testes serão baseados em dados pré-selecionados que garantam a efetividade, eficiência e confiabilidade do procedimento.
10.1.2 A periodicidade da realização dos Testes de Mídias deverá ser definido formalmente pelo proprietário da informação em conjunto com o administrador da Gerência de Backup e deverá está descrita no Plano de Backup.
10.2 Para cada teste de grupo de backup deverão ser registradas no mínimo as seguintes informações: nome, data, responsável, tipo de mídia, resultado, observação.
10.3 O esquema de validação e demais informações relevantes de cada grupo de Backup serão definidas no Plano de Backup.
10.4 Se restaurações de dados forem realizadas em períodos iguais ou menores que os definidos para os testes, a equipe responsável pela execução dos testes poderá, a partir dos resultados obtidos, considerar que tais ações têm validade como teste naquele período.

11 TEMPO DE RETENÇÃO DOS DADOS

11.1 O tempo de retenção de cada tipo de dado deverá ser definido formalmente pelo proprietário da informação em conjunto com o administrador da Gerência de Backup e deverá ser descrito no Plano de Backup.

12 MEIOS DE ARMAZENAMENTO

12.1 Os meios de armazenamento poderão variar entre fita, armazenamento "na nuvem" ou espelhamento em discos remotos.
12.2 É recomendável a utilização de software de backup dedicado para realização dos procedimentos.
12.3 As mídias de backup deverão ser armazenadas com identificação, em ambiente que garanta a sua integridade física e lógica, em conformidade com as especificações do fabricante e em localidade diversa da origem dos dados.
12.4 Transporte das Mídias
12.4.1 Deverão ser consideradas as seguintes diretrizes para o transporte de mídias:
12.4.1.1 As mídias e informações nelas contidas deverão ser protegidas contra o acesso não autorizado, modificação, remoção e danos durante o transporte externo aos limites físicos da organização.
12.4.1.2 As mídias de backup só poderão ser transportadas de forma registrada e controlada, por pessoa formalmente autorizada e em recipiente lacrado.
12.4.1.3 Deverão ser adotados controles para evitar o acesso não autorizado ao conteúdo da mídia, como utilização de recipientes lacrados e lacre explícito de pacotes que revele qualquer tentativa de acesso.

Fls. 10
03/08/18

12.4.1.4 A embalagem deverá ser suficiente para proteger o conteúdo contra dano físico e fatores ambientais que possam reduzir a possibilidade de restauração dos dados, como a exposição ao calor, umidade ou campos eletromagnéticos.

12.5 Descarte das Mídias

12.5.1 As mídias defeituosas ou inservíveis serão encaminhadas para picotamento, incineração, procedimentos de sobrescrita de dados remanescentes (disco rígido) ou outro procedimento que impossibilite a recuperação dos dados por terceiros e devem ter sua data de descarte registrada em controles sempre que possível para se manter uma trilha de auditoria.

12.5.2 As mídias de backup devem ser substituídas no período indicado pelo fabricante ou em casos de erro das mesmas, resguardando os princípios de segurança em relação ao sigilo das informações e descarte de mídias.

13 PLANO DE CONTINGÊNCIA

13.1 Um Plano de Contingência deverá ser definido no caso do não funcionamento do esquema de backup definido nesta Norma.

14 RESPONSABILIDADES

14.1 Compete ao Comitê de Segurança da Informação e Comunicação – CSIC elaborar as diretrizes para os procedimentos de Backup e Restauração da Informação e a fiscalização do cumprimento desta Norma.

14.2 Compete aos Administradores e responsáveis pela gerência de Backup:

14.2.1 Implementar as diretrizes presentes nesta Norma de Backup e Restauração da Informação;

14.2.2 Executar os procedimentos de administração de Backup e Restauração das informações, medindo tempos de execução e quantidade de dados que estão sendo copiados.

14.2.3 No caso de ocorrer falha na execução do procedimento, averiguar a origem e procurar a solução para ocorrência do erro na execução do backup.

14.2.4 Acompanhar o surgimento de novas tecnologias que forneçam velocidades de gravação superior ou novas formas de realização de backup.

14.2.5 Realização de testes periódicos de restauração, no intuito de averiguar os processos de backup e estabelecer melhorias.

14.2.6 Garantir que os mecanismos de proteção física dos dados estejam instalados e operando de forma satisfatória.

14.3 Compete aos responsáveis pelos dados corporativos:

14.4 Zelar pela garantia de que os dados por si manipulados sejam arquivados em uma das unidades de armazenamento remoto dos Computadores Servidores do IFAP, através de procedimentos definidos nesta Norma, para que o dado seja captado e utilizado de forma adequada.

15 DISPOSIÇÕES GERAIS

15.1 A DITI poderá propor alterações a esta norma;

15.2 Os casos omissos serão dirimidos pelo Comitê Gestor de Tecnologia da Informação, junto com o Comitê Gestor de Segurança da Informação;

15.3 Esta norma será divulgada através da internet, intranet ou e-mail institucional. Uma vez que o usuário inicia a utilização dos serviços disponibilizados, o faz porque concorda com esta norma. Desta forma, quando houver qualquer modificação desta, se submete a anuência automática, a menos que se manifeste oficialmente contrário;

16 VIGÊNCIA

INSTITUTO FEDERAL DE EDUCAÇÃO,
CIÊNCIA TECNOLOGIA DO AMAPÁ
Diretoria de Tecnologia da Informação

NORMATIZA O BACKUP, TESTE E RECUPERAÇÃO DE DADOS NO ÂMBITO DO IFAP

Fls. 11
03/08/18

16.1 Esta política entrará em vigor na data de sua publicação, ficando revogadas todas e quaisquer disposições em contrário;

17 ANEXO

INSTITUTO FEDERAL Amapá	INSTRUÇÃO TÉCNICA	Técnico: XXXX	REVISÃO: 01
	TÍTULO: PLANO DE BACKUP		Página: 1/1
	OBJETIVO: Procedimentos a serem adotados para a realização de backup de dados.	Data Criação: X/X/2018	SETOR:

Data da Modificação	Modificações Realizadas	Responsável Técnico

Fls. 12
03/08/18
Rubrica

PLANO DE BACKUP – BANCO DE DADOS

INFORMAÇÕES DE BACKUP

Descrição do esquema:			
Categoria:		Tipo de backup:	
Ferramenta utilizada:		Tipo de agente:	

Localização	Nome VM	S.O.	Endereço IP local	Endereço IP Público	Nome DNS

RESPONSABILIDADES

Serviço/Aplicação	Responsáveis pela gerência de backup

NOMENCLATURA DOS VOLUMES

Serviço/Aplicação	Nome do volume	Local de armazenamento

PERIODICIDADE

Sistema/Aplicação	Backup Full	Backup diferencial	Backup incremental

RETENÇÃO

	Completo	Incremental	Diferencial
			-

TESTE E VALIDAÇÃO

	Validação	Responsável	Periodicidade

Observações:	