Norma Interna de Backup e Restore

Instituto Federal Catarinense

Versão 1.0

Blumenau, 03 de JUNHO de 2024

ÍNDICE

1. Objetivo

A Norma Interna 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 área de Tecnologia da Informação e formalmente definidos como de necessária salvaguarda no IFC, para se manter a continuidade do negócio.

No sentido de assegurar sua missão 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 Norma Interna de Backup e Restauração de Dados Digitais, onde se estabelece o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais, visando garantir a segurança, integridade e disponibilidade, em conformidade com a Política de Segurança da informação e Comunicação – PoSIC.

2. Escopo

1. Esta Norma Interna se aplica a todos os servidores e sistemas on-premise e cloud, gerenciados pelo IFC. O escopo desta Norma Interna de backup será revisado a cada 2 anos.
2. Esta Norma Interna se aplica a todos os sistemas que podem ser criadores e/ou usuários de tais dados. A Norma Interna também se aplica a terceiros que acessam e usam sistemas e equipamentos de TI ou que criam, processam e/ou armazenam dados de propriedade do IFC.
3. Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos centros de processamento de dados mantidos pelas unidades de TI, ficando sob a responsabilidade do indivíduo que usa o(s) dispositivo(s).
4. A salvaguarda dos dados em formato digital pertencentes a serviços de TI do IFC, 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.

3. Termos e Definições

Para os efeitos desta Norma Interna, são estabelecidos os seguintes conceitos e definições:

ADMINISTRADOR DE BACKUP - responsável pelo planejamento de soluções de backup, definição de padrões, configurações e atendimento avançado de resolução de incidentes e problemas

ÁREA TÉCNICA – Área responsável pela operação técnica dos ativos e serviços de TI

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

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;

BACKUP COMPLETO (Full): modalidade de backup na qual os dados são copiados em sua totalidade;

BACKUP DIFERENCIAL - modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados;

BACKUP INCREMENTAL - modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup - seja, diferencial ou incremental - são copiados.

CLIENTES DE BACKUP - todo equipamento servidor no qual é instalado o agente de backup;

CRITICIDADE - grau de importância dos dados para a continuidade das atividades e serviços da organização

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;

DESCARTE - eliminação correta de dados, documentos, unidades de armazenamento e acervos digitais

ELIMINAÇÃO - Exclusão de dado ou conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

FORMATAÇÃO DE BAIXO NÍVEL - tipo de método de limpeza de HD que apaga todos os vestígios de arquivos do disco por meio de ação mecânica

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;

INFRAESTRUTURA PRIMÁRIA – 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;

JANELA DE BACKUP - período de tempo durante o qual cópias de segurança sob execução agendada ou manual poderão ser executadas;

JOB - Rotina de execução do backup.

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;

OPERADOR DE BACKUP - pessoa responsável por procedimentos de atendimento de primeiro nível, acompanhamento de execução de rotinas de backup, realização de restaurações de arquivos de usuários, manutenção de troca de fitas no robô e gerenciamento de estoque de fitas locais;

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

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;

RECUPERAÇÃO DE DESASTRE - estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;

4. Referência legal e de boas práticas quando aplicável

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

5. Declarações da Norma Interna

Dos princípios gerais

1. Esta Norma Interna de Backup e Restauração de Dados deve estar alinhada com as Políticas internas do IFC
2. As rotinas de backup devem ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI.
3. As rotinas de backup devem utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada.
4. 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.
5. O armazenamento de backup, se possível, deve ser realizado em um local distinto da infraestrutura crítica. É desejável que se tenha um site de backup em um local remoto ao da sede da organização para armazenar cópias extras dos principais backups, a exemplo dos backups de dados de serviços críticos.
6. Recomenda-se que a infraestrutura de rede de backup deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.
7. Manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de backup.
8. Em situações em que a confidencialidade é importante, convém que cópias de segurança sejam protegidas através de encriptação.

Da frequência e retenção dos dados

1. Os backups dos serviços de TI do IFC devem ser realizados utilizando-se as seguintes frequências temporais, que estarão definidas no MI – Backup e Restore e Planos de Backup.

   I – Diária;

   II – Semanal;

   III – Mensal;

   IV – Anual.
2. Os ativos envolvidos no processo de backup são considerados ativos primários para a organização.
3. A solicitação de salvaguarda dos dados referentes aos serviços de TI, deve ser realizada pelos responsáveis, com a anuência prévia e formal da gestão, 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:

   I – Escopo (dados digitais a serem salvaguardados);

   II – Tipo de *backup* (completo, incremental, diferencial);

   III – Frequência temporal de realização do backup (diária, semanal, mensal, anual);

   IV – Retenção;

   V – RPO;

VI – RTO.

4. A alteração das frequências e tempos de retenção definidos no MI – Backup e Restore deve ser precedida de solicitação e justificativa formais encaminhadas aos responsáveis pela execução do Backup. A aprovação para execução da alteração depende da anuência do Diretor de Tecnologia da Informação.
5. 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.

Do uso da rede

1. O administrador de backup deve considerar o impacto da execução das rotinas de backup sobre o desempenho da rede de dados do IFC, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI do IFC.
2. A execução do backup deve concentrar-se, preferencialmente, no período de janela de backup.
3. O período de janela de backup deve ser determinado pelo administrador de backup em conjunto com a área técnica responsável pela administração da rede de dados do IFC.

Do transporte e armazenamento

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

   I – A criticidade do dado salvaguardado;
   II – O tempo de retenção do dado;
   III – A probabilidade de necessidade de restauração;
   IV – O tempo esperado para restauração;
   V – O custo de aquisição da unidade de armazenamento de backup;
   VI – A vida útil da unidade de armazenamento de backup.

2. O administrador de backup deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.
3. 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.
4. A execução das rotinas de backup deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.
5. 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.
6. 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.

Dos testes de backup

7. Os backups serão verificados periodicamente:
    a) Quando necessário, os logs de backup serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do backup.
    b) Ações corretivas serão tomadas quando os problemas de backup forem identificados, a fim de reduzir os riscos associados a backups com falha.
    c) A TI manterá registros de backups e testes de restauração para demonstrar conformidade com esta Norma Interna .
    d) Os testes devem ser realizados em todos os backups produzidos independente do ambiente.
8. Os testes de restauração dos backups devem ser realizados, por amostragem semestralmente, em equipamentos 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.
9. Verificar se foi atendido os níveis de serviço pactuados, tais como os Recovery Time Objective – RTOs.
10. 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
11. Quaisquer exceções a esta Norma Interna serão totalmente documentadas e aprovadas pela DTI.
12. Para a execução dos testes de restore, que deve ser semestral, todas as evidências devem ser armazenadas

Do Descarte da Mídia

1. A mídia de backup será retirada e descartada conforme descrito neste documento:
    a. 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.
    b. A TI garantirá a destruição física da mídia antes do descarte.
    c. O uso de terceiros para descarte e certificação segura de descarte é recomendado
    d. 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

1. O administrador de backup, de recursos e o operador de backup devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de backup.

6. Procedimentos

1. Os procedimentos relacionados a esta Norma Interna estão descritos no MI-TI Backup e Restore e os planos de backup nos anexo II e III.
2. A criação do plano de backup, conforme modelo anexos,, fica sob responsabilidade da equipe técnica de TI da unidade e aprovada pela instância superior da coordenação/diretoria.
3. O pedido de restauração de backup deve ser realizado via chamado para a equipe responsável, com autorização da chefia imediata do requerente e da autoridade máxima do campus ou pró-reitor da área.

7. Não conformidade

Em caso de violação desta Norma Interna poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

ANEXO I

Mudanças da Versão 2.0

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

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

Foram realizadas alterações:

ITEM	ALTERAÇÃO/INCLUSÃO/EXCLUSÃO	DESCRIÇÃO

ANEXO II

DESCRIÇÃO DOS PLANOS DE BACKUP

1. INTRODUÇÃO

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

2. OBJETIVO

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

3. CAMPO DE APLICAÇÃO

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

4. VIGÊNCIA

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

5. RESPONSABILIDADES

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

6. RELAÇÃO DE SISTEMAS

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

8. PROCESSO DE BACKUP

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

8.1. Banco de Dados

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

8.2. Máquinas Virtuais

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

8.3. Sistema Operacional

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

8.4. Servidores

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

8.5. Arquivos de Configuração de ativos

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

8.6. Servidor de Arquivos

8.6.1. <Descreva qual servidor de arquivos utilizado>

8.7. Descreva a mídia de backup a ser utilizada no campus

Realizado <frequência> , obedecendo a seguinte rotina:

8.7.1 <frequência:> <tipo de backup>

8.8. Réplica OFF-Site

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

ANEXO III

PLANO DE *BACKUP* E RESTAURAÇÃO (TEMPLATE)

JOB_____

1. ESCOPO/ABRANGÊNCIA

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

2. FREQUÊNCIA DE REALIZAÇÃO

<diário, semanal, mensal, anual>

3. TIPO DE CÓPIA A SER REALIZADA

<completa/full, incremental ou diferencial>

4. TEMPO DE RETENÇÃO

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

5. UNIDADE DE ARMAZENAMENTO

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

6. JANELA DE *BACKUP*

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

7. ESTRATÉGIA DE *BACKUP*

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

8. PERIODICIDADE DE TESTE DE RESTAURAÇÃO

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

9. PROCEDIMENTO DE TESTE DE RESTAURAÇÃO

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