MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAZONAS
GABINETE DA REITORIA

PORTARIA Nº 668/GR/IFAM, DE 08 DE MAIO DE 2025.

Institui a Política de Backup e Restauração no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Amazonas (IFAM), conforme Processo nº 23443.007448/2024-26.

A REITORA SUBSTITUTA DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO AMAZONAS – IFAM, no uso de suas atribuições legais e estatutárias que lhe confere a Portaria nº 532/GR/IFAM, de 31/03/2022, publicada no Diário Oficial da União – DOU Nº 63, de 1º/04/2022, Seção 2, pág. 32, **R E S O L V E:**

Art. 1º INSTITUIR a Política de *Backup* e Restauração do IFAM, com o objetivo de garantir a segurança, a disponibilidade e a integridade dos dados institucionais.

CAPÍTULO I
DO PROPÓSITO E ESCOPO

Art. 2º A Política de *Backup* e Restauração de Dados Digitais objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelas unidades de tecnologia da informação (TI) e formalmente definidos como de necessária salvaguarda no Instituto Federal de Educação, Ciência e Tecnologia do Amazonas, para se manter a continuidade do negócio.

Art. 3º A Política de que trata este documento aplica-se a todas as unidades do IFAM que tenham sob sua guarda dados em suporte digital, incluindo dados fora da Instituição armazenados em um serviço de nuvem Pública ou Privada.

Art. 4º A salvaguarda e restauração dos dados digitais do IFAM abrange exclusivamente repositórios institucionais custodiados pelas unidades de TI, armazenados nos centros de processamento de dados.

Parágrafo único. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Art. 5º A salvaguarda dos dados em formato digital pertencentes a serviços de TI do IFAM, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

§ 1º As rotinas de *"backup"* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

§ 2º As rotinas de *"backup"* devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

§ 3º As rotinas de *"backup"* devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

§ 4º O armazenamento de *"backup"*, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um site de *"backup"* em um local remoto ao da sede da organização para armazenar cópias extras dos principais *"backups"*, a exemplo dos *"backupx"* de dados de serviços críticos.

§ 5º Recomenda-se que a infraestrutura de rede de *"backup"* deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

§ 6º Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de *"backup"*.

§ 7º Em situações em que a confidencialidade é importante, as cópias de segurança serão protegidas através de encriptação.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 6º Para os fins desta Política, considera-se:

I - administrador de *"backup"*: responsável pelo planejamento de soluções de *"backup"*, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas;

II - área técnica: unidade responsável pela operação técnica dos ativos e serviços de TI;

III - ativo crítico: equipamento físico, unidade de armazenamento e dados que possuem elevada importância para a continuidade das atividades e serviços e concretização dos objetivos da organização;

IV - *"backup"*: cópia de segurança de dados computacionais, que pode ser utilizada ou consultada após sua restauração, em caso de indisponibilidade, perda ou alteração dos dados originais;

V - *"backup"* completo: modalidade de *"backup"* em que todos os dados a serem salvaguardados são copiados integralmente (cópia de segurança completa) para uma unidade de armazenamento, independentemente de terem sido ou não alterados desde o último *"backup"*;

VI - *"backup"* incremental: modalidade de *"backup"* em que são salvaguardados apenas os dados novos ou modificados desde o último *"backup"* de qualquer modalidade efetuado;

VII - *"backup"* diferencial: modalidade de *"backup"* em que são salvaguardados apenas dados novos ou modificados desde o último *"backup"* completo efetuado;

VIII - criticidade: grau de importância dos dados para a continuidade das atividades e serviços da organização; IX - descarte: eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais;

IX - disponibilidade: garantia de que o dado esteja acessível e utilizável sob demanda de pessoa física ou determinado serviço de TI, órgão ou entidade devidamente autorizados;

X - gestor da informação: agente público formalmente responsável pela operação do serviço ou sistema de TI e pelas informações produzidas em seu processo de trabalho;

XI - imagem de backup: arquivo gerado pela solução de backup, não necessariamente no formato original dos arquivos que contêm os dados salvaguardados;

XII - janela de backup: período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XIII - operador de backup: responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô e gerenciamento de estoque de fitas locais;

XIV - plano de continuidade de negócios (PCN): plano que define as etapas necessárias para recuperação dos processos de negócio logo após uma interrupção, identificando também os gatilhos para invocação, as pessoas a serem envolvidas, as comunicações, etc.

XV - restauração: processo de recuperação e disponibilização de dados salvaguardados em determinada imagem de backup;

XVI - retenção: período de tempo pelo qual os dados devem ser salvaguardados e estar aptos à restauração;

XVII - recovery point objective (RPO): ponto no tempo em que os dados dos serviços de TI devem ser recuperados após uma situação de parada ou perda, correspondendo ao prazo máximo em que se admite perder dados no caso de um incidente;

XVIII - recovery time objective (RTO): tempo estimado para restaurar os dados e tornar os serviços de TI novamente operacionais, correspondendo ao prazo máximo em que se

admite manter os serviços de TI inoperantes até a restauração de seus dados, após um incidente;

XIX - rotina de backup: procedimento utilizado para se realizar um backup;

XX - serviço de TI: sistema de informação ou qualquer solução de tecnologia da informação que armazene informações em formato digital;

XXI - unidade de armazenamento: dispositivo para armazenamento de dados em suporte digital; e

XXII - unidade de armazenamento de backup: unidade de armazenamento com características específicas para retenção de cópia de segurança de dados digitais.

CAPÍTULO III

DOS PADRÕES OPERACIONAIS

Seção I

DOS PRINCÍPIOS GERAIS

Art. 7º A Política de Backup e Restauração de Dados deve ser alinhada com a Política de Segurança da Informação da Instituição.

Art. 8º A Política de Backup e Restauração de Dados Digitais deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 9º As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

Art. 10. As rotinas de backup devem possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

Art. 11. Os serviços de TI críticos do IFAM, formalmente estabelecidos pelo Comitê de Desenvolvimento Institucional (CDI), são: o Portal Institucional, o Sistema Integrado de Gestão Acadêmica e Administrativa (SIG), Plataformas/Sistemas de Seleção, Sistemas de Revistas eletrônicas as pastas compartilhadas em domínio e o Repositório Institucional.

Parágrafo único. Compete ao Comitê de Desenvolvimento Institucional (CDI) deliberar sobre futuras atualizações da relação dos serviços críticos.

Seção II

DAS FERRAMENTAS DE BACKUP

Art. 12. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.

Art. 13. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização.

Parágrafo único. Compete à Diretoria de Gestão de Tecnologia da Informação (DGTI) solicitar, à Administração, com as justificativas pertinentes, as contratações necessárias para manter os ativos sempre atualizados e em quantidade necessária ao atendimento da demanda do IFAM.

Seção III

DA FREQUÊNCIA E RETENÇÃO DOS DADOS

Art. 14. Os backups dos serviços de TI críticos do IFAM devem ser realizados utilizando-se as seguintes frequências temporais:

I - diária;

II - semanal;

III - mensal; e

IV - anual.

Art. 15. Os serviços de TI críticos e não críticos devem ser resguardados sob um padrão mínimo, o qual deve observar uma correlação frequência/retenção de dados.

Parágrafo único. As frequências e retenções dos backups dos serviços de TI serão definidas em norma específica a ser elaborada pela DGTI em conjunto com os gestores das informações.

Art. 16. O backup de serviços de TI não críticos deve ser formalmente solicitado ao administrador de backup pelo responsável técnico pelo serviço de TI.

Art. 17. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenções diferenciadas.

Art. 18. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelos responsáveis técnicos dos serviços de TI, com a anuência prévia e formal dos gestores das informações, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (dados digitais a serem salvaguardados);

II - tipo de backup (completo, incremental, diferencial);

III - frequência temporal de realização do backup (diária, semanal, mensal, anual);

IV - retenção;

V - RPO; e

VI - RTO.

Art. 19. A restauração de dados não será viabilizada em caso de perdas anteriores à conclusão da cópia de segurança. Dados criados ou modificados entre execuções de cópias de segurança subsequentes não serão protegidos por soluções de backup.

Art. 20. A alteração das frequências e tempos de retenção deve ser precedida de solicitação e justificativa formais encaminhadas ao administrador de backup. A aprovação para execução da alteração depende da anuência do gestor da informação.

Seção IV

DO USO DA REDE

Art. 21. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do IFAM, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI da Instituição.

Art. 22. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

Art. 23. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados do IFAM.

Seção V

DAS UNIDADES DE ARMAZENAMENTO DE BACKUPS

Art. 24. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I - a criticidade do dado salvaguardado;

II - o tempo de retenção do dado;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração;

V - o custo de aquisição da unidade de armazenamento de backup; e

VI - a vida útil da unidade de armazenamento de backup.

Art. 25. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 26. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

Art. 27. As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade e temperatura, e com acesso restrito a pessoas autorizadas pelo administrador de backup.

Art. 28. Quando da necessidade de descarte de unidades de armazenamento de backups, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

SEÇÃO VI

DOS TESTES DE BACKUP

Art. 29. Os backups devem ser testados periodicamente, com o objetivo de garantir a sua confiabilidade e a integridade dos dados salvaguardados.

Art. 30. Os testes de restauração dos backups devem ser realizados, por amostragem, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos e tecnológicos disponíveis em cada unidade do IFAM.

Art. 31. A periodicidade, a abrangência, os procedimentos e as rotinas inerentes aos testes de backup serão definidos em norma específica a ser elaborada pela DGTI em conjunto com os gestores das informações.

SEÇÃO VII

DESCARTE DE MÍDIAS

Art. 32. A mídia de backup será retirada e descartada conforme descrito neste documento:

I - A TI garantirá que a mídia não contenha mais imagens de backup ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados;

II - A TI garantirá a destruição física da mídia antes do descarte;

III - O uso de terceiros para descarte e certificação segura de descarte é recomendado; e

IV - Para a formatação é recomendado o uso dos métodos:

a) NIST Clear: O método limpa os dados em todos os locais endereçáveis por meio de técnicas lógicas. Ele é geralmente aplicado por meio de comandos padrão do tipo “Leitura” e “Escrita” no dispositivo de armazenamento;

b) NIST Purge: O método Purge (Purgar) de sanitização de mídia oferece um nível mais alto de segurança para dados confidenciais, tornando a recuperação de dados inviável por meio de tais técnicas como sobrescrita, apagamento de blocos e criptografia; e

c) NIST Destroy: O método Destroy (Destruir) de sanitização de mídia envolve a destruição física da mídia de armazenamento, proporcionando o mais alto nível de proteção de dados para informações altamente sensíveis ou dispositivos irreparáveis.

CAPÍTULO IV

DAS RESPONSABILIDADES

Art. 33. O administrador de backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup, mediante solicitação da DGTI.

§ 1º O administrador e o operador de backup do IFAM, no âmbito da Administração Central, serão formalmente indicados pelo diretor da DGTI, entre os servidores lotados na DGTI.

§ 2º Nas unidades do IFAM, o administrador e o operador de backup serão formalmente designados pelo diretor de unidade ou pelo coordenador da Coordenação de Tecnologia da Informação e Comunicação (CTIC), quando houver.

§ 3º Caso não seja possível a indicação de servidores distintos, o mesmo servidor poderá exercer os papéis de administrador e operador de backup.

Art. 34. São atribuições do administrador de backup:

I - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pelo IFAM;

II - providenciar a criação e manutenção dos backups;

III - configurar as soluções de backup;

IV - manter as unidades de armazenamento de backups preservadas, funcionais e seguras;

V - definir os procedimentos de restauração e neles auxiliar;

VI - verificar diariamente os eventos gerados pela solução de backup, tomando as providências necessárias para remediação de eventuais falhas;

VII - tomar medidas preventivas para evitar falhas;

VIII - reportar imediatamente ao setor a que está subordinado os incidentes ou erros que causem indisponibilidade ou impossibilitem a execução ou restauração de backups;

IX - gerenciar mensagens e registros de auditoria (LOGs) diários dos backups;

X - disponibilizar informações que subsidiem as decisões referentes à gestão de capacidade relacionada aos backups;

XI - propor modificações visando ao aperfeiçoamento da Política de Backup e Restauração de Dados Digitais, objeto desta Política; e

XII - providenciar a execução dos testes de restauração.

Art. 35. São atribuições do operador de backup:

I - restaurar ou recuperar os backups em caso de necessidade;

II - operar e manusear as unidades de armazenamento de backups;

III - informar ao administrador de backup qualquer problema que impossibilite a restauração de um backup. Art. 35. São atribuições das áreas técnicas:

IV - solicitar restaurações de dados, com anuência do gestor da informação;

V - sanar dúvidas técnicas do administrador de backup acerca das informações salvaguardadas;

VI - validar, tecnicamente, o resultado das restaurações eventualmente solicitadas; e

VII - validar, tecnicamente, o resultado dos testes de restauração dos backups.

Art. 36. São atribuições dos gestores da informação:

I - solicitar, formalmente, a salvaguarda das informações geridas e dar anuência à solicitação feita pela área técnica para restauração de dados;

II - validar, negocialmente, o resultado das restaurações eventualmente solicitadas; e

III - validar, negocialmente, o resultado dos testes de restauração dos backups.

Art. 37. A solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações.

Parágrafo único. O operador de backup terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

CAPÍTULO V

DAS DISPOSIÇÕES FINAIS

Art. 38. Esta Política deverá ser amplamente divulgada no IFAM, fazendo-se ainda constar, em destaque, na página da DGTI.

Art. 39. Esta Política poderá ser revisada a qualquer tempo, para fins de eventual atualização, quando identificada a necessidade de alteração em qualquer de seus dispositivos.

Art. 40. A DGTI, os CTICs e os gestores das informações tomarão as providências necessárias para a adequação das rotinas e dos procedimentos de backups definidos nesta Política.

Art. 41. Casos excepcionais não abordados nesta Política serão decididos pelo CDI, com análise da DGTI, e, sendo necessário, pelas unidades de TI ou pelos gestores das informações.

Art. 42. Esta política entra em vigor a partir da data de sua publicação.

Dê-se ciência. Publique-se. Cumpra-se.

Maria Francisca Morais de Lima

Assinado digitalmente por Maria Francisca Morais de Lima
ND: CN=Maria Francisca Morais de Lima, E=gabinete@ifam.edu.br
Razão: Eu estou aprovando este documento
Localização:
Foxit PDF Reader Versão: 12.1.2

Reitora substituta

ANEXO I

REFERÊNCIA LEGAL E BOAS PRÁTICAS

Orientação	Seção
Acórdão 1.109/2021-TCU-Plenário	Em sua integra
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua integra
Decreto Nº 10.046/2019 - Governança no Compartilhamento de Dados (GCD)	Art. 2, XXIII
Decreto Nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER)	Anexo, Item 2.3.4 e 2.3.5
Decreto Nº 9.573/2018 - Política Nacional de Segurança de Infraestruturas Críticas (PNSIC),	Anexo, art.3, Inciso I, II e V;
Decreto Nº 9.637/2018 - Política Nacional de Segurança da Informação (PNSI)	CAPÍTULO I - Art.2, Incisos III e IV CAPÍTULO II - Art.3, Inciso III, IV, VIII XI CAPÍTULO VI - Seção IV – Art.15;
Framework Control Objectives for Information and Related Technology – Cobit, conjunto de boas práticas a serem aplicadas à governança da TI;	v4.1: DS11: Gerenciar Dados v5: DSS01.01, DSS04.08; DSS06.04, DSS04.08, DSS05.06; DSS06.05-06, DSS04.08, DSS001.01; DSS05.02-05; DSS06.03; DSS06.06
Guia do Framework de Privacidade e Segurança da Informação	Controle 11;
Framework Information Technology Infrastructure Library – ITIL, v. 4, conjunto de boas práticas a serem aplicadas na infraestrutura, operação e gerenciamento de serviços de TI	Gestão da Segurança da Informação;
Instrução Normativa 01/GSI/PR	Art.12, Inciso IV, alínea g, h;
Instrução Normativa Nº 03/GSI/PR, de 28 de maio de 2021,	Capítulo IV;
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados,	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50;
Lei Nº 12.527/2011 – Lei de Acesso à Informação (LAI)	Em sua íntegra
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos	A.12.3 Cópias de segurança;
Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;	12.3 Cópias de segurança; e
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

ANEXO II

Mudanças da Versão 2.0

Este anexo tem a finalidade de fornecer os destaques das mudanças inseridas nesta versão do Modelo de Política de Backup.

Primeiramente, ressalta-se que as mudanças inseridas nesta versão, em comparação com a anterior, visam a adequação com o Guia do Framework de Privacidade e Segurança da Informação v1 elaborado e publicado pela SGD em novembro de 2022.

Foram realizadas alterações:

ITEM	ALTERAÇÃO/INCLUSÃO/EXCLUSÃO	DESCRIÇÃO

ANEXO III

1. INTRODUÇÃO

Esse documento contém o Plano de Backup do < *Reitoria/campus XXXX*> do IF__, e tem como objetivo definir os procedimentos que deverão ser seguidos pela < *Setor de TIC da Unidade* > , nas atividades relacionadas aos procedimentos de backup, restauração e testes de dados em conformidade com a Política de Backup e Restauração de Dados Digitais do IF__- PORTARIA REIT/IFFLU N° 1261.

2. OBJETIVO

<Descrever o objetivo deste Plano de Backup para a sua Unidade>.

3. CAMPO DE APLICAÇÃO

Esta rotina se aplica à < *EQUIPE TI do(a) Campus/Reitoria* > e engloba todos os dados custodiados por esta unidade do IF.

4. VIGÊNCIA

A vigência deste plano é de 1 ano a contar da data de sua aprovação.

5. RESPONSABILIDADES

NOME	RESPONSABILIDADE
< Nome completo do Responsável>	Responsável da área de TI do Campus por elaborar o plano de backup de sua unidade.
< Nome completo do Responsável>	Responsável pela operação de backup do campus.

6. RELAÇÃO DE SISTEMAS CRÍTICOS DO *CAMPUS*/REITORIA

6.1. <xxxxxx> ;
6.2. <xxxxxx> .

7. RELAÇÃO DOS SISTEMAS NÃO CRÍTICOS DO *CAMPUS*/REITORIA

7.1. <xxxxxx> ;
7.2. <xxxxxx> .

8. PROCESSO DE BACKUP

O processo de Backup será aplicado com as plataformas e sistemas utilizados por esta Unidade e está estruturado da seguinte forma: **<Caso um dos itens abaixo não se aplique ao IF, as linhas poderão ser excluídas>**

8.1. Banco de Dados

<Descrever a periodicidade, a mídia, quais SGBDs serão utilizados entre outras informações que julgar pertinentes, como por exemplo> .

8.2. Máquinas Virtuais

<Descrever plataformas e tecnologias de virtualização utilizadas; tipo e periodicidade do backup> .

8.3. Sistema Operacional

8.3.1 < Descrever, em tópicos, quais Sistemas Operacionais serão utilizados > .

8.4. Servidores

<Descrever como o backup do ambiente dos Servidores está configurado e qual a frequência temporal de realização desse backup (diária, semanal, mensal); se Off-site ou local; quanto ao firewall, como o backup da configuração é feito, com que frequência temporal> .

8.5. Arquivos de Configuração de ativos

<Descreva onde os arquivos de configuração de cada mudança implementada são salvos> .

8.6. Servidor de Arquivos

8.6.1. <Descreva qual servidor de arquivos utilizado>

8.7. Descreva a mídia de backup a ser utilizada no *Campus*

Realizado <frequência> , obedecendo a seguinte rotina:

8.7.1 <frequência:> <tipo de backup>

8.8. Réplica OFF-Site

Realizada <frequência> , sendo que cada VM tem seu backup realizado <frequência>. No <prazo> seguinte da criação do referido backup, o mesmo é exportado para o storage de backup off-site, obedecendo o seguinte agendamento:

ANEXO IV

JOB_____

1. **ESCOPO/ABRANGÊNCIA**

<quais arquivos de dados ou de sistema, quais bases de dados, quais tabelas, quais pastas/folders>

2. **FREQUÊNCIA DE REALIZAÇÃO**

<diário, semanal, mensal, anual>

3. **TIPO DE CÓPIA A SER REALIZADA**

<completa/full, incremental ou diferencial>

4. **TEMPO DE RETENÇÃO**

<Observar a correlação frequência/retenção de dados declarados na Política>

5. **UNIDADE DE ARMAZENAMENTO**

<Informar mídia de armazenamento em local seguro diferente do local original>

6. **JANELA DE *BACKUP***

<Informar período no qual a execução das cópias de segurança deverá ocorrer preferencialmente>

7. **ESTRATÉGIA DE *BACKUP***

<Detalhar o esquema de realização das cópias de segurança; informar quais tecnologias e equipamentos será utilizado neste esquema; informar a capacidade necessária para os dados a serem copiados/armazenados; informar quando deve ser agendada a geração de *backups*; informar os responsáveis pela execução e acompanhamento>

8. **PERIODICIDADE DE TESTE DE RESTAURAÇÃO**

<Informar período regular de teste de restauração/recuperação (*restore*) das cópias de segurança>

9. **PROCEDIMENTO DE TESTE DE RESTAURAÇÃO**

<Detalhar quais os procedimentos de teste de recuperação/restauração (*restore*) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento>