RESOLUÇÃO Nº 08 DO COMITÊ DE GOVERNANÇA DIGITAL DE 15 DE OUTUBRO DE 2021

Dispõe sobre a Política Backup, Retenção e Restauração de Dados e seus anexos do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina.

O PRESIDENTE DO COMITÊ DE GOVERNANÇA DIGITAL DO INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, no uso das atribuições que lhe foram conferidas pelo Art. 6º, inciso IV e Art. 9º, deste comitê.

RESOLVE:

Art. 1º Publicar a Política Backup, Retenção e Restauração de Dados e seus anexos.

Art. 2º Esta Resolução entra em vigor na data de 01 de dezembro de 2021.

Obs.: Súmula da reunião do CGD disponível em:
https://sigrh.ifsc.edu.br/sigrh/downloadArquivo?idArquivo=2230720&key=74823b18c50d6a3f0cf689a3528b7e30

POLÍTICA DE BACKUP, RETENÇÃO E RESTAURAÇÃO DE DADOS

1 Introdução

O presente documento estabelece uma política de cópia de segurança (*backup*), retenção e restauração (*restore*) dos dados e serviços ofertados e hospedados pela Diretoria de Tecnologia da Informação e Comunicação (DTIC) do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC).

Além da política referida este documento apresenta em seus anexos o detalhamento dos planos de backup, retenção e restauração de dados e do plano de back para os câmpus do IFSC.

2 Glossário

1. Administrador de backup →servidor do quadro da DTIC ou CTIC responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de backup e restore;

2. Backup → cópia de dados de um dispositivo de armazenamento para outro para que possa ser restaurado em caso da perda dos dados originais.

3. Backup incremental →somente os arquivos novos ou modificados desde a última execução do procedimento de backup são copiados.

4. Backup completo → todos os dados são copiados durante o procedimento de backup.

5. Disaster → evento que origina a indisponibilidade de dados (parcial ou completa) ou serviços.

6. Restore → restauração de dados a partir de um backup armazenado.

7. Recovery → retorno ao estado original (anterior ao “disaster”) de dados ou serviços.

8. Retenção → período de tempo em que o conteúdo da mídia de backup deve ser preservado;

9. Snapshot → ponto de restauração de máquinas virtuais que permite o retorno a um estado anterior.

3 Considerações Inicias

1. A abrangência desta política se estende a toda a comunidade do Instituto Federal de Santa Catarina.
2. Esta política bem como seus anexos deverão ser revisados a cada 2 (dois) anos ou quando necessário.
3. Esta política bem como seus anexos deverão ser apreciados pelo Comitê Técnico de TIC e aprovados pelo Comitê de Governança Digital.

4 Orientações Gerais

1. A Realização do backup deverá respeitar as janelas de execução estabelecidas no Plano de Backup;
2. Quando houver mídias ou dispositivos de armazenamento (fitas), estas deverão ser armazenadas em ambiente com estrutura obediente à norma ABNT NBR ISO/IEC 27002:2013, em localidade diversa da origem dos dados (backup “off-site”);
3. Quando o backup for realizado em ambiente on-site deverá ser previsto no Plano de Backup, em atendimento à norma ABNT NBR ISO/IEC 27002:2013, retenção dos dados principais em ambiente remoto (nuvem ou outra localidade da instituição);
4. Quaisquer procedimentos programados nos equipamentos “servidores” e que impliquem riscos ao seu funcionamento ou em quaisquer dispositivos de armazenamento em data center somente deverão ser executados após a realização do backup dos seus dados.
5. A Diretoria de Tecnologia da Informação e Comunicação deverá subsidiar treinamento, certificações e reciclagens bianuais (ou sempre que a tecnologia for substituída) necessárias para o desenvolvimento das atividades dos servidores da Coordenadoria de Infraestrutura de Redes envolvidos nas atividades descritas nesta política através dos

recursos do Fundo de TIC/Capacitações.

5 Papéis e Responsabilidades

No processo de backup/restauração estarão envolvidos os seguintes atores:

1. Administrador de backup
    1. DTIC: em número não inferior a 2 (dois), são técnicos da Coordenadoria de Infraestrutura e Redes (dados hospedados na DTIC);
    2. CTIC: 1 (um) técnico da Coordenadoria de TIC (dados hospedados no Câmpus);

    Estes servidores deverão ser responsáveis e qualificados para as tarefas de configuração dos serviços de backup e também da restauração dos dados em casos de desastre ou solicitação dos responsáveis pelos dados.

É responsabilidade do Administrador de Backup:

1. Propor modificações visando o aperfeiçoamento da política de backup;
2. Criar e manter os backups;
3. Configurar a ferramenta de backup e os clientes;
4. Criar e testar scripts;
5. Criar e manter mídias;
6. Testar o backup e restore;
7. Criar notificações e relatórios;
8. Verificar periodicamente os relatórios gerados pela ferramenta de backup;
9. Restaurar os backups em caso de necessidade; e
10. 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;

6 Estratégia Geral de Backup

1. Serviços e dados que serão incluídos no backup, tendo como prioridade:
    1. Bancos de Dados;

2. Máquinas Virtuais;
3. Servidores de Arquivos;
4. Servidores Web;
5. Arquivos dos Sistemas Operacionais;

2. Formato de backup
    1. O backup será realizado a partir de software proprietário com suporte e atualização (DTIC) ou software livre ou gratuito (Câmpus);
    2. O backup será realizado em disco;
    3. Replicação do backup em nuvem pública (DTIC);

3. Por padrão será adotado o seguinte esquema de realização de backups (exceto se especificada necessidade especial no item 4):
    1. Backups incrementais, realizados diariamente de segunda-feira a sábado;
    2. Backups completos, criados por consolidação através do modelo "backup incremental forever".
    3. Para melhor uso e disponibilidade dos recursos e para zelar pela maior segurança dos dados a DTIC poderá implementar mudanças que deverão ser ratificadas pelo Comitê de Governança Digital.
4. Necessidades especiais de backup
    1. Máquinas Virtuais → O backup das máquinas virtuais como imagem – *snapshots* (adequado para fins de *disaster recovery*), será feito na seguinte periodicidade:
        1. Diários através do modelo de backup incremental forever, com retenção de até 7 dias.
5. Banco de Dados → Preferencialmente os bancos de dados deverão ser exportados no formato de dump onde facilite a importação em outro ambiente.

7 Retenção de Backup

1. Diário: últimos 7 dias (*on-site* – Disco);

2. Mensal: 30 dias (*off-site* - Nuvem);

8 Teste de confiança

1. Os backups mensais deverão ser testados quanto à integridade e recuperabilidade dos objetos, de maneira amostral, no mínimo, duas vezes ao ano.
2. Caso seja detectada falha na realização do backup ou se após a finalização o mesmo estiver incompleto, novo backup deverá ser executado com vistas ao seu armazenamento.
3. Para todos os testes realizados deverá ser gerado um relatório que ficará sob guarda da do CIR.

9 Recuperação de desastre

1. As cópias armazenadas em ambiente remoto serão utilizadas para a Recuperação de Desastres;
2. A geração das cópias de Recuperação de Desastres ocorrerá após a realização do teste do backup mensal (30 dias).

10 Disposições finais

1. A implementação dessa política está sujeita a disponibilidade de recursos financeiros e humanos.
2. Esta política poderá ser complementada por normas e procedimentos específicos.
3. Casos excepcionais ou não previstos serão encaminhados à DTIC.

ANEXO I – PLANO DE BACKUP

A norma ABNT NBR ISO/IEC 27002:2013 fornece diretrizes para gestão de segurança da informação, levando em consideração os ambientes de risco das organizações. A norma foi projetada para ser usada como referência na seleção e implementação de controles de segurança da informação comumente aceitos.

1 Infraestrutura Física

Estrutura física que compõe o *data center* localizado na Reitoria do IFSC e sob o gerenciamento da Diretoria de Tecnologia da Informação e Comunicação.

Servidor Tipo: Blade - Chassis HPE BLc7000				
Marca/Modelo	N° de Lâminas	Processamento	Memória	Sistema Operacional
HPE ProLiant BL465c Gen8 Server Blade	14	02 processadores 2.6GHz - 16 Core	192 GB	Virtualizador ESXi 6.0
HPE ProLiant BL460c Gen9 Server Blade	02	02 processadores 2.20GHz - 48 Core	256 GB	Virtualizador ESXI 6.7

Servidor Tipo: Blade - Chassis HPE Synergy 12000 CTO Frame				
Marca/Modelo	N° de Lâminas	Processamento	Memória	Sistema Operacional
HPE Synergy 480 Gen 10 CTO Compute Module	05	02 processadores 2,1 GHz - 20 Core	768 GB	Virtualizador ESXI 7.

Servidor Tipo: Storage						
Marca Modelo	N° de Discos/ Tipo	N° de Discos/ Tipo	N° de Discos/ Tipo	N° de Discos/ Tipo	N° de Gavetas	Armazenamento Bruto
DELL EMC VNX5300	10x discos 200GB SSD	55x discos 900GB SAS	30x discos 1TB NL-SAS	30x discos 2TB NL-SAS	6	141,5 TB

Servidor Tipo: Storage						
Marca Modelo	N° de Discos/ Tipo	N° de Discos Tipo	N° de Discos Tipo	N° de Discos Tipo	N° de Gavetas	Armazenamento Bruto
HPE 3PAR 8000	4x discos 400 GB SSD	8x discos 3.8 TB SSD	20x discos 1TB FC	48x discos 8TB NL-SAS	1	409 TB

2 Cobertura do Backup

1. Será realizado backup de todos os dados e serviços hospedados no *data center* da Reitoria (DTIC) com prioridade para:
    1. Ambiente Virtual de Aprendizagem (Plataforma Moodle);
    2. Base Dados Postgresql;
    3. Base de Dados Oracle;
    4. Biblioteca Virtual (Plataforma Sophia);
    5. Central Telefônica;
    6. Nuvem Privada (Plataforma ownCloud);
    7. Portal Institucional (Plataforma Liferay);
    8. Portal de Avaliação Docente;
    9. Portal de Ingresso;
    10. Portal de Dados Abertos;
    11. Serviço Fone@RNP;
    12. Servidor de antivírus;
    13. Serviço de Formulário Eletrônico (Limesurvey);
    14. Serviço de periódicos (OJS);
    15. Serviço de Conferência WEB (RNP);
    16. Serviço de Armazenamento de Arquivos (SAMBA/Minerva);

17. Serviços de redes (DNS, DHCP, outros);
18. Servidor de Câmeras;
19. Sistema de Chamados (Plataforma OTRS);
20. Sistema de Eleição (Plataforma Hélios);
21. Sistema Integrado de Gestão (SIPAC, SIGAA, SIGRH, SIGAdmin e SIG Certame).

3 Detalhamento do Plano de Backup

1. **Ferramenta de backup**
    1. Veeam Backup & Replication Enterprise Plus
2. **Monitoramento**
    1. No procedimento de geração das cópias de segurança ocorre o monitoramento e documentação da execução do procedimento, por meio de registros (logs) relativos a todos os itens copiados, a fim de detectar eventuais falhas e assegurar que houve a realização integral das cópias de segurança.
3. **Objetos de backup**
    1. Serão objetos do backup *on-site*:
        1. Todos os sistemas hospedados no *data center* da DTIC;
        2. Servidor de arquivos;
        3. Portal institucional;
        4. Plataforma de EaD (moodle.ifsc.edu.br);
        5. Plataforma de disco virtual;
    2. Serão objetos do backup *off-site*:
        1. Sistema Integrado de Gestão;
        2. Plataforma EaD (moodle.ifsc.edu.br);

3. Portal Institucional;
4. Servidor de arquivos.

4. **Formato de Backup**
    1. Backups incrementais (denominados diários) de segunda-feira a sábado, realizados preferencialmente no contraturno ao turno de funcionamento da instituição, com até sete dias de retenção;
    2. Backups completos são criados por consolidação através do modelo "backup incremental forever", ou sempre que solicitado pelo responsável pelo dado, desde que haja recurso disponível. Dependendo da necessidade do responsável por um determinado serviço ou sistema poderá ser realizado backup completo desde que haja recurso disponível.
5. **Frequência de realização de Backup**
    1. A frequência de realização das cópias de segurança será semanal no modo de cópia completa (full) e diário no modo incremental.
    2. O processo de cópia de segurança completa ocorrerá a cada sábado e as cópias incrementais, diárias, de segunda a sábado.
    3. O procedimento de realização de cópias de segurança acontecerá no intervalo das 22 h de um dia até as 05 h do dia seguinte.

4 Segurança Física e Lógica

1. Acesso físico ao *data center* da Reitoria (DTIC) onde estão armazenadas as cópias de segurança *on-site* se dará por biometria, senha ou aproximação de tags.
    1. A sala do *data center* possui câmera de segurança monitorando o acesso diário no local.
    2. As cópias de segurança quando requererem confidencialidade serão encriptadas utilizando-se a ferramenta de backup Veeam Backup & Replication Enterprise Plus.
2. A ferramenta de backup Veeam Backup & Replication Enterprise Plus emite alertas por

email quando ocorrem falhas na execução das cópias de segurança. Em função disto será realizado anualmente teste de recuperação/restauração (restore) das cópias de segurança, a fim de detectar tempestivamente eventuais falhas lógicas e físicas (nas mídias de armazenamento).

ANEXO II – PLANO DE RETENÇÃO DE BACKUP

A retenção dos dados institucionais obedecerá a capacidade física/lógica da infraestrutura disponibilizada no *data center* da DTIC.

1. **Modos de Retenção**
    1. A retenção dos dados e sistemas/serviços (máquinas virtuais) se dará no modo on-site (dentro do ambiente físico do *data center*) e *off-site* (fora do ambiente físico do *data center*).
2. **Período de Retenção**
    1. O backup *on-site* terá retenção de até 7 dias (DTIC);
    2. O backup *off-site* terá retenção de até 30 dias (DTIC);

- A retenção por 7 dias dependerá da expansão física do servidor de armazenamento;
- A retenção por 30 dias dependerá de contratação de serviço em nuvem;

3. **Versionamento de Backup**
    1. As cópias de segurança guardadas on-site terão até 7 dias de retenção, compreendendo 7 versões;
    2. As cópias de segurança em site remoto terão até 30 dias de retenção, compreendendo apenas 1 versão.

ANEXO III – PLANO DE RESTAURAÇÃO DE BACKUP

A restauração de backup ocorrerá mediante solicitação do responsável pelo dado armazenado dentro do *data center* da DTIC:

- Dados dos sistemas e serviços;
- Dados de pastas setoriais;
- Dados de portais.

A solicitação de restauração será feita através do e-mail suporte.ti@ifsc.edu.br e pelo telefone (48) 3877-9049.

A restauração das informações deverá acontecer no menor tempo possível (RTO - Recovery Time Objective), principalmente havendo indisponibilidade de serviços que dependam da operação de "restore".

- O administrador do backup deverá prover testes que indiquem qual é o menor tempo para restauração de arquivos, pastas, banco de dados, serviços e sistemas.
- O administrador do backup terá o prazo de 360 dias a partir da data de publicação deste plano para informar os tempos mínimos de restauração.

Anualmente será realizado, por amostragem, dois testes de restauração de dados. Esta periodicidade é definida com base nos alertas emitidos pela ferramenta de backup, que identificam algum incidente da realização do backup. Desta forma não se faz necessário um intervalo menor de tempo (semanal ou mensal).

ANEXO IV – PLANO DE BACKUP, RETENÇÃO E RESTAURAÇÃO DE DADOS DOS CÂMPUS

Nos câmpus do IFSC são realizados backups de serviços e sistemas que atendem a necessidades específicas dos mesmos. Em alguns câmpus também é realizado backup de diretórios com arquivos de usuários.

1 BACKUP

1. **Cobertura do Backup**

   Será realizado backup de serviços e sistemas hospedados no data center dos Câmpus com prioridade para:

   1. Ambiente Virtual de Aprendizagem (Plataforma Moodle);
   2. Base Dados;
   3. Central Telefônica;
   4. Portal do Câmpus;
   5. Portal de Ingresso;
   6. Serviço Fone@RNP;
   7. Servidor de antivírus;
   8. Serviço de Armazenamento de Arquivos (SAMBA/Minerva);
   9. Serviços de redes (DNS, DHCP, outros);
   10. Servidor de Câmeras;

2. **Detalhamento do Plano de Backup**

   1. **Ferramenta de backup**

      1. Ferramenta gratuita ou em software livre.

   2. **Monitoramento**

      1. No procedimento de geração das cópias de segurança deverá ocorrer o monitoramento e documentação da execução do procedimento, por meio de registros (logs) relativos a todos os itens copiados, a fim de detectar eventuais

falhas e assegurar que houve a realização integral das cópias de segurança.

3. **Formato de Backup**

    1. Backups incrementais (denominados diários) de segunda-feira a sábado, realizados preferencialmente no contraturno ao turno de funcionamento da instituição, com até sete dias de retenção;

    2. Backups completos uma vez por semana ou sempre que solicitado pelo responsável pelo dado. Dependendo da necessidade do responsável por um determinado serviço ou sistema poderá ser realizado backup completo desde que haja recurso disponível.

4. **Frequência de realização de backup**

    1. A frequência de realização das cópias de segurança será semanal no modo de cópia completa (full) e diário no modo incremental.

    2. O processo de cópia de segurança completa ocorrerá a cada sábado e as cópias incrementais, diárias, de segunda a sábado.

    3. O procedimento de realização de cópias de segurança acontecerá no intervalo das 22 h de um dia até as 05 h do dia seguinte.

3. **Segurança Física e Lógica**

    1. O acesso físico ao *data center* dos câmpus onde estão armazenadas as cópias de segurança *on-site* se dará por biometria, senha ou aproximação de tags.
    2. A sala do *data center* deverá possuir câmera de segurança monitorando o acesso diário no local.
    3. As cópias de segurança quando requererem confidencialidade serão encriptadas;

2 RETENÇÃO

A retenção dos dados institucionais obedecerá a capacidade física/lógica da infraestrutura disponibilizada no *data center* de cada Câmpus.

1. **Modos de Retenção**
    1. A retenção dos dados e sistemas/serviços se dará no modo on-site (dentro do ambiente físico do *data center*).
2. **Período de Retenção**
    1. O backup *on-site* terá retenção de até 7 dias;
3. **Versionamento de backup**
    1. **A**s cópias de segurança guardadas on-site terão até 7 dias de retenção, compreendendo 7 versões;

3 RESTAURAÇÃO

A restauração de backup ocorrerá mediante solicitação do responsável pelo dado armazenado dentro do *data center* dos Câmpus:

- Dados dos sistemas e serviços;
- Dados de pastas setoriais;

A solicitação de restauração será feita através do e-mail suporte.ti.sigla_do_campus@ifsc.edu.br e pelo telefone disponibilizado em cada CTIC.

A restauração das informações deverá acontecer no menor tempo possível (RTO – Recovery Time Objective), principalmente havendo indisponibilidade de serviços que dependam da operação de "restore".

- O administrador do backup deverá prover testes que indiquem qual é o menor tempo para restauração de arquivos, pastas, banco de dados, serviços e sistemas.
- O administrador do backup terá o prazo de 360 dias a partir da data de publicação deste plano para informar os tempos mínimos de restauração.

Anualmente será realizado, por amostragem, dois testes de restauração de dados. Esta periodicidade é definida com base nos alertas emitidos pela ferramenta de backup, que identificam algum incidente da realização do backup. Desta forma não se faz necessário um intervalo menor de tempo (semanal ou mensal).