REGRAS DE BACKUP, RETENÇÃO E RESTAURAÇÃO DE DADOS - NTI UFABC - 2024

Introdução

O presente documento estabelece o planejamento para o processo de backup, retenção e restauração dos dados e serviços ofertados e hospedados pelo Núcleo de Tecnologia da Informação (NTI) da Universidade Federal do ABC (UFABC).

Objetivos

Art. 1º O objetivo deste documento é definir a estratégia de backup para as informações armazenadas digitalmente nos sistemas e bancos de dados sob a gestão do órgão de TI da UFABC. O propósito é estabelecer diretrizes claras para as etapas de cópia, armazenamento e restauração dos dados de backup hospedados no Data Center, com a finalidade de assegurar a segurança, integridade e disponibilidade dessas informações.

Glossário

Art. 2º Para o disposto neste documento considera-se:

I – **Backup Completo (full):** modalidade de backup na qual os dados são copiados em sua totalidade;
II – **Backup Diferencial:** modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup completo são copiados;
III – **Backup Incremental:** modalidade de backup na qual somente os arquivos novos ou modificados desde o último backup - seja ele completo, diferencial ou incremental - são copiados.
IV – **Clientes de backup:** todo equipamento servidor no qual é instalado o agente de backup;
V – **Recuperação de Desastre:** estratégia de recuperação de dados motivada por sinistros de grave amplitude física ou lógica;
VI – **Mídia de backup:** meio físico ou virtual no qual efetivamente armazenam-se os dados de um backup;
VII – **Retenção:** período de tempo em que o conteúdo da mídia de backup deve ser preservado;
VIII – **Objeto:** qualquer dado passível de backup e restauração;
IX – **Tarefa de Backup (Job):** atividade que é executada sob demanda ou de acordo com um agendamento e vincula um ou mais objetos a uma modalidade de backup e um período de retenção.

Aplicação

Art. 3º A abrangência deste procedimento se estende a todos os sistemas gerenciados pelo NTI.

Referências

Art. 4º A presente estratégia tem como referências os seguintes documentos:

I – Posic UFABC - Política de Segurança da Informação e Comunicações - Resolução do CETIC nº 03 de 2018
II – Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;
III – Norma ABNT NBR ISO/IEC 27002:2013 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;
IV – Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais.
V - Lei nº 12.965/2014 - Marco Civil da Internet

Papéis e Responsabilidades

Art. 5º A Divisão de Data Center exercerá o papel de Administrador de Backup, ficando responsável pelos procedimentos relativos aos serviços de backup e restauração.

Art. 6º São atribuições da Divisão de Data Center:

I. Propor modificações visando o aperfeiçoamento do procedimento de backup;
II. Criar e manter as tarefas de backup;
III. Configurar a ferramenta de backup e os clientes;
IV. Criar e manter mídias;
V. Testar o backup e a restauração;
VI. Criar notificações e relatórios;
VII. Verificar periodicamente os relatórios gerados pela ferramenta de backup;
VIII. Restaurar os backups em caso de necessidade;
IX. 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;
X. Fazer manutenções periódicas dos dispositivos de backup;
XI. Fazer o carregamento das mídias necessárias para os backups programados;
XIII. Fazer o armazenamento das mídias de backup em cofre apropriado.

Estratégia Geral de Backup

Art. 7º Apenas os ativos de TIC que estão sob responsabilidade do NTI serão passíveis de inclusão no processo de backup.

I) Não serão feitas cópias de segurança das seguintes informações:

1. Arquivos binários de programas;
2. Arquivos em servidores de terceiros que não tenham relação com a UFABC, seus projetos e atividades;
3. Servidores não hospedados no Data Center
4. Arquivos sem acesso ou modificação por mais de 5 anos

Art. 8º Os procedimentos de backup deverão ser atualizados quando houver:

I – novas aplicações desenvolvidas;
II – novos locais de armazenamento de dados ou arquivos;
III – novas instalações de bancos de dados;
IV – novos aplicativos instalados;
V – outras informações que necessitem de backup deverão ser informadas ao Administrador de Backup, pelo Administrador do recurso/servidor.

Art. 9º Modalidades de cópias de segurança realizadas

I) Quanto a quantidade de dados copiados:

- Incremental -
- Diferenciais -
- Full - Backup completo

II) Quanto a mídia de armazenamento

- Disco
- Fita

I) Quanto ao local dos dados copiados:

- On Premise - Localmente na infraestrutura da UFABC
- Nuvem - Em local externo à UFABC

Art. 10. Retenção do backup em DISCO

II) Independente da criticidade do ativo, o tempo de retenção seguirá da seguinte forma:

Tipo de backup	**Tempo de retenção**
Full	7 dias

Art. 11. Preservação do backup em FITA (Anexo A)

I) De forma geral, o tempo de retenção do backup em fita segue da seguinte forma:

Tipo de backup	Quando	Retenção
Full	Anual	1 à 2 anos
Diferencial	Mensal	1 à 2 anos
Incremental	Diário	1 à 2 anos

Art. 13. Quanto a Rotina de Backup

I) A rotina de backup seguirá de acordo com a criticidade das informações armazenadas no ativo de TI, sendo da seguinte forma:

Criticidade do Ativo	Tipo de Backup	Rotina
Alta	Full	Trimestral
Alta	Diferencial	Semanal
Média	Full	Semestral
Média	Diferencial	Semanal
Baixa	Full	Anual
Baixa	Diferencial	Mensal/Quinzenal

Art. 14. Quanto aos Testes:

I) Os backups dos ativos críticos **deverão ser testados** quanto à integridade e tempo de recuperação dos dados, podendo ser feito nas modalidades:

- Teste paralelo
- Simulação real

Art 15. Anualmente será realizado um **teste de restauração** de dados.

I) Caso seja detectada falha no backup ou se o mesmo estiver incompleto, um novo backup deverá ser executado com vistas ao seu armazenamento.

II) Para todos os testes realizados, um relatório deverá ser gerado e entregue à Coordenação do NTI.

Art. 16. Quaisquer procedimentos programados nos equipamentos que impliquem riscos ao seu funcionamento ou em quaisquer dispositivos de armazenamento do CPD, somente deverão ser executados após a realização do backup dos seus dados.

Art. 17. A guarda do backup deverá ser feita pela equipe de Data Center que deverá observar:

a. quanto à Mídias de backup

Para uso de mídias de armazenamento, serão utilizadas fitas de tecnologia LTO (Linear Tape Open), discos rígidos e discos sólidos.

b. quanto ao local de armazenamento

I) Deverão ser armazenados uma cópia localmente e uma cópia fora da infraestrutura da UFABC, em Nuvem.

II) Os seguintes requisitos deverão ser observados no local onde ficarão armazenadas as mídias:

- Acesso restrito e registrado;
- Monitoramento e vigilância 24h;
- Manter a chave do cofre sempre guardada, devendo ser vigiada e seu acesso controlado

c. Catalogação de fitas

A catalogação das fitas é feita manualmente através de software de gerência de Backup - Tape Library, com apoio de uso de etiquetas que são inseridas manualmente nas fitas.

d. Reuso de fitas

As fitas poderão ser reutilizadas no processo de backup, sempre que necessário.

Art. 18. Quanto ao descarte

I) Se houver mídias de backup a serem descartadas, essas deverão ser destruídas de forma a impedir a sua reutilização ou acesso indevido aos dados por pessoas não autorizadas.

Segurança Física e Lógica

Art. 19. O Acesso físico ao Data Center onde estão armazenadas as cópias de segurança on-site deverá ser por biometria, chave monitorada ou aproximação de tags em cartão.

Art. 20. A sala do Data Center deverá possuir câmera de segurança monitorando o acesso diário no local.

Art. 21. As cópias de segurança, **quando requererem confidencialidade por alguma legislação**, deverão ser encriptadas.

Art. 22. A ferramenta de backup **deverá emitir alertas por e-mail** quando ocorrem falhas na execução das cópias de segurança.

Art. 23. Restauração do backup

I) A restauração das informações deverá ser solicitada via central de serviços de acordo com a aplicação utilizada (e-mail, pasta da rede, site). Em caso de indisponibilidade de acesso à Central de Serviços, a solicitação poderá ser feita pelo e-mail datacenter@ufabc.edu.br

II) 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”.

III) 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.

Art. 24. O documento de “Estratégia de Backup” deverá ser revisado minimamente a cada 2 anos pela divisão de Data Center, ou em caso de mudança de tecnologia ou atualização crítica, devendo ser aprovada pela Coordenação Geral de Gestão de TI da Universidade Federal do ABC

Anexo A - Rotina e Retenção do backup em fita

	VM (máquina virtual)	RPO (ponto de restauro)	Rotina de Backup	Retenção em fita - full | diferencial | incremental
1	webmail (roundcube)	365 dias	1 backup full por ano / diferencial mensal	1 ano
2	imap	6 horas	(Trimestral) 4 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
3	postfix	365 dias	1 backup full por ano / diferencial mensal	1 ano
4	dns master	24 horas	Sem backup - usar playbook	sem backup
5	ns1	24 horas	Sem backup - usar playbook	sem backup
6	openldap	6 horas	(Trimestral) 4 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
7	samba 4	6 horas	(Trimestral) 4 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
8	shiboleth	180 dias	Sem backup em fita - backup em disco	sem backup
9	netel-moodleLB	365 dias	Sem backup em fita - usar playbook	sem backup
10	netel-moodledb	6 horas	(Trimestral) 4 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
11	netel-moodleNFS	6 horas	(Trimestral) 4 backup fulls por ano / Backup Diferencial semanal/ Backup incremental por dia	1 ano
12	sigaa1	180 dias	1 backup full por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
13	sigaa2	180 dias	1 backup fulls por ano / Backup Diferencial	1 ano

			semanal/ Backup incremental diário	
14	postgree-matricula	24 horas	Por demanda	1 ano
15	share	24 horas	(Trimestral) 4 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
16	share novo	24 horas	(Trimestral) 4 backup fulls por ano ou quando houver alteração da pasta/ Backup Diferencial mensal/ Backup incremental diário	1 ano
17	SIG-1	24 horas	1 backup full por ano / Backup Diferencial mensal/ Backup incremental diário	1 ano
18	SIG-BD	24 horas	2 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
19	SIG-LB	180 dias	1 backup full por ano / Backup Diferencial quinzenal	1 ano
20	SIG-Arquivos	24 horas	2 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
21	SIG homolog Processos 177.104.50.6	24 horas	2 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
22	SIG-Arquivos-Processos 177.104.50.93	24 horas	2 backup fulls por ano / Backup Diferencial semanal/ Backup incremental diário	1 ano
23	site-UFABC	24 horas	2 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	1 ano
24	sites-wordpress-php7	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	2 anos
25	sites-wordpress-php5	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	2 anos
26	sites-joomla-php7	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	2 anos

27	sites-joomla-php5	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	2 anos
28	sites	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	2 anos
29	sites-sftp	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	1 ano
30	prof	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	2 anos
31	site-prograd	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diario	2 anos
32	rapsign	48 horas	1 backup full por ano / Backup Diferencial mensal/ Backup incremental diário	1 ano
33	oracle64	48 horas	1 backup full por ano / Backup Diferencial mensal/ Backup incremental diário	1 ano
34	semplanilhas	48 horas	1 backup full por ano / Backup Diferencial mensal/ Backup incremental diário	1 ano
35	levantamento	48 horas	1 backup full por ano / Backup Diferencial mensal/ Backup incremental diário	1 ano
36	backup-scripts (syslog, radius)	24 horas	(Trimestral) 4 backup full por ano / Backup Diferencial semanal/ Backup incremental diário	2 anos