	Política de Backup		
	Código: POL-CRI-009	Subarea: ---	Tempo Execução:
	Estado: APROVADO		Classificação: Publica
	Autor: FernandoLacerdaDeOliveiraReis		
	Revisor: MichelPetersonAndrade		
	Última atualização: 10 Mar 2023		

A Universidade Federal da Bahia (UFBA) dispõe de uma série de informações valiosas e fundamentais para as suas atividades de ensino, pesquisa e extensão. Uma grande parte dessas informações está concentrada nos servidores institucionais, hospedados na Superintendência de Tecnologia da Informação (STI-UFBA).

Os ativos de informação de uma organização, assim como as tecnologias que as suportam, possuem diversas vulnerabilidades, que podem ser exploradas atingindo os requisitos de confidencialidade, integridade e disponibilidade das informações.

Segundo as normas ABNT NBR ISO/IEC 17799:2005 (ISO/IEC 27002) 27001:2006, um dos controles necessários para manter a integridade e disponibilidade da informação e das tecnologias associadas corresponde à realização periódica de cópias de segurança (backup), seguindo uma política de geração de cópias de segurança definida pela organização.

Segundo as mesmas normas citas acima as cópias de segurança das informações devem ser efetuadas e testadas regularmente conforme definição da política de geração de cópias de segurança. Este documento consiste na política referenciada na norma, definindo todos os termos que deverão ser levados em consideração no desenvolvimento e operação dos processos e procedimentos de backup.

1 Diretrizes Gerais

Ficam estabelecidos como diretrizes gerais da Política de Backup da Rede UFBA, os seguintes pontos:

1. Perda das informações instituicionais da universidade sejam revertidas ao seu estado de no máximo 1 (um) dia útil à ocorrência.
2. Garantir a disponibilidade das informações, serviços e sistemas da UFBA, durante as atividades da universidade.
3. Reduzir o tempo de indisponibilidade de sistemas críticos e informações devido a falhas ou desastres.
4. As mídias de cópias de segurança sejam verificadas e testadas regularmente para garantir que elas são suficientemente confiavéis para uso de emergência, quando necessário. [ISO/IEC 17799:2005].
5. É importante e obrigatório que as mídias de cópias de segurança sejam armazenadas em local distinto dos servidores de origem.

2 Escopo

Esta política limita-se às informações armazenadas nos servidores hospedados na sala de computadores da Superintendência de Tecnologia da Informação (STI) da UFBA e que estejam relacionadas com as atividades acadêmicas e administrativas da UFBA.

3 Definições

- Ativo: qualquer coisa que tenha valor para a organização. [ISO/IEC 13335-1:2004]
- Controle: forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal.

[ISO/IEC 17799:2005]

- Backup Incremental: cópia dos dados modificados desde o último backup realizado com sucesso.
- Política: Conjunto de parâmetros que definem a retenção das informações copiadas;
- Backup Full: cópia completa de todos os dados mapeados do ativo.
- Backup Diferencial: cópia dos dados modificados desde o último backup FULL realizado com sucesso.
- CRI: Coordenação de Redes e Infraestrutura/UFBA.
- Software de Gerência de Backup: aplicação utilizada para gerenciar o backup do ambiente;
- Co-location: Serviço de hospedagem de recursos de Tecnologia da Informação;
- Pool: Conjunto de volumes de discos ou fitas que armazenam os dados copiados.

4 Termos da Política

4.1 Informações que serão copiadas

Deverão ser feitas cópias de segurança das seguintes informações:

- Bancos de dados, sistema de arquivos e demais ativos de informação institucionais;
- Estado do sistema operacional dos servidores;
- Arquivos de Configurações dos serviços hospedados;
- Arquivos de logs dos servidores;
- Banco de dados e arquivos de configuração do Software de Gerência do Backup;
- Informações de servidor colocation, definidas pelo responsável, através de formulário de hospedagem do servidor preenchido no momento da solicitação;

Não serão feitas cópias das seguintes informações:

- Arquivos binários de programas;
- Arquivos de multímidias que não estejam relacionados as àreas acadêmicas e administrativas da UFBA.
- Arquivos de servidores de terceiros que não tenham relação com a UFBA, seus projetos e atividades;
- Servidores não hospedados na sala de computadores da STI.

As exceções ao item 1.2 deverão ser solicitadas ao Comitê Gestor do processo de backup, o qual é responsável por aprovar a inserção da informação na rotina de backup.

4.2 Modalidades de cópias de segurança realizadas

Os tipos de cópia de segurança realizados são incrementais, diferenciais ou full para todas as informações listadas no item 1.1.

4.3 Periodicidade das cópias de segurança

Nome	Tipo de Cópias	Quando Realizar	Criticidade
Diário	Incremental	Diariamente	Alta
Quinzenal	Full	A cada quinze dias	Alta
Mensal Diff	Diferencial	Uma vez ao mês	Alta
Mensal Full	Full	Uma vez ao mês	Alta
Trimestral	Full	Trimestralmente	Alta
Semestral	Full	Semestralmente	Alta

Anual	Full	Uma vez por ano ao final de dezembro	Alta

Obs.: As cópias incrementais deverão ser realizadas diariamente, com exceção dos servidores de email, Ilheus e Itabuna, que não farão seus backups incrementais aos sabádos para não concorrer com o backup full do Zimbra.

Obs.: As cópias full deverão ser iniciadas no primeiro dia útil do mês e finalizadas até o décimo quinto dia útil, com exceção do ambiente de banco de dados de produção onde são realizados duas cópias mensais full de quinze em quinze dias e uma cópia full anual com período de retenção de 5 (cinco) anos, realizada sempre na última semana do mês de dezembro.

4.4 Mídias de armazenamento

Como mídias de armazenamento, serão utilizadas fitas de tecnologia LTO (Line Tape Open) e discos.

4.5 Tempo de preservação das cópias de segurança

O tempo de preservação das cópias de segurança são definidas pelos tipos de cópias as quais são caracterizadas como incrementais e arquivamentos. Para cada tipo de cópia o tempo de preservação está relacionada a criticidade do tipo de serviço os quais serão abordados a seguir:

Serviços com Criticidade Alta

Serviço de E-mail: Política **EMAIL**

Tipo de Cópias	Quando	Retenção
Incremental	Diariamente	40 dias
Full	Mensalmente	365 dias (1 ano)

Serviço de Banco de Dados Produção: Política **DATABASE**

Tipo de Cópia	Quando Realizar	Retenção
Incremental	Diariamente	40 dias
Full	Mensalmente	180 dias (6 meses)
Full	Mensalmente	365 dias (1 ano)
Full	Última semana do mês de dezembro	1.825 dias (5 anos)

Serviço de Servidor de Arquivos: Política **FILESERVERS**

Tipo de Cópia	Quando Realizar	Retenção
Incremental	Diariamente	40 dias
Diferencial	Mensalmente	365 dias
Full	Trimestralmente	426 dias (14 meses)

Serviços com Criticidade Média

Serviço de Logs: Política **LOGSERVERS**

Tipo de Cópias	Quando	Retenção
Incremental	Diariamente	40 dias
Full	Mensalmente	365 dias (1 ano)

Politicas Gerais de Servidores: Política **SERVERS**

Tipo de Cópia	Quando Realizar	Retenção
Incremental	Diariamente	40 dias
Diferencial	Mensalmente	365 dias
Full	Trimestralmente	426 dias (14 meses)

Serviços com Criticidade Baixa

Serviço de Banco de Dados Homologação: Política **DATABASE_DEV_HOMOLOG**

Tipo de Cópia	Quando Realizar	Retenção
Incremental	Diariamente	40 dias

4.6 Armazenamento das mídias

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 no claviculário da Operação.
- Temperatura ambiente entre 18° e 27°C;
- Nível de umidade entre 40% e 60%;

Informações sobre os locais onde estão armazenadas as mídias de backup não devem ser divulgadas.

As mídias de backup deverão ser armazenadas em cofre com chave e/ou segredo, na unidade remota, e no cofre de mídias, na STI-UFBA .

As chaves para acesso ao cofre com as mídias no local remoto ficarão com os profissionais da Operacao e/ou com o Administrador de Backup.

As mídias das cópias, bem como o backup do banco de dados do Software de Gerência do Backup, serão enviadas à(s) localidade(s) remota(s) todas as terças e quintas, por um funcionário da CRI/UFBA, devidamente identificado.

4.7 Considerações Adicionais

É importante verificar constantemente os procedimentos dos backups diários assim como os procedimentos de auditoria dos backups, pois ambos são importantes para execução dos processos de backups realizados pela Equipe da Operação.

Estes procedimentos deverão ser revisados semestralmente.

Os profissionais da operação deverão executar as rotinas de backup e restauração, assim como ter acesso às mídias de armazenamento.

Todas as cópias salvas nas mídias descritas na seção 4 devem ser protegidas contra a leitura das informações armazenadas por pessoas não autorizadas.

A catalogação das mídias é feita manualmente através do Software de Gerência de Backup, seguindo o padrão 000XXXLY, onde "XXX" é um número seqüencialmente definido pelo barcode da fita e Y o nível da tecnologia LTO.

Devem ser verificados e cumpridos os prazos de utilização especificados pelo fabricante para cada tipo de mídia utilizado.

Deverá ser realizada semestralmente uma auditoria sobre a execução dos procedimentos de backup, verificando a conformidade destes com esta política e levantando problemas e suas soluções, e melhorias nos procedimentos.

A equipe definida para a realização da auditoria deverá ser formada pelo administrador do processo de backup e por outras pessoas designadas pela coordenação da CRI/UFBA.

O resultado da auditoria deverá ser entregue à coordenação da CRI, que poderá propor alterações nesta política, se necessário.

4.8 Responsabilidades

Comitê Gestor (Formado por 5 pessoas)

- Alocação dos recursos necessários para a execução dos procedimentos;
- Designação do funcionário responsável pela administração do processo de backup;
- Designação do funcionário responsável pela guarda da(s) chave(s) do armário ou cofre na localidade remota;
- Avaliar e autorizar as solicitações de inserção de ativos de informação citados no item 1.2. na rotina de backup;
- Em conjunto com o gestor da informação, avaliar, atualizar e aprovar a Política de Backup da Rede UFBA;

Coordenação da CRI

- Verificar as ocorrências de problemas na execução dos procedimentos juntamente com o administrador do backup;
- Avaliação e atualização da Política de Backup da Rede UFBA;

Administrador do backup

- Gerência do processo de backup;
- Analisar e solucionar os problemas relacionados com o backup;
- Sugerir modificações nos procedimentos de backup, de acordo com as análises dos problemas ocorridos;
- Execução dos procedimentos de verificação dos backups realizados;
- Reportar à coordenação da CRI os problemas acontecidos na execução dos procedimentos;
- Elaboração, verificação e atualização do processo de backup.

Operadores

- Execução dos procedimentos de backup e restauração da informação;
- Execução do procedimento de verificação das cópias;
- Execução do procedimento de Inclusão e Remoção do servidor na rotina de backup;
- Transporte das mídias de armazenamento;
- Execução dos procedimentos de verificação do estado das mídias;
- Execução dos procedimentos de movimentação dos dados em discos;
- Execução do procedimento retirada das fitas nas libraries.

Gestor da Informação (Glossário)

- Fornecimento da relação dos diretórios e arquivos a serem copiados;

4.9 Processos e Procedimentos Envolvidos

A implementação desta política está descrita no Processo de Backup, que é composto pelos seguintes procedimentos:

- Procedimento de Inserção/Remoção de uma Máquina na Rotina de Backup
- Procedimento de Verificação dos Backups Automáticos
- Procedimento de Restauraçao de Informação
- Procedimento de Inicialização e Finalização do Serviço Bareos
- Procedimento de Backup do System State
- Procedimento de Restore do System State
- Procedimento de Auditoria do Backup
- Mapeamento do Ambiente Bareos
- Procedimento Backup do BD do Bareos
- Procedimento de expansão do espaço disponível para Pools
- Procedimento de atualização dos diretórios da rotina de backup
- Procedimento de verificação dos backups realizados
- Procedimento Inclusão de Fitas na Unidade LTO
- Procedimento de Armazenamento de Backup Off-site

5 Referências

[ABNT ISO/IEC 17799:2005] ABNT. Tecnologia da Informação – Código de prática para a gestão da segurança da informação. NBR ISO/IEC 17799. Associação Brasileira de Normas Técnicas. 2005.

[ABNT ISO/IEC 27002:2013] ABNT. Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. NBR ISO/IEC 27002, Associação Brasileira de Normas Técnicas. 2013.

[ABNT ISO/IEC 27001:2006] ABNT. Tecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. NBR ISO/IEC 27001, Associação Brasileira de Normas Técnicas. 2006.

[P-SUP-01] Processo de Backup. Divisão de Suporte do Centro de Processamento de Dados da Universidade Federal da Bahia. 2004.

6 Controle de versão

Rev	Data	Descrição	Itens revisados	Revisado por
00	27/04/2020	Criacao do Documento	--	fernando.lacerda
01	27/04/2020	Revisao do Documento	--	michel.peterson