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

# MINUTA- POLÍTICA DE BACKUPS

Estabelece a Política de *Backups* no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Tocantins (IFTO).

## CAPÍTULO I
## DO ESCOPO

Art. 1° A Política de *Backups* tem o objetivo de instituir diretrizes, competências e responsabilidades que visam à segurança, proteção e disponibilidade dos ativos de dados digitais custodiados pela área de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no IFTO, para se manter a continuidade do negócio, em casos de indisponibilidades ou perda por erro humano, ataques, catástrofes naturais ou outras ameaças.

Art. 2° Esta norma se aplica a todos os dados digitais no âmbito do IFTO, incluindo dados fora da instituição armazenados em serviço de nuvem pública ou privada.

§ 1º Dados críticos neste contexto de gestão de *backups* incluem banco de dados, dados e arquivos digitais armazenados na estrutura física do serviço de armazenamento e compartilhamento de arquivos administrado pela área de TI, conteúdo web armazenados nos servidores onde se encontram o Portal Institucional e demais sítios das áreas acadêmicas e administrativas do instituto e dados digitais de demais servidores alocados fisicamente no parque computacional do IFTO.

§ 2º A Equipe de Tratamento e Resposta de Incidentes Cibernéticos deve definir quais recursos, sistemas operacionais, máquinas virtuais, *softwares*, sistemas de informação e serviços de TI terão backups realizados.

§ 3º A salvaguarda dos dados em formato digital pertencentes aos serviços de TI do IFTO, 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 as partes envolvidas.

§ 4º Os procedimentos de gestão de *backup* configurados no sistema de gestão de *backups* administrado pela área de TI não contemplam:

I - dados armazenados nos discos locais das estações de trabalho e dispositivos eletrônicos das áreas de gestão, ensino, pesquisa e extensão; e

II - dados armazenados nos servidores configurados e utilizados pelas áreas finalísticas do IFTO, sem o prévio conhecimento da área de TI.

## CAPÍTULO II
## DOS TERMOS E DEFINIÇÕES

Art. 3° Para fins de compreensão dos termos utilizados nesta Política serão utilizados os seguintes conceitos e definições:

I - administrador de backup: pessoa responsável pela gestão de cópias de segurança de dados, informações, bases de dados, recursos, sistemas e serviços de TI;

II - ameaça: conjunto de fatores externos com o potencial de causar dano para um sistema ou organização;

III - atividade: ação ou conjunto de ações executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;

IV - ativo: tudo que tenha valor para a organização, material ou não;

V - ativos de informação: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;

VI - *backup/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;

VII - banco de dados: coleção de dados inter-relacionados, representando informações sobre um domínio específico. São coleções organizadas de dados que se relacionam, a fim de criar algum sentido (informação) e de dar mais eficiência durante uma consulta ou a geração de informações ou conhecimento;

VIII - comitê de segurança da informação (CSI): grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da administração pública federal;

IX - computação em nuvem: modelo de fornecimento e entrega de tecnologia de informação que permite acesso conveniente e sob demanda a um conjunto de recursos computacionais configuráveis, sendo que tais recursos podem ser provisionados e liberados com mínimo gerenciamento ou interação com o provedor do serviço de nuvem;

X - controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso ao uso de recursos físicos ou computacionais. Via de regra, requer procedimentos de autenticação;

XI - controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estrutura organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal;

XII - controles de segurança: certificado que autoriza uma pessoa natural para o tratamento de informação classificada;

XIII - criptografia: arte de proteção da informação, por meio de sua transformação em um texto cifrado (criptografado), com o uso de uma chave de cifragem e de procedimentos computacionais previamente estabelecidos, a fim de que somente o(s) possuidor(es) da chave de decifragem possa(m) reverter o texto criptografado de volta ao original (texto pleno). A chave de decifragem pode ser igual (criptografia simétrica) ou diferente (criptografia assimétrica) da chave de cifragem;

XIV - CTIR GOV - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, subordinado ao Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República;

XV - descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

XVI - diretriz: descrição que orienta o que deve ser feito e como para se alcançarem os objetivos estabelecidos nas políticas;

XVII - documento: unidade de registro de informações, qualquer que seja o suporte ou o formato;

XVIII - e-mail: sigla de correio eletrônico (*electronic mail*);

XIX - eliminação: exclusão de dado ou conjunto de dados, armazenados em banco de dados, independentemente do procedimento empregado;

XX - equipe de tratamento e resposta a incidentes cibernéticos (ETIR): grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade;

XXI - evento: qualquer mudança de estado que tem importância para a gestão de um item de configuração ou serviço de tecnologia da informação. Em outras palavras, qualquer ocorrência dentro do escopo de tecnologia da informação que tenha relevância para a gestão dos serviços entregues ao cliente;

XXII - evento de segurança: qualquer ocorrência identificada em um sistema, serviço ou rede, que indique uma possível falha da política de segurança, falha das salvaguardas ou mesmo uma situação até então desconhecida, que possa se tornar relevante em termos de segurança;

XXIII - firewall: ferramenta para evitar acesso não autorizado, tanto na origem quanto no destino, a uma ou mais redes. Podem ser implementados por meio de *hardware* ou *software*, ou por meio de ambos. Cada mensagem que entra ou sai da rede passa pelo firewall, que a examina a fim de determinar se atende ou não os critérios de segurança especificados;

XXIV - gestão de continuidade de negócios em segurança da informação: processo que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação, a marca da organização e suas atividades de valor agregado;

XXV - gestão de segurança da informação: processo que visa integrar atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e organizacional, aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação;

XXVI - incidente: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

XXVII - incidente cibernético: ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema;

XXVIII - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XXIX - informação: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XXX - internet: rede global, composta pela interligação de inúmeras redes;

XXXI - medidas de segurança: medidas destinadas a garantir sigilo, inviolabilidade, integridade, autenticidade e disponibilidade da informação classificada em qualquer grau de sigilo;

XXXII - plano de continuidade de negócios em segurança da informação: documentação dos procedimentos e das informações necessárias para que os órgãos ou entidades da administração pública federal mantenham seus ativos de informação críticos e a continuidade de suas atividades críticas em local alternativo, em um nível previamente definido, em caso de incidente;

XXXIII - plano de gestão de incidentes: plano de ação claramente definido e documentado, para ser usado em caso de incidente que basicamente englobe os principais recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;

XXXIV - plano de gestão de riscos em segurança da informação: documentação que compõe o processo de gestão de riscos de segurança da informação, que deve conter, pelo menos, a abrangência da aplicação da gestão de riscos, delimitando seu âmbito de atuação e os ativos de informação que serão objeto de tratamento; a metodologia a ser utilizada que deverá contemplar, no mínimo, critérios de avaliação e de aceitação de riscos; os tipos de riscos; o nível de severidade dos riscos; um modelo do relatório de identificação, análise e avaliação dos riscos de segurança da informação com as orientações necessárias para sua elaboração; e um modelo do relatório de tratamento de riscos de segurança da informação com as orientações necessárias para sua elaboração;

XXXV - política: intenções e diretrizes globais formalmente expressas pela direção;

XXXVI - política de segurança da informação: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação;

XXXVII - prestador de serviço: pessoa envolvida com o desenvolvimento de atividades, de caráter temporário ou eventual, exclusivamente para o interesse do serviço, que poderão receber credencial especial de acesso;

XXXVIII - rede de computadores: conjunto de computadores, interligados por ativos de rede, capazes de trocar informações e de compartilhar recursos, por meio de um sistema de comunicação;

XXXIX - recursos de processamento da informação: qualquer sistema de processamento da informação, serviço ou infraestrutura, ou as instalações físicas que os abriguem;

XL - risco: no sentido amplo, trata-se da possibilidade de ocorrência de um evento que pode impactar o cumprimento dos objetivos. Pode ser mensurado em termos de impacto e de probabilidade;

XLI - risco de segurança da informação: risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XLII - segurança da informação: preservação da confidencialidade, integridade, disponibilidade, adicionalmente outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

XLIII - serviços: meio de fornecimento de valor a clientes, com vistas a entregar os resultados que eles desejam, sem que tenham que arcar com a propriedade de determinados custos e riscos;

XLIV - SI: sigla de segurança da informação;

XLV - sistema de informação: conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos

recursos de tecnologia, informação e comunicações de forma integrada;

XLVI - tecnologia da informação: ativo estratégico que apoia processos de negócios institucionais, mediante a conjugação de recursos, processos e técnicas, utilizados para obter, processar, armazenar, disseminar e fazer uso de informações; e

XLVII - usuário: pessoa física ou jurídica, seja servidor público, estudante ou prestador de serviços, voluntário habilitado pela administração para acessar os ativos de informação do IFTO.

## CAPÍTULO III
## DAS DIRETRIZES GERAIS

Art. 4° As diretrizes gerais constituem os pilares da gestão de *backups* no IFTO, norteando a elaboração de normas internas complementares, planos, procedimentos, ações e controles que garantem que os princípios básicos de gestão de *backups* sejam respeitados:

§ 1º Esta política deve estar alinhada com a Política de Segurança da Informação, aos princípios, diretrizes e legislações pertinentes que regem a administração pública federal, bem como as normas internas do IFTO e gestão de continuidade de negócios em nível organizacional.

§ 2º Regras para criação e restauração de *backups* devem garantir a proteção e a disponibilidade dos recursos, sistemas de informação e serviços de TI no IFTO.

§ 3º Procedimentos de criação e restauração de dados devem estar alinhados com os objetivos de negócios, identificando os dados críticos que precisam ser protegidos e garantir que as estratégias para a realização de cópias de segurança atendam às necessidades do IFTO.

§ 4º Estratégias para a criação de *backups* devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.

§ 5º Quando possível deve-se manter reserva de recursos de infraestrutura tecnológica para realização de testes de restauração de *backups*.

## CAPÍTULO IV
## DA GESTÃO DE BACKUPS

Art. 5° O gerenciamento de *backups* é uma parte crítica da segurança da informação e da continuidade dos negócios e deve ser executado conforme recursos disponibilizados pelo IFTO.

§ 1º A gestão de *backups* deve considerar a recuperação de desastres e incluir planos de contingência/continuidade de negócios em segurança da informação para situações em que a infraestrutura principal esteja inacessível.

§ 2º Um processo de recuperação/restauração de dados deve ser estabelecido, mantido e documentado continuamente.
§ 3º Uma solução automatizada para a gestão de *backups* deve ser implementada e mantida continuamente.

§ 4º Os dados críticos devem ser identificados de forma a orientar as estratégias de criação e restauração de *backups*.

§ 5º Mecanismos de controle de acesso físico ou lógico devem ser implementados para proteger as cópias de segurança.

§ 6º Sempre que possível os *backups* devem criptografados para garantir a confidencialidade dos dados.

§ 7º A salvaguarda dos dados em formato digital pertencentes ao IFTO mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem computacional, deve estar garantida por acordos ou contratos que formalizam a relação entre os envolvidos.

## Seção I
## Do Planejamento

Art. 6° As estratégias de *backups* de dados devem determinar quais dados devem ser protegidos por meio de cópias de segurança. No IFTO foram definidos os seguintes dados a serem protegidos:

I - registros acadêmicos de estudantes;

II - informações e documentos de identificação pessoal de servidores, estudantes, estagiários, voluntários e prestadores de serviços;

III - registros financeiros da instituição;

IV - processos administrativos;

V - documentos administrativos, tais como: políticas, procedimentos, registros de reuniões, contratos, acordos com fornecedores e demais documentos relacionados à gestão administrativa e acadêmica do IFTO;

VI - materiais de ensino e aprendizado como conteúdo didático, planos de aula, livros digitais e qualquer conteúdo criado ou adquirido para fins educacionais devem ser resguardados por cópias de segurança; e

VII - configurações de sistemas de tecnologia como servidores, sistemas de gestão escolar, bancos de dados e quaisquer outras configurações de TI que sejam críticas para as operações.

## Seção II
## Da Criação

Art. 7° A criação de estratégias de *backups* deve garantir que os dados estejam protegidos e possam ser recuperados de maneira confiável quando necessário.

§ 1º Sempre que possível cópias de dados e informações institucionais devem ser realizadas regularmente de forma automatizada, de acordo com um cronograma estabelecido, garantindo assim que os dados mais recentes estejam sempre disponíveis para a recuperação.

§ 2º A segmentação de dados deve ser realizada sempre que possível observando quais dados devem ser armazenados localmente, em nuvem ou outro dispositivo de armazenamento.

§ 3º Ao definir as estratégias de *backup*s deve-se definir o objetivo da cópia de segurança, incluindo a frequência de *backup*, tempo de recuperação (RTO) e ponto de recuperação (RPO).

§ 4º Para a criação de estratégias de *backups*, o administrador de *backups* deve realizar a avaliação de necessidades identificando: dados e sistemas críticos, requisitos de retenção e metas de recuperação de dados.

§ 5º Cópias de segurança integrais dos servidores/máquinas virtuais que hospedam sistemas críticos para o IFTO devem ser realizadas regularmente.

## Seção III
## Da Retenção

Art. 8° A retenção de *backups* deve considerar quanto tempo as cópias de segurança devem ser mantidas antes de serem descartadas.

§ 1º Políticas de retenção de dados devem ser estabelecidas para determinar por quanto tempo os *backups* serão mantidos levando em consideração requisitos regulatórios e legais.

§ 2º O IFTO deve reter várias versões de arquivos de forma a permitir a recuperação total de um sistema, recursos ou serviço de TI, conforme os recursos tecnológicos disponíveis na instituição.

§ 3º Quando possível as estratégias de tempo de retenção devem observar a seguinte recomendação:

I - diária: 7 dias da semana;

II - semanal: 4 últimas semanas;

III - mensal: 12 últimos meses; e

IV - anual: 5 últimos anos.

## Seção IV
## Da Restauração

Art. 9° 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 importantes devido a falhas de *software, hardware*, erros humanos, ataques cibernéticos ou desastres naturais.

§ 1º Servidores da área de TI devem ser treinados para realizar a restauração de dados de forma eficaz e segura.

§ 2º Um plano de recuperação de dados deve ser definido, documentado e revisado continuamente, incluindo os procedimentos para restaurar *backups* em caso de falhas ou eventos catastróficos.

§ 3º Ao elaborar o plano para recuperação/restauração de dados deve-se determinar e priorizar a ordem dos sistemas e dados a serem restaurados, com base na importância para o IFTO.

§ 4º Um ambiente para restauração de dados isolado do ambiente de produção deve ser estabelecido e mantido atualizado.

§ 5º Os procedimentos de restauração de dados devem estar alinhados com a política de segurança da informação e conformidade com a LGPD e planos institucionais.

§ 6º Antes de iniciar a restauração de dados o administrador de *backups* deve verificar a integridade dos *backups* de forma a certificar que os dados não estejam corrompidos e estejam disponíveis para a restauração.

§ 7º Testes regulares de recuperação de dados devem ser realizados para garantir que os *backups* sejam funcionais e que os procedimentos de recuperação sejam eficazes.

§ 8º Todas as etapas do processo de restauração de dados, incluindo datas, horas e detalhes específicos sobre cada ação realizada devem ser documentadas.

## Seção V
## Dos Testes

Art. 10° Os testes de restauração de *backups* devem garantir que em caso de falhas ou perda de dados, os dados possam ser recuperados.

§ 1º Um plano de testes deve ser estabelecido e mantido incluindo todos os detalhes necessários como quais *backups* serão testados, quais sistemas ou dados serão restaurados e qual é o procedimento a ser realizado.

§ 2º Um ambiente deve ser configurado, de forma separada do ambiente de produção, para a execução dos testes evitando-se assim qualquer impacto nos sistemas de produção.

§ 3º Procedimentos de testes de recuperação de dados devem ser estabelecidos e mantidos para garantir que os *backups* sejam eficazes e que a recuperação seja possível quando necessário.

§ 4º Testes de restauração de dados devem ser realizados de forma a ajudar a identificar problemas antes de precisar restaurar dados em uma situação de crise.

§ 5º Os testes devem ser realizados por amostragem em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar *backups* bem-sucedidos.

§ 6º Testes devem levar em consideração as políticas de retenção de dados, para que se saiba quanto tempo os *backups* devem ser mantidos e como eles devem ser excluídos.

§ 7º Sempre que possível os testes devem simular cenários de falhas como exclusões acidentais, corrupção de dados ou ataques de *malware*.

§ 8º Na medida do possível deve-se realizar teste de restauração de sistemas completos em máquinas virtuais ou *hardware* de teste para garantir que os sistemas possam ser reconstruídos com sucesso.

§ 9º Sempre que possível deve-se avaliar o tempo necessário para restaurar os dados e sistemas para determinar se os *backups* podem ser restaurados dentro do período de tempo aceitável.

§ 10º Os resultados dos testes devem ser documentados, incluindo quaisquer problemas encontrados e as etapas tomadas para resolvê-los.

## Seção VI
## Da Auditoria e Conformidade

Art. 11° A auditoria e conformidade de dados devem garantir que a cópia de dados sejam feitos de forma adequada, segura e em conformidade com regulamentos e políticas internas pertinentes.

§ 1º Os procedimentos de *backup* devem ser regularmente auditados para garantir que estejam em conformidade com a legislação vigente.

§ 2º Registros das atividades de *backup*, incluindo datas, horas, tipo de dados copiados e quaisquer ações realizadas durante o processo de *backup* devem ser mantidos continuamente.

§ 3º Verificações regulares de integridade dos *backups* devem ser realizadas para identificar qualquer corrupção de dados ou problemas de armazenamento.

§ 4º Os *backups* devem estar em conformidade com regulamentos de privacidade de dados e segurança da informação.

§ 5º A área de TI deverá manter registros de *backups* e testes de restauração para demonstrar conformidade com esta política.

§ 6º Os registros de *backups* deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do *backup* e se o procedimento foi concluído com sucesso.

§ 7º Sistema de monitoramento da execução dos *backups* deve ser implementado e mantido para acompanhar o status da realização da atividade, permitindo assim a identificação de

problemas e tomar medidas corretivas mais ágeis.

§ 8º Alertas e notificações de falhas na realização de cópias de segurança devem ser configuradas no sistema de gestão de *backup* para que a equipe de TI seja informada imediatamente em caso de falhas ou problemas de integridade dos dados.

## Seção VII
## Do Descarte

Art. 12° O descarte de dados deve ocorrer de forma segura observando os requisitos definidos na legislação pertinente.

§ 1º A equipe responsável pelo descarte de *backups* deverá ser treinada para que estejam cientes dos procedimentos e da importância da eliminação segura do dados.

§ 2º Regras de descarte de *backups* deverão ser revisadas periodicamente para garantir que estejam alinhadas com as necessidades atuais da organização e com as mudanças nas regulamentações de privacidade de dados e segurança da informação.

§ 3º A eliminação de *backups* deverá estar em conformidade com as leis e regulamentos de privacidade de dados e sustentabilidade ambiental.

§ 4º Sempre que possível métodos seguros de descarte deverão ser utilizados como a destruição física de discos rígidos ou mídia de armazenamento, trituradoras de papel, desmagnetização de discos dentro outros.

§ 5º Antes de descartar *backups* deverão ser realizadas cópias de registros importantes, como *logs* de auditoria e documentação de conformidade que podem ser necessários para fins legais ou regulatórios.

§ 6º B*ackups* que contenham dados sensíveis ou confidenciais deverão ser tratados com segurança durante o descarte.

## CAPÍTULO V
## DOS TIPOS DE BACKUP

Art. 13° A seleção dos tipos de *backups* faz parte da definição da estratégia de proteção de dados de uma organização. No IFTO as estratégias de *backup* deverão ser estabelecidas e mantidas conforme os seguintes tipos de *backup*:

I - completo: tipo de *backup* que copia todos os arquivos, pastas ou volumes para destinos estabelecidos como servidores, sistemas ou nuvem computacional;

II - incremental: tipo de *backup* que copia apenas os dados que foram alterados ou adicionados desde o último *backup* completo ou incremental já realizado;

III - diferencial: compara o conteúdo do backup existente com o último evento para gravar somente as alterações realizadas.

Art. 14° A definição da frequência dos *backups* afeta diretamente a capacidade da organização de recuperar dados em caso de perda. Neste sentido, a frequência para a realização dos *backups* deve ser determinada com base nas necessidades específicas do IFTO e no impacto da perda de dados.

§ 1º As estratégias *de backup* devem ser programadas preferencialmente de forma automática em horários de menor ou nenhuma utilização dos recursos, serviços, sistemas e rede computacional.

§ 2º Os *backups* deverão ser realizados conforme as seguintes frequências:

I - diariamente: *backups* de dados, bases de dados e sistemas críticos iniciados a partir das 23 horas;

II - mensalmente: *backups* de bases de dados e sistemas críticos realizados até o último dia do mês a partir das 23 horas;

III - semestralmente: *backups* de máquinas virtuais/servidores e infraestrutura de rede realizados até o último dia do semestre a partir das 23 horas; e

IV - anualmente: *backups* de máquinas virtuais/servidores e infraestrutura de rede realizados até o último dia do ano a partir das 23 horas.

## CAPÍTULO VI
## DA PERIODICIDADE

Art. 15° Os dados críticos, tais como banco de dados, arquivos de dados e sistemas críticos devem ter *backups* realizados considerando as estratégias a seguir:

I - os *backups* diários deverão ser executados de segunda à domingo, a partir das 23 horas, em modo incremental, diferencial e completo, com retenção de 7 dias, conforme disponibilidade de recursos tecnológicos;

II - os *backups* semanais deverão ser executados nos finais de semana, iniciando aos sábados e domingos, em modo completo de acordo com a especificidade de cada serviço ou sistema de informação, conforme disponibilidade de recursos tecnológicos;

III - os *backups* mensais deverão ser executados no último dia do mês, em modo completo, com retenção nos 12 (doze) últimos meses, quando houver recursos disponíveis; e

IV - os *backups* completos anuais deverão ser executados no mês de dezembro, com retenção de 5 últimos anos, quando houver recursos tecnológicos disponíveis.

## CAPÍTULO VII
## DO USO DA REDE

Art. 16° O administrador de *backup* deve considerar o impacto da execução das rotinas de *backup* sobre o desempenho da rede de dados, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI, evitar problemas de desempenho da rede e garantir a integridade dos dados de *backup*.

§ 1º Estratégias de *backups* devem ser desenvolvidas levando em consideração a largura de banda disponível, a frequência dos *backups* e os requisitos de retenção de dados.

§ 2º A execução de rotinas de *backup* devem ser agendadas, preferencialmente, durante períodos de baixo tráfego de rede, fora do horário comercial, para minimizar o impacto no desempenho da rede.

§ 3º Técnicas de compactação e deduplicação para reduzir o volume de dados que precisam ser transferidos pela rede devem ser utilizadas para economizar largura de banda.

§ 4º Criptografia de dados deve ser utilizada para proteger os dados durante a transferência pela rede.

§ 5º Dados críticos devem ser priorizados para *backup* e recuperação mais rápida, se necessário.

§ 6º Ferramentas de monitoramento de rede devem ser implementadas para acompanhar o uso da largura de banda durante a realização dos *backups* com a finalidade de identificar gargalos ou problemas de desempenho.

§ 7º A segmentação da rede deve ser considerada para isolar o tráfego de *backup* de outras atividades da rede e evitar interferências.

§ 8º Testes de carga devem ser realizados para avaliar o impacto dos *backups* na rede e ajustar a programação e as configurações conforme necessário.

## CAPÍTULO VIII
## DO ARMAZENAMENTO

Art. 17° Os *backups* devem ser mantidos em locais isolados dos sistemas de produção para protegê-los contra eventos que afetam os sistemas primários, como ataques de *ransomware*, podendo envolver armazenamento em nuvem computacional, locais físicos separados ou outras estratégias de isolamento.

§ 1º Os *backups* devem ser armazenados de forma segura e protegida contra acesso não autorizado e ameaças cibernéticas.

§ 2º Para prover a redundância de dados e sistemas e atender à continuidade do negócio em caso de desastre, quando possível, o IFTO deve utilizar os seguintes locais para armazenamento de cópias de segurança de dados:

I - local: dados armazenados localmente dentro da Unidade Reitoria, tais como: discos rígidos ou servidores dedicados. Este local oferece rápida recuperação, mas pode estar sujeito a falhas locais, como incêndios, tempestades, inundações ou roubo;

II - nuvem computacional: dados armazenados em servidores remotos em data centers de provedores de serviço ou instituições parceiras. Oferece escalabilidade, redundância e proteção contra desastres locais, mas requer largura de banda para a transferência de dados; e

III - híbrido: combina *backup* local com nuvem computacional para aproveitar as vantagens de ambos os métodos. Oferece recuperação rápida de dados locais e proteção contra desastres na nuvem.

## CAPÍTULO IX
## DOS PROCEDIMENTOS DE BACKUP

Art. 18° Os procedimentos para realização de *backups* e restauração de dados, sempre que possível devem ser automatizados e documentados, seguindo os requisitos de privacidade e segurança da informação. Os procedimentos de *backup* devem ser atualizados sempre que houver:

I - novas aplicações desenvolvidas;

II - novos locais de armazenamento de dados ou arquivos criados/disponibilizados;

III -novos arquivos com relevância para o funcionamento do serviço;

IV - novas instalações/configurações de bancos de dados;

V - novos aplicativos instalados; e

VI - outras informações que necessitem de proteção através de *backups*.

Parágrafo único. Em caso de falha em algum procedimento de *backup* ou impossibilidade da sua execução, o administrador de *backup* deve adotar as providências necessárias para promover a salvaguarda das informações através de outro mecanismo, como por exemplo: nova execução do *backup* em horário comercial ou cópia dos dados para outro servidor.

## CAPÍTULO X
## DOS PLANOS DE BACKUP

Art. 19° O IFTO deve ter planos de *backups* específicos para cada recurso, base de dados, sistema de informação e serviço de TI. Para que os planos de *backup* sejam efetivos deve-se observar minimamente:

I - quais arquivos de dados, diretórios, serviços e sistemas devem ser copiados;

II - quais bases de dados devem ser copiadas;

III - quais arquivos de configuração devem ser copiados;

IV - quais arquivos de *logs* de sistema devem ser copiados;

V - quais procedimentos devem ser executados para a recuperação dos *backups*;

VI - qual a frequência para a realização das cópias de segurança;

VII - qual o tipo de cópia deve ser realizada (completo, diferencial, incremental);

VIII - qual o tempo de retenção de *backups*;

IX - quais requisitos específicos de segurança da informação devem ser considerados;

X - qual o local de armazenamento do *backup*; e

XI - quais procedimentos de testes e recuperação de cópias de segurança devem ser realizados.

## CAPÍTULO XI
## DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Art. 20° A equipe de TI de cada unidade deverá definir os procedimentos relativos a *backup* e restauração de dados de sua unidade. No processo de gerenciamento de *backups* são definidos os seguintes papéis e responsabilidades:

I - responsável pelo setor de TI: servidor com a função de gerenciar a equipe de TI na unidade. Esta pessoa tem as seguintes responsabilidades:

a) definir os procedimentos e orientações complementares necessários à aplicação das disposições estabelecidas nesta política;

b) estabelecer e manter atualizado o plano de gestão de *backups* de sua unidade; e

c) gerenciar a realização de testes periódicos de restauração no intuito de avaliar a efetividade dos processos de *backup* e estabelecer melhorias.

II - administrador de *backup*: servidor da área de TI responsável pela definição, manutenção, testes e auditoria de *backups.* Esta pessoa realiza as tarefas de configuração dos serviços de *backup* e também restaura dados, em casos de desastre ou por solicitação. Tem as seguintes responsabilidades:

a) propor e manter atualizadas as diretrizes e os procedimentos relativos aos serviços de *backup* e restauração de dados;

b) propor soluções de cópia de segurança das informações digitais institucionais produzidas ou custodiadas pelo IFTO;

c) definir modelos de documentos para todo o processo de gestão de *backups*;

d) configurar e manter atualizado o *software* de gerenciamento de *backups*;

e) criar procedimentos relativos aos serviços de *backup e restore*, bem como armazenar as

mídias móveis e assegurar o cumprimento das normas aplicáveis;

f) criar e manter *scripts* (tarefas) de *backup*;

g) manter *backups* dos sistemas que forem formalmente solicitados;

h) criar e testar *scripts* de criação e restauração de dados;

i) fazer o armazenamento do *backup* em local apropriado;

j) verificar periodicamente os relatórios gerados pelo *software* de *backup*;

k) fazer manutenções periódicas dos dispositivos de *backup*;

l) gerenciar mensagens e *logs* diários dos *backups*, fazendo o tratamento dos erros de forma que o procedimento de *backup* tenha sequência e os erros na sua execução sejam eliminados;

m) comunicar ao responsável pelo serviço os erros e ocorrências de anomalias durante os procedimentos de *backup* e restauração de dados;

n) propor modificações visando o aperfeiçoamento da política de *backup*;

o) restaurar os *backups* em caso de necessidade;

p) documentar a geração, teste, armazenamento e recuperação das cópias de segurança corporativa;

q) manter documentação pertinente ao *backup*, incluindo planos de *backup* (nível operacional), planos de testes, registros (*logs*) de execução e monitoramento;

r) realizar e controlar o inventário de *backups*;

s) prever a realização de testes periódicos de restauração, no intuito de averiguar os processos de *backup* e estabelecer melhorias;

t) realização de testes periódicos de restauração em conjunto com o responsável pelo serviço, no intuito de averiguar os processos de *backup* e estabelecer melhorias; e

u) fazer manutenção periódica dos dispositivos de *backup.*

III - responsável pelo serviço: pessoa responsável por definir o que deve constar no *backup* periódico dos dados. Esta pessoa tem as seguintes responsabilidades:

a) definir junto com a área de negócios, os requisitos de *backup* e retenção de dados para o sistema ou serviço que está sendo desenvolvido ou implantado no IFTO;

b) informar ao Administrador de *Backup* a inclusão/alteração/exclusão de procedimentos/rotinas de *backup* do serviço;

c) verificar periodicamente a rotina do serviço, identificando qualquer erro que possa interferir nos procedimentos de *backup*;

d) acompanhar periodicamente juntamente com Administrador de *Backup* o andamento das rotinas de *backup* do serviço, a fim de mitigar quaisquer inconsistências;

e) informar ao Administrador de *Backup* qualquer mudança no serviço, tais como: endereço de servidor, credenciais de acesso, ou qualquer outra alteração que possa interferir na rotina de *backup*;

f) propor modificações visando o aperfeiçoamento desta política;

g) realizar testes de rotinas de *restores* periódicas, em conjunto com o Administrador de *Backup*, para certificar de que o serviço está sendo executado corretamente; e

h) responder formalmente por qualquer dano que a perda de dados do serviço possa oferecer.

IV - Usuário: pessoa que utiliza os recursos, sistemas e serviços disponibilizados pelo IFTO. Esta pessoa tem a seguinte responsabilidade:

a) realizar backup de dados pessoais armazenados em ativos de TI periodicamente ou quando

houver necessidade de formatação do sistema operacional, das informações contidas em computadores sob sua responsabilidade.

## CAPÍTULO XII
## DAS PENALIDADES

Art. 21° Ações que violem esta política serão passíveis de investigação, podendo implicar em penas e sanções legais impostas por meio de medidas administrativas, sem prejuízo das demais medidas cíveis e penais cabíveis.

§ 1º Casos omissos não tratados neste documento serão submetidos, analisados e decididos pelo Comitê de Segurança da Informação.

## CAPÍTULO XIII
## DA APROVAÇÃO E REVISÃO

Art. 22° Esta política bem como os documentos gerados a partir dela deverão ser revisados, aprovados e atualizados em função de alterações na legislação no âmbito da administração pública federal e alterações nas políticas e normas internas do IFTO, ou quando considerada necessária pelo Comitê de Segurança da Informação.

## CAPÍTULO XIV
## DAS DISPOSIÇÕES FINAIS

Art. 23° As regras, procedimentos, medidas e controles para a gestão de *backups* serão detalhadas em normas internas complementares, que detalharão suas particularidades e procedimentos relativos à segurança da informação alinhados às diretrizes emanadas pelo Comitê de Segurança da Informação e aos respectivos planos institucionais e estrutura organizacional do IFTO.

Art. 24° Esta política e suas atualizações, bem como normas internas complementares, devem ser divulgadas amplamente a todos os usuários, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

Art. 25° A alta administração deverá disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução das diretrizes contidas nesta política.

Art. 26° Esta política entra em vigor a partir da data de sua publicação.

---

Documento assinado eletronicamente por **Fabiana Ferreira Cardoso**, **Gestora de Segurança da Informação**, em 11/12/2023, às 23:15, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

---

Documento assinado eletronicamente por **Kleyton Matos Moreira**, **Diretor**, em 13/12/2023, às 17:31, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

---

A autenticidade deste documento pode ser conferida no site http://sei.ifto.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **2197570** e o código CRC **94ADD2F5**.

Avenida Joaquim Teotônio Segurado
Quadra 202 Sul, ACSU-SE 20, Conjunto 1, Lote 8 - Plano Diretor Sul
CEP 77020-450 Palmas - TO
(63) 3229-2200
www.ifto.edu.br - reitoria@ifto.edu.br

**Referência:** Processo nº 23235.004586/2023-28 SEI nº 2197570