Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia Baiano
Órgão de Assessoramento - Comitê de Governança Digital

PORTARIA 4/2025 - OA-CGD/IFBAIANO, de 28 de novembro de 2025

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL, no uso de suas atribuições legais previstas no artigo 6º do Regimento Interno do Comitê de Governança Digital, e, considerando:

- o teor do Processo nº 23327.250819.2025-03 e,

- a deliberação dos membros do CGD, em sua 3ª Reunião Extraordinária, realizada em 19.11.2025.

RESOLVE:

Art. 1º Aprovar a Política de Backup e Restore de Dados do IF Baiano, conforme documento anexo.

Art. 2º Esta Portaria entra em vigor nesta data.

Marcelito Trindade Almeida
Presidente

Documento assinado eletronicamente por:

- **Marcelito Trindade Almeida**, **DIRETOR(A) EXECUTIVO(A) - CD3 - RET-DIREX**, em 28/11/2025 09:55:51.

Este documento foi emitido pelo SUAP em 27/11/2025. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 778780
Código de Autenticação: fa1ed355e1

INSTITUTO FEDERAL
Baiano

Política de Backup e Restauração de Dados Digitais

Versão 1.0

2025

Sumário

Política de Backup e Restauração de Dados Digitais

OBJETIVO

Art. 1º A Política de Backup e Restauração de Dados Digitais define diretrizes, critérios, papéis e requisitos essenciais para garantir a segurança, proteção e disponibilidade dos dados digitais custodiados pelos Núcleos de Gestão de Tecnologia da Informação das Unidades Organizacionais do IF Baiano, sendo formalmente definidos como de necessária salvaguarda com o objetivo de garantir à continuidade do negócio, bem como à sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças. O presente documento apresenta a Política de Backup e Restauração de Dados, visando garantir a segurança, integridade e disponibilidade dos dados.

ESCOPO

Art. 2º As diretrizes presentes neste documento devem ser aplicadas em todas as Unidades Organizacionais do IF Baiano que tenham dados sob sua custódia.

Art. 3º A preservação e recuperação dos dados do IF Baiano abarca exclusivamente os sistemas de informações em ambientes de produção e homologados sob a responsabilidade dos Núcleos de TI, armazenados no centro de processamento de dados destas Unidades Organizacionais.

Parágrafo único: Os dados armazenados localmente, nos desktops/notebooks dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, não serão preservados nem recuperados, ficando a responsabilidade pelo armazenamento sob o respectivo usuário/dispositivo.

Art. 4º A preservação dos dados em formato digital pertencentes a serviços de TI do IF Baiano, que estejam sob custódia de 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.

TERMOS E DEFINIÇÕES

Art. 5º Para fins de compreensão dos termos utilizados nesta Política serão adotadas as seguintes definições:

I. **ADMINISTRADORES DE BACKUP:** responsáveis por gerenciar o armazenamento seguro e eficiente dos dados eletrônicos de uma instituição.

II. **AMEAÇAS CIBERNÉTICAS:** um conjunto de riscos que o ambiente digital oferece para usuários e organizações. Elas se referem a situações, mecanismos e ações maliciosas realizadas por hackers em busca de explorar vulnerabilidades de rede, sistemas e dispositivos. O objetivo é comprometer a segurança da informação, obter acesso não autorizado, interromper serviços e causar danos.

III. **ÁREA TÉCNICA**: área responsável pela operação técnica dos ativos e serviços de TI.

IV. **ATIVO CRÍTICO OU ESSENCIAL**: dados, unidade de armazenamento e equipamento físico, que possui elevada importância para a continuidade das atividades, serviços e concretização dos objetivos do IF Baiano;

V. **ATAQUE**: é qualquer esforço intencional para roubar, expor, alterar, desativar ou destruir dados, aplicações ou outros ativos por meio de acesso não autorizado a uma rede, sistema de computador ou dispositivo digital.

VI. **BACKUP OU CÓPIA DE SEGURANÇA**: conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;

VII. **BACKUP COMPLETO:** modalidade de backup no qual todos os dados programados para serem salvaguardados são copiados em sua totalidade (cópia de segurança completa) para uma unidade de armazenamento.

VIII. **BACKUP DIFERENCIAL:** modalidade de backup na qual apenas os dados novos ou modificados desde o último backup completo são copiados;

IX. **BACKUP INCREMENTAL:** modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup são copiados, independentemente da modalidade realizada anteriormente.

X. **COMITÊ DE GOVERNANÇA DIGITAL (CGD):** grupo de pessoas com a responsabilidade de determinar e priorizar as ações de Tecnologia da Informação e Comunicação no IF Baiano;

XI. **CRITICIDADE:** grau de importância dos dados para a continuidade das atividades e serviços do IF Baiano;

XII. **CUSTODIANTE DA INFORMAÇÃO**: qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal, direta e indireta, que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controles de segurança em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação;

XIII. **DIRETORIA DE GESTÃO TECNOLOGIA DA INFORMAÇÃO (DGTI):** órgão executivo que planeja, dirige, avalia e executa as políticas de Tecnologia da Informação em todo o IF Baiano;

XIV. **DISPONIBILIDADE:** propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

XV. **JANELA DE BACKUP:** período durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

XVI. **MÍDIA**: Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos, CDs, fitas e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

XVII. **PLANO DE BACKUP E RESTAURAÇÃO**: documento norteador dos procedimentos necessários à realização do backup e a sua restauração em caso de necessidade;

XVIII. **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;

XIX. **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;

XX. **RESTAURAÇÃO:** processo de recuperação e disponibilização de dados salvaguardados;

XXI. **RESPONSÁVEIS PELOS DADOS:** são pessoas ou um grupo de pessoas, da área de negócio, que manipulam e usam os dados nas suas atividades.

XXII. **RETENÇÃO:** período pelo qual os dados devem ser salvaguardados e aptos à restauração;

XXIII. **ROTINA DE BACKUP:** procedimento utilizado para se realizar um backup;

XXIV. **SISTEMA DE INFORMAÇÃO:** conjunto de elementos materiais ou intelectuais de TI colocados à disposição dos usuários em forma de serviços ou bens;

XXV. **UNIDADE DE ARMAZENAMENTO DE BACKUP:** dispositivo para armazenamento de dados em suporte digital com características específicas para retenção de cópia de segurança de dados digitais;

XXVI. **UNIDADE ORGANIZACIONAL:** refere-se à Reitoria e a cada campi do IF Baiano;

XXVII. **USUÁRIO:** pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, aluno e pessoa da sociedade civil habilitada pela administração para acessar os ativos de informação do IF Baiano.

REFERÊNCIA LEGAL

Orientação	Seção
Acórdão 1.109/2021-TCU-Plenário	Em sua íntegra
Decreto 10.332/2020 - Estratégia de Governo Digital 2020-2022	Em sua íntegra
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
Portaria GSI/PR nº 93, de 18 de outubro de 2021	Em sua íntegra

DIRETRIZES OPERACIONAIS

Art. 6º As rotinas de backup deverão ser direcionadas para garantir a rápida restauração das informações, especialmente em situações de indisponibilidade dos sistemas essenciais que dependem do processo de recuperação de dados e que sejam considerados críticos para o IF Baiano.

Art. 7º Os sistemas de informação críticos às atividades institucionais do IF Baiano deverão ser formalmente especificados pelo Comitê de Governança Digital (CGD).

Art. 8º As rotinas de backup deverão atender a requisitos mínimos específicos de acordo com o tipo de sistema ou dado salvaguardado, priorizando os sistemas de informações críticos às atividades do IF Baiano.

Art. 9º Deverão ser empregadas soluções de backup e restauração específicas e especializadas para este fim, preferencialmente aquelas capazes de atuar de forma automatizada.

Art. 10 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 do Instituto para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.

Art. 11 Recomenda-se que a infraestrutura de rede de backup deve ser separada, lógica e fisicamente, dos sistemas críticos do IF Baiano.

Art. 12 Deve-se manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração e backup.

Art. 13 Situações em que a confidencialidade é essencial, recomenda-se a proteção das cópias de segurança com encriptação.

Art. 14 A Política de Backup e Restauração de Dados deve estar alinhada à Política de Segurança da Informação do IF Baiano.

Art. 15 A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios.

Art. 16 A solicitação de salvaguarda dos dados relacionados aos sistemas de informações e serviços do IF Baiano deverá ser realizada pelos responsáveis pelos dados, mediante aprovação prévia e formal da gestão. Essa solicitação deve refletir os requisitos de negócio da Unidade Organizacional, assim como os requisitos de segurança da informação e proteção dos dados envolvidos, considerando a criticidade da informação para a continuidade das operações do IF Baiano.

Da frequência e retenção dos dados

Art. 17 As seguintes frequências temporais deverão ser observadas para a realização das cópias de segurança dos serviços de Tecnologia da Informação do IF Baiano.

I – Diária;

II – Semanal;

III – Mensal;

IV – Anual.

Art. 18 Os sistemas de informação essenciais às atividades do IF Baiano deverão ser resguardados, observando os seguintes padrões de frequência e tempo de retenção dos dados:

I – Diária: 1 semana;

II – Semanal: 1 meses;

III – Mensal: 1 ano;

IV – Anual: 5 anos.

Art. 19 Os sistemas de informação não essenciais às atividades do IF Baiano deverão ser resguardados observando os seguintes padrões de frequência e tempo de retenção dos dados:

I - Semanal: 2 mês;

II – Mensal: 1 ano;

III – Anual: 5 anos.

Parágrafo único. Caso seja necessário a realização de backup diário para sistema não essencial a retenção será de 1 (uma) semana.

Art. 20 Poderão ser estabelecidos, para cada sistema de informação, frequência e tempo diferenciado, de acordo com o nível de criticidade, desde que os padrões estabelecidos sejam observados.

Art. 21 Os sistemas de informação abrangidos por esta política deverão ser protegidos observando o padrão de frequência e tempo de retenção, definido em Planos de Backup e Restauração específicos.

Art. 22 As áreas responsáveis por cada dado, em conjunto com o núcleo de TI, deverão formalizar em documento quais dados devem ser protegidos, incluindo a frequência e o período de retenção necessários, a fim de compor os Planos de Backup e Restauração dos sistemas sob sua custódia, conforme o modelo apresentado no Anexo I desta política.

Art. 23 Deverá ser observado pelas áreas responsáveis pelos dados os requisitos regulatórios e legais para determinar a frequência de backup, e o tempo de retenção, a segurança da informação, a proteção dos dados envolvidos e a criticidade da informação para a continuidade da operação do IF Baiano.

Art. 24 O Plano de Backup e Restauração deverá incluir, pelo menos, os seguintes requisitos (vide anexo):

I. Serviço;
II. Escopo (dados a serem salvaguardados);
III. Tipo de *backup* (completo, incremental, diferencial);
IV. Frequência temporal de realização do backup (diária, semanal, mensal, anual);
V. Tempo Retenção;
VI. Unidade de armazenamento;
VII. Janela de backup;
VIII. Estratégia de backup;

IX. Procedimento de teste de restauração;

X. Frequência temporal de teste de restauração;

XI. Procedimento de restauração;

XII. RPO;

XIII. RTO.

Do uso da rede

Art. 25 O desempenho da rede e os possíveis impactos que a execução das rotinas de backup poderão causar aos sistemas computacionais do IF Baiano devem ser considerados para assegurar que o tráfego necessário para esse procedimento não cause a indisponibilidade dos demais sistemas da instituição durante o horário de expediente.

Art. 26 A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.

Art. 27 A Diretoria de Gestão de Tecnologia da Informação (DGTI), em conjunto com a área técnica responsável pela administração da rede, deverá determinar os períodos de janela de backup exclusivos aos sistemas sob sua custódia.

Do transporte e armazenamento

Art. 28 A seleção das unidades de armazenamento deverá considerar as seguintes características dos dados a serem resguardados:

I – A criticidade do dado;

I – O tempo de retenção;

II – A probabilidade de necessidade de restauração;

III – O tempo esperado para restauração;

IV – O custo de aquisição da unidade de armazenamento de backup;

V – A vida útil da unidade de armazenamento de backup.

Art. 29 Deverá ser identificada a possibilidade de utilização de diferentes tecnologias para a realização de cópias de segurança, visando recomendar a melhor solução para cada cenário.

Art. 30 Poderão ser empregadas técnicas de compressão de dados, desde que o acréscimo no tempo de restauração dos dados seja considerado aceitável.

Art. 31 A execução das rotinas de backup deve incluir a previsão do aumento da capacidade dos dispositivos utilizados para armazenamento.

Art. 32 As unidades de armazenamento dos backups devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de backup. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

Art. 33 Os backups devem ser armazenados de forma segura e protegida contra acesso não autorizado e ameaças cibernéticas

Dos testes de backup e restauração

Art. 34 Os backups serão verificados periodicamente:

I. Os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup;
II. Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha;
III. A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta política.
IV. Os testes devem ser realizados em todos os backups produzidos independente do ambiente.

Art. 35 Os testes de restauração dos backups devem ser realizados, por amostragem, semanalmente, em equipamentos servidores diferentes dos que atendem os ambientes de

produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.

Art. 36 Recomenda-se validar se os níveis de serviço pactuados, como o Recovery Time Objective – RTO, foram devidamente atendidos.

Art. 37 Os registros dos teste de restauração deverão incluir, no mínimo, o tipo de sistema/serviço que teve o seu restabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do backup e se o procedimento foi concluído com sucesso.

Art. 38 A recuperação/restauração de dados é um processo crítico que deve ser executado para garantir a continuidade das operações de uma organização após a perda de informações essenciais devido a falhas de software, hardware, erros humanos, ataques cibernéticos ou desastres naturais.

Art. 39 Deverá ser definido um plano de recuperação de dados, documentado e revisado continuamente, incluindo os procedimentos para restaurar backups em caso de falhas ou eventos catastróficos.

Art. 40 No plano de recuperação/restauração de dados deve-se determinar e priorizar a ordem dos sistemas e dados a serem restaurados, com base na importância para o IF Baiano.

Do Descarte da Mídia

Art. 41 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.

Art. 42 Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

Art. 43 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
IV. Para a formatação é recomendado o uso dos métodos:

- **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.
- **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
- **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

Das Responsabilidades

Art. 43 São atribuições dos responsáveis técnicos e gestores das rotinas de backup e restauração de dados do IF Baiano:

I - Elaborar o planejamento dos recursos necessários para a implementação das políticas e planos de backup e restauração;

II - Propor soluções de cópias de segurança das informações produzidas ou armazenadas pelas unidades organizacionais do IF Baiano;

III - Providenciar a criação e manutenção das cópias de segurança;

IV - Configurar as soluções de backup;

V - Manter as unidades de armazenamento de backups funcionais, preservadas e

seguras;

VI - Acionar suporte de terceiros em caso de falha nas unidades de armazenamento;

VII - Elaborar o Plano de Backup e Restauração;

VIII - Monitorar periodicamente os eventos gerados pela solução de backup e tomar as providências necessárias para corrigir possíveis falhas.

IX - Implementar ações preventivas para evitar falhas;

X - Reportar imediatamente os incidentes ou falhas que causem indisponibilidade ou que impeçam a restauração das cópias de segurança;

XI - Gerenciar mensagens e registros de auditoria (LOGs) dos backups;

XII - Providenciar a execução dos testes de restauração;

XIII - Restaurar ou recuperar os backups em caso de necessidade

Disposições Finais

Art. 44 A Política de Backup e Restauração de Dados do IF Baiano deverá ser divulgada.

Art. 45 Esta norma poderá ser revisada a qualquer tempo, quando identificada a necessidade de alteração, não excedendo o período máximo de 2 (dois) anos.

Art. 46 Caberá ao Comitê Gestor de Segurança da Informação esclarecer os casos omissos a esta Norma.

Art. 47 O usuário que fizer uso de forma indevida ou não autorizada dos recursos de tecnologia da informação, bem como agir em desacordo com os termos dessa política, fica sujeito à aplicação das penalidades previstas na Lei 8.112/90 e na legislação pertinente.

Art. 48 Está normativa entra em vigor a partir da data de sua publicação.

ANEXO I

PLANO DE *BACKUP* E RESTAURAÇÃO (MODELO)

1. SERVIÇO

<nome do serviço/sistema>

2. ESCOPO/ABRANGÊNCIA

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

3. FREQUÊNCIA DE REALIZAÇÃO

<diário, semanal, mensal, anual>

4. TIPO DE CÓPIA A SER REALIZADA

<completa/full, incremental ou diferencial>

5. TEMPO DE RETENÇÃO

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

6. UNIDADE DE ARMAZENAMENTO

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

7. JANELA DE *BACKUP*

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

8. 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>

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)>

10. FREQUÊNCIA DE TESTE DE RESTAURAÇÃO

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

11. PROCEDIMENTO DE RESTAURAÇÃO

<Detalhar quais os procedimentos para realizar a recuperação/restauração (restore) das cópias de segurança quando necessário (ou seja, o “como” recuperar os backups)>

12. ASSINATURAS

<Assinatura dos responsáveis pela execução e gestão das rotinas de *backup*>

Cargo/Função:

Data: <dd/mm/aaaa>

Documento Digitalizado Público

Política de Backup e Restauração de Dados Digitais

Assunto: Política de Backup e Restauração de Dados Digitais
Assinado por: Robson Ramos
Tipo do Documento: Plano (externo)
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Robson Cordeiro Ramos**, **DIRETOR(A) - CD3 - RET-DGTI**, em 04/12/2025 14:47:30.

Este documento foi armazenado no SUAP em 04/12/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1213982
Código de Autenticação: ae8eda85d0

Documento Digitalizado Público

Política de Backup e Restore de Dados do IF Baiano_ Portaria nº 04/2025 -CGD

Assunto: Política de Backup e Restore de Dados do IF Baiano_ Portaria nº 04/2025 -CGD
Assinado por: Viviane Menezes
Tipo do Documento: ANEXO
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Viviane Santana Menezes**, **SECRETARIO EXECUTIVO**, em 04/12/2025 15:15:53.

Este documento foi armazenado no SUAP em 04/12/2025. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifbaiano.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1214026
Código de Autenticação: 6445a2ed2b