Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

RESOLUCAO Nº434/2024/CONSUP/IFSULDEMINAS

19 de dezembro de 2024

Dispõe sobre a aprovação da Política de backup e restauração de dados digitais do IFSULDEMINAS.

O Reitor e Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais – IFSULDEMINAS, Professor Cleber Avila Barbosa, nomeado pelo Decreto de 04.08.2022, publicado no DOU de 05.08.2022, seção 2, página 1 e em conformidade com a Lei 11.892/2008, no uso de suas atribuições legais e regimentais, em reunião realizada no dia 18 de dezembro de 2024, **RESOLVE:**

Art. 1º - **Aprovar** a Política de backup e restauração de dados digitais do Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais - IFSULDEMINAS. (Anexo).

Art. 2º - Esta Resolução entra em vigor na data de sua assinatura.

Cleber Avila Barbosa
Presidente do Conselho Superior
IFSULDEMINAS

Documento assinado eletronicamente por:

- **Cleber Avila Barbosa**, **REITOR(A) - CD1 - IFSULDEMINAS**, em 19/12/2024 15:54:32.

Este documento foi emitido pelo SUAP em 19/12/2024. Para comprovar sua autenticidade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsuldeminas.edu.br/autenticar-documento/ e forneça os dados abaixo:

Código Verificador: 511625
Código de Autenticação: ec7585e861

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS DO IFSULDEMINAS

Versão 1.0
Minas Gerais, Dezembro de 2024

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

Histórico de Versões

Data	Versão	Descrição	Autor
18/12/2024	1.0	Política de Backup e Restauração de dados digitais do IFSULDEMINAS	DTI / NTIs

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

Política de Backup e Restauração de Dados Digitais do IFSULDEMINAS

Responsável	Diretoria de Tecnologia da Informação - DTI e Núcleos de Tecnologia da Informação do IFSULDEMINAS.
Aprovado por:	Comitê Gestor de Tecnologia da Informação - CGTI / Comitê de Governança Digital - CGD / Conselho Superior - CONSUP
Localização de armazenamento	Portal DTI. O Anexo lll (Plano de restauração de dados) está acessível somente para interessados.
Data da Aprovação pelo CONSUP	18/12/2024

Capítulo I - Propósito

Art. 1º. 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 pela Diretoria de Tecnologia da Informação do IFSULDEMINAS e Núcleos de Tecnologia da Informação dos campi, formalmente definidos como de necessária salvaguarda no IFSULDEMINAS, para se manter a continuidade do negócio. No sentido de assegurar a missão institucional do IFSULDEMINAS, é fundamental estabelecer mecanismos que permitam a guarda dos dados e 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 Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

Capítulo II - Escopo

Art. 2º. Esta política se aplica a todos os dados digitais armazenados nos centros de processamento de dados (datacenter) mantidos pelas Unidades Provedoras de Solução de TI do IFSULDEMINAS, incluindo dados fora do IFSULDEMINAS armazenados em um serviço de nuvem Pública ou Privada, exceto nos casos onde a Unidade Provedora de Solução de TI não tenha acesso aos mecanismos de backup.

§1º Os dados de sistemas armazenados no datacenter institucional por meio do Termo de uso de serviço em nuvem da DTI não estão no escopo desta política, uma vez que a responsabilidade pelo backup dos dados de tais sistemas é de responsabilidade do solicitante do serviço.

Art. 3º. Dados críticos, neste contexto, incluem arquivos das aplicações, bancos de dados, arquivos de mídia das aplicações, e configurações das máquinas virtuais e equipamentos de rede. A definição de dados críticos e o escopo desta política de backup serão revisados quando houver necessidade.

Art. 4º. Os serviços de TI críticos das unidades do IFSULDEMINAS devem ser formalmente elencados pelas respectivas unidades de TI dos campi, por meio do Anexo II - Plano de backup, e apreciados pelo Comitê Gestor de Tecnologia da Informação e Comitê de Governança Digital do IFSULDEMINAS.

Art. 5º. Já ficam previamente estabelecidos como sistemas e soluções críticos, os sistemas e soluções elencados no Anexo II (Plano de backup do IFSULDEMINAS).

Art. 6º. Esta política se aplica a agentes públicos que podem ser criadores e/ou usuários de tais dados. A política também se aplica a terceiros que acessam e usam, no IFSULDEMINAS, sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do IFSULDEMINAS.

Art. 7º. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados (datacenter) mantidos pelas Unidades Provedoras de Solução de TI, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Art. 8º. A salvaguarda dos dados em formato digital, pertencentes a serviços de TI do IFSULDEMINAS, 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. Em caso de serviços hospedados por outras entidades, públicas ou privadas, onde não há o serviço de backup especificado em contrato, a Unidade Provedora do Serviço deve responsabilizar-se pelo backup conforme acordado no Anexo II (Plano de backup).

Capítulo III - Termos e Definições

Art. 9º A política de backup e restauração de dados do IFSULDEMINAS utilizará as seguintes definições:

- BACKUP OU CÓPIA DE SEGURANÇA - Conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada;
- 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;
- ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;
- MÍDIA - Mecanismos em que dados podem ser armazenados. Além da forma e da tecnologia utilizada para a comunicação - inclui discos ópticos, magnéticos e papel, entre outros. Um recurso multimídia combina sons, imagens e vídeos;

- INFRAESTRUTURA CRÍTICA – instalações, serviços, bens e sistemas, virtuais ou físicos, que se forem incapacitados, destruídos ou tiverem desempenho extremamente degradado, provocarão sério impacto social, econômico, político, internacional ou à segurança;
- UNIDADE GESTORA DE SOLUÇÃO (UGS) - Unidade responsável pela gestão de solução de TI, conforme Política de Governança de Tecnologia da Informação do IFSULDEMINAS (Resolução nº 308/2022);
- UNIDADE PROVEDORA DE SOLUÇÃO (UPS) - Unidade responsável pelo provimento de solução de TI, conforme Política de Governança de Tecnologia da Informação do IFSULDEMINAS (Resolução nº 308/2022);
- *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;
- *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;
- *Backup* do tipo Completo (*full*): cópia de todos os arquivos, independentemente de terem sido modificados ou não.
- *Backup* do tipo Incremental: cópia de todos os arquivos que foram modificados desde o último backup, seja ele completo ou incremental.
- *Backup* do tipo Diferencial: cópia de todos os arquivos que foram modificados desde o último backup completo.

Capítulo IV - Dos Princípios Gerais

Art. 10º A política de backup e restauração de dados do IFSULDEMINAS terá os seguintes princípios gerais:

I. A Política de Backup e Restauração de Dados deve estar alinhada com a Política de Segurança da Informação do IFSULDEMINAS;

II. A Política de Backup e Restauração de Dados deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional;

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

IV. As rotinas de backup devem utilizar soluções mantidas pelas Unidades Provedoras de Solução de TI e especializadas para este fim, preferencialmente de forma automatizada;

V. 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;

VI. O armazenamento de backup pode ser realizado no mesmo local da infraestrutura crítica. É desejável e recomendado que se tenha um sítio de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos;

VII. A infraestrutura de rede de backup, quando possível, deve ser separada, lógica e fisicamente, dos sistemas críticos da organização;

VIII. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup;

IX. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Capítulo V - Da frequência e retenção dos dados

Art. 11º. A política de backup e restauração de dados do IFSULDEMINAS utilizará as diretrizes listadas a seguir para a frequência e retenção de dados:

I. Os backups dos serviços de TI críticos do IFSULDEMINAS devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados e frequências temporais estabelecidas no Plano de Restauração de dados (Anexo lll);
II. Os serviços de TI NÃO críticos do IFSULDEMINAS devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados: backup semanal, retenção de 30 dias;
III. Os serviços de TI em desuso, mantidos somente para consulta de dados, devem ser resguardados sob um padrão mínimo de um (1) backup;
IV. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados;
V. Os ativos envolvidos no processo de backup são considerados ativos críticos para a organização;
VI. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pela Unidade Gestora da Solução, com a anuência prévia e formal da Unidade

Provedora de Solução de TI, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos abaixo e que constam de forma detalhada no Anexo lll (Plano de restauração de dados):

A. Escopo;
B. Tipo de *backup* (completo, incremental, diferencial);
C. Frequência temporal de realização do backup (x horas, diária, semanal);
D. Retenção;
E. RPO;
F. RTO.

VII. A alteração das frequências e tempos de retenção, definidos nesta seção, deve ser precedida de solicitação e justificativas formais da Unidade Gestora da solução, encaminhadas à Unidade Provedora de Solução de TI. A aprovação da alteração depende da anuência da Unidade Provedora de Solução de TI;

VIII. As Unidades Gestoras dos sistemas críticos e não críticos deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e as Unidades Provedoras de Solução de TI responsáveis pelo backup deverão zelar pelo cumprimento das diretrizes estabelecidas.

Capítulo VI - Do uso da rede

Art. 12º. O coordenador da Unidade Provedora de Solução de TI responsável pelo backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do IFSULDEMINAS, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI do IFSULDEMINAS;

Art. 13º. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup;

Art. 14º. O período de janela de backup deve ser determinado pelo coordenador da Unidade Provedora de Solução de TI responsável pelo backup.

Capítulo VII - Do transporte e armazenamento

Art. 15º. A política de backup e restauração de dados do IFSULDEMINAS utilizará as diretrizes listadas a seguir para o transporte e armazenamento de dados:

I. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:
   A. A criticidade do dado salvaguardado;
   B. O tempo de retenção do dado;
   C. A probabilidade de necessidade de restauração;
   D. O tempo esperado para restauração;
   E. O custo de aquisição da unidade de armazenamento de backup;
   F. A vida útil da unidade de armazenamento de backup.

II. O coordenador da Unidade Provedora de Solução de TI responsável pelo backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

III. 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.

IV. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

V. No caso de desligamento do usuário (de forma permanente), o backup de seus arquivos em nuvem deverá ser mantido por, no mínimo, 30 dias. Após esse período, os arquivos poderão ser excluídos a qualquer tempo.

VI. Os centros de processamento de dados (datacenter) das Unidades Provedoras de Solução de TI responsáveis pelo armazenamento dos backups devem ser acondicionados em locais apropriados, com controle de fatores ambientais sensíveis, como temperatura, e com acesso restrito a pessoas autorizadas pelo coordenador da Unidade Provedora de Solução de TI responsável pelo backup. Além disso, as condições de temperatura devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

VII. 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.

Capítulo VIII - Dos testes de backup

Art. 16º. Os backups serão verificados periodicamente, seguindo a metodologia apresentada:

I. Diariamente, considerando os dias úteis, 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 Unidade Provedora de Solução de TI responsável pelo backup manterá registros dos backups realizados para demonstrar conformidade com esta política, informando no registro as verificações realizadas, assim como erros encontrados e/ou ações corretivas realizadas. Os registros deverão ser realizados em canal específico da ferramenta de comunicação da Unidade Provedora de TI, ou ainda em planilha específica.
IV. Os registros das verificações de logs devem ser realizados nos backups de serviços críticos listados no Anexo II (Plano de backup).
V. Os procedimentos técnicos para a verificação de backups deverão ser tratados em Instrução técnica específica a ser elaborada pela Unidade Provedora de Solução de TI.

Art. 17º. Os testes de restauração de dados (backups) serão realizados e verificados periodicamente, seguindo a metodologia apresentada:

I. Os testes de restauração dos backups devem ser realizados, por amostragem, semestralmente, em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observando os recursos humanos de TI e tecnologias disponíveis, a fim de verificar backups bem-sucedidos.
II. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
III. Os registros deverão conter, 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. Os registros deverão ser realizados em canal específico da ferramenta de comunicação da Unidade Provedora de TI, ou ainda em planilha específica.
IV. Os procedimentos técnicos para os testes de restauração de backup deverão ser tratados em Instrução técnica específica a ser elaborada pela Unidade Provedora de Solução de TI.

Capítulo IX - Procedimento de restauração de backup

Art. 18º. O atendimento de solicitações de restauração de backup de dados deverá obedecer às seguintes orientações:

I. A solicitação de restauração de backup deverá partir da Unidade Gestora da solução responsável pelo sistema, através de abertura de chamado na Central de serviços do SUAP. Em caso de incidente, a Unidade Provedora de Solução de TI deverá comunicar à Unidade Gestora de Solução de TI e o dirigente máximo da unidade, e proceder com a restauração de backup, sem a necessidade de anuência da Unidade Gestora de solução de TI. Em caso de identificação de perda de dados, dentro do RPO estabelecido, a Unidade Provedora de Solução de TI deverá comunicar à Unidade Gestora de Solução para as devidas providências.
II. A restauração de backups somente será possível nos casos em que este tenha sido atingido pela estratégia de backup.

Art. 19º. O cronograma e diretrizes de restauração de dados:

I. O tempo de restauração, preferencialmente definido em Acordo de Nível de Serviço entre a Unidade Gestora e a Unidade Provedora de Solução de TI, é proporcional ao volume de dados necessários para a restauração. Os tempos de restauração de dados dos ativos de TI constam no Anexo lll (Plano de restauração de dados). Esta estimativa é do tempo de atendimento da Unidade Provedora de Solução de TI responsável pelo backup, não contemplando o tempo antes ou após o pedido à equipe, e considerando um cenário de normalidade sem catástrofes naturais ou falhas que danifiquem e impeçam o uso de equipamento necessário para o backup.
II. Os backups serão restaurados observando a prioridade para restauração de acordo com a criticidade de cada um.

Capítulo X - Do descarte de mídia

Art. 20º. A mídia de backup será retirada e descartada conforme descrito neste documento:

I. A Unidade Provedora de Solução de TI responsável pelo backup 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 Unidade Provedora de Solução de TI responsável pelo backup garantirá a destruição física da mídia antes do descarte.
III. O uso de terceiros para descarte com certificação segura de descarte é recomendado desde que o dispositivo já esteja destruído e que possa inviabilizar qualquer recuperação de dados.
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
    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 XI - Das Responsabilidades

Art. 21º. O coordenador da Unidade Provedora de Solução de TI responsável pelo backup e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

Art. 22º. O coordenador da Unidade Provedora de Solução de TI, juntamente com o operador responsável pelo backup, tem como atribuições:

I. Propor soluções de cópia de segurança das informações digitais institucionais produzidas ou custodiadas pela sua unidade do IFSULDEMINAS;
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;

Art. 23º. O coordenador da Unidade Provedora de Solução de TI poderá propor às Unidades Gestoras de solução de TI, por meio de notificação, otimizações nos sistemas, sempre visando o bom funcionamento dos backups. Caso a Unidade Gestora de Solução de TI não atenda as proposições da notificação, o backup poderá ser desativado, e a Unidade Gestora notificada sobre tal desativação.

Art. 24º Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

Art. 25º O Dirigente máximo de cada unidade do IFSULDEMINAS é o responsável por priorizar investimentos em equipamentos que garantam a conformidade desta Política de backup e restauração de dados digitais.

Art. 26º. Todos os usuários de serviços e soluções de TI do IFSULDEMINAS deverão declarar ciência do conhecimento e entendimento da Política de backup e restauração de dados do IFSULDEMINAS através de consentimento no sistema de identificação institucional Sou IFSULDEMINAS.

Art. 27º. Quaisquer exceções a esta política devem ser tratadas pela Unidade Provedora de Solução de TI responsável pelo backup.

Art. 28º. As Unidades Provedoras de Solução de TI terão o tempo de doze meses para total implementação da Política de Backup e Restauração de dados digitais do IFSULDEMINAS, a partir da data de sua publicação.

Referência legal e de boas práticas

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

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

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

Ministério da Educação
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Sul de Minas Gerais
IFSULDEMINAS

ANEXO I - Histórico de alterações

Este anexo tem a finalidade de fornecer o histórico de alterações realizadas na Política de Backup e Restauração de dados digitais do IFSULDEMINAS. Tendo em vista que esta é a primeira versão, não foram inseridas informações de alterações.

ITEM	ALTERAÇÃO/INCLUSÃO/EXCLUSÃO	DESCRIÇÃO

ANEXO II - Plano de backup das unidades do IFSULDEMINAS

Os planos de backup das Unidades provedoras de solução de TI estão disponíveis no drive do CGTI, por meio deste link: https://drive.google.com/drive/folders/1G12f5GTLqYihlaH8nhdWRL_YC1i9YK_2.

ANEXO III - Plano de restauração de dados das unidades do IFSULDEMINAS

O plano de restauração de dados é um documento interno, restrito às Unidades provedoras e Unidades Gestoras de solução de TI, assim como aos demais envolvidos com o negócio. O plano está disponível neste link.

Cópia de documento digital impresso por Iracy Lima (84799498649) em 23/12/2024 10:10.

Documento Digitalizado Público

Minuta da Política de Backup e Restauração de dados digitais do IFSULDEMINAS

Assunto: Minuta da Política de Backup e Restauração de dados digitais do IFSULDEMINAS
Assinado por: Ramon Silva
Tipo do Documento: Documento
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Cópia Simples

Documento assinado eletronicamente por:

- **Ramon Gustavo Teodoro Marques da Silva**, **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO - CD3 - IFSULDEMINAS - DTI**, em 20/12/2024 17:03:21.

Este documento foi armazenado no SUAP em 20/12/2024. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsuldeminas.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 623411
Código de Autenticação: dd0c7ae8ee

Documento Digitalizado Público

RESOLUCAO Nº434/2024/CONSUP/IFSULDEMINAS. com anexo

Assunto: RESOLUCAO Nº434/2024/CONSUP/IFSULDEMINAS. com anexo
Assinado por: Iracy Lima
Tipo do Documento: Resolução
Situação: Finalizado
Nível de Acesso: Público
Tipo do Conferência: Documento Original

Documento assinado eletronicamente por:

- **Iracy Renno Moreira de Lima**, **Iracy Renno Moreira de Lima - 3515 - TÉCNICOS EM SECRETARIADO; TAQUÍGRAFOS E ESTENOTIPISTAS - Augustus Terceirização Ltda (23055018000196)**, em 23/12/2024 10:13:29.

Este documento foi armazenado no SUAP em 23/12/2024. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifsuldeminas.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 623627
Código de Autenticação: 951b862cae