1. INTRODUÇÃO

Esse documento contém o Plano de Backup do Centro de Referência de Cordeiro do IFFluminense, e tem como objetivo definir os procedimentos que deverão ser seguidos pela Coordenação de Tecnologia da Informação e Comunicação, nas atividades relacionadas aos procedimentos de backup, restauração e testes de dados em conformidade com a Política de Backup e Restauração de Dados Digitais do IFF PORTARIA disponível REIT/IFFLU N° 1261, em https://cdd.iff.edu.br/documentos/portarias/reitoria/gabinete/2023/dezembro/portaria-1703884122.23.

2. OBJETIVO

O plano de backup é uma ferramenta fundamental que visa garantir a segurança e a disponibilidade dos dados de uma organização em caso de falhas de hardware, corrupção de dados, ataques cibernéticos ou desastres naturais. Os objetivos gerais do plano de backup do Centro de Referência de Cordeiro são:

2.1. Proteção de dados: O principal objetivo de um plano de backup é garantir a proteção dos dados da organização. Isso envolve fazer cópias de segurança dos dados críticos e sensíveis para evitar perdas irreparáveis em caso de falha do sistema.

2.2. Garantir a continuidade do negócio: Um plano de backup eficaz ajuda a manter a continuidade das operações mesmo em situações adversas. Se ocorrer uma falha no sistema principal, os dados podem ser restaurados a partir das cópias de segurança, minimizando o tempo de inatividade e reduzindo o impacto nas operações comerciais.

2.3. Cumprimento de regulamentos e normas: Um plano de backup deve garantir que a organização esteja em conformidade com esses requisitos, armazenando e protegendo os dados de acordo com as diretrizes estabelecidas.

2.4. Recuperação de desastres: O plano de backup deve incluir procedimentos claros e eficazes para a recuperação de desastres. Isso significa que, em caso de incidente grave, como incêndio, inundação ou ataque cibernético, os dados podem ser restaurados rapidamente e com o mínimo de perda possível.

2.5. Proteção contra ameaças cibernéticas: Com o aumento das ameaças cibernéticas, como ransomware e malware, é crucial que o plano de backup inclua medidas para proteger os dados contra essas ameaças. Isso pode envolver a criação de cópias de segurança off-line ou em locais seguros, além de implementar protocolos de segurança robustos para prevenir ataques.

2.6. Testes e validação: Um plano de backup não é eficaz a menos que seja testado regularmente para garantir que os procedimentos de backup e recuperação funcionem conforme o esperado. Os

testes de backup devem ser realizados periodicamente para verificar a integridade dos dados de backup e a capacidade de recuperação do sistema.

2.7. Escalabilidade e flexibilidade: O plano de backup deve ser escalável e flexível o suficiente para acompanhar o crescimento e as mudanças na organização. À medida que novos sistemas e dados são adicionados, o plano de backup deve ser ajustado para garantir que todos os dados críticos sejam protegidos adequadamente.

2.8. Gerenciamento eficiente dos recursos: Um plano de backup eficaz deve gerenciar os recursos de armazenamento de forma eficiente, garantindo que os dados sejam armazenados de maneira econômica, sem comprometer a segurança ou a integridade dos dados.

3. CAMPO DE APLICAÇÃO

Esta rotina se aplica à equipe da Coordenação de TI do campus Pádua, responsável pelo atendimento de TI a unidade de Cordeiro no momento da publicação desta política, e engloba todos os dados, em formato digital, custodiados por esta unidade do IFFluminense.

4. VIGÊNCIA

A vigência deste plano é de 2 anos a contar da data de sua aprovação.

5. RESPONSABILIDADES

NOME	**RESPONSABILIDADE**
Rodrigo Augusto de Oliveira Barros	Responsável da área de TIC da Unidade por elaborar o plano de backup de sua unidade.
João Vitor Esposte Campos / Rodrigo Augusto de Oliveira Barros	Responsável pela operação de backup da unidade.

6. RELAÇÃO DE SISTEMAS CRÍTICOS DA UNIDADE

Sistemas **críticos** são aqueles cuja falha temporária provoca impacto imediato e significativo nas áreas de negócio que dependem de sua operação, podendo resultar na paralisação parcial ou total dessas áreas.

6.1. Servidor de Virtualização (ProxMox);

6.2. Firewall da Rede (pfSense);

6.3. Controladores de Domínio (Samba 4);

6.4. Servidor de Arquivos (Samba);

6.5. Servidor de Impressão (Samba);

6.6. Servidor de Autenticação para Alunos (FreeRadius);

6.7. Servidor de Autenticação para Servidores (FreeRadius).

7. RELAÇÃO DOS SISTEMAS NÃO CRÍTICOS DA UNIDADE

Sistemas **não críticos** são aqueles cuja falha não acarreta grandes prejuízos para as áreas de negócio envolvidas, permitindo a continuidade das operações com um mínimo de impacto operacional.

7.1. Servidor de Banco de Dados (PostgreSQL);

7.2. Servidor de Gerenciamento de Senhas/Cofre Digital (BitWarden);

7.3. Gateway de acesso remoto (Guacamole);

7.4. Gerenciador de Ativos de TI (OCS Inventory);

7.5. Proxy Reverso p/ Expor Aplicações Internas Específicas (HA Proxy);

7.6. Plataforma de monitoramento de rede e sistemas (Zabbix);

7.7. Orquestrador de Contêineres (Kubernetes);

7.8. Diversos Sistemas Internos de TIC (rodando em containers Docker, LXC ou Kubernetes) ;

7.9. Servidor RSAT de Administração do Domínio.

8. PROCESSO DE BACKUP

O processo de Backup será aplicado com as plataformas e sistemas utilizados por esta unidade (Centro de Referência de Cordeiro), de acordo com o formulário do esquema de backup (modelo no ANEXO II - ANEXOS DO PLANO DE BACKUP), com o formulário para testes de restauração e validação de backup(modelo no ANEXO II - ANEXOS DO PLANO DE BACKUP), e está estruturado da seguinte forma:

8.1. Banco de Dados

Vide seção 8.2

8.2. Máquinas Virtuais

Contêineres LXC:

- Servidor de Banco de Dados Postgre SQL: SV-160-DB01 (ProxMox ID: 109)

- Controlador de Domínio Primário: TICDC-160-DC01 (ProxMox ID: 103)

- Controlador de Domínio Secundário: SV-160-DC02 (ProxMox ID: 106)

- Servidor de Arquivos: SV-160-FS01 (ProxMox ID: 110)

- Servidor de Impressão: SV-160-PS01 (ProxMox ID: 111)

- Servidor NFS: SV-160-NF01 (ProxMox ID: 101)

- Servidor de Gerenciamento de Senhas: SV-160-PSW01 (ProxMox ID: 115)

- Gerenciador de Ativos de TI: SV-160-OCS01 (ProxMox ID: 102)

- Proxy Reverso Interno: SV-160-HA01 (ProxMox ID: 112)

Máquinas Virtuais:

- Servidor RSAT: SV-160-RSAT01 (ProxMox ID: 105)

Utilização do Esquema GFS (Grandfather-Father-Son), sendo esta uma estratégia de backup que mantém diferentes níveis de backups ao longo do tempo. Inclui backups diários (sons - filhos), semanais (Father - pais) e mensais (Grandfather - avós), permitindo a recuperação granular de dados em diferentes pontos no tempo com base na necessidade.

O backup destes ativos consiste em duas fases, sendo:

Fase 1: backup do contêiner por meio da ferramenta de backup do ProxMox;

Fase 2: backup da pasta /var/lib/vz do ProxMox, onde são armazenados os backups da virtualizadora, por meio do cliente Bácula vinculado a ferramenta de backup da Reitoria.

O Backup offsite provido pela Reitoria utiliza fitas LTO como mídia de armazenamento, sendo disponibilizado ao campus o espaço total de 3TB do referido volume.

Os Sistemas Operacionais utilizados serão descritos no item 8.3. Sistema Operacional

8.3 Sistema Operacional

8.3.1. O Hypervisor ProxMox é baseado em Debian;

8.3.2. Os Contêineres LXC são todos baseados em Ubuntu Server LTS;

8.3.3. O Servidor RSAT utiliza Windows 10 Pro.

8.4. Servidores

- Servidor de Virtualização: SR-160-000077 (ProxMox Server)

Utilização do Esquema GFS (Grandfather-Father-Son), sendo esta uma estratégia de backup que mantém diferentes níveis de backups ao longo do tempo. Inclui backups diários (sons - filhos), semanais (Father - pais) e mensais (Grandfather - avós), permitindo a recuperação granular de dados em diferentes pontos no tempo com base na necessidade.

O backup deste ativo consiste em uma fase, sendo:

Fase 1: backup das pastas importantes do ProxMox abaixo:

1. **/etc/pve**: Ainda contém a configuração global do Proxmox VE, incluindo configurações de cluster, armazenamento, redes e outros.

2. **/etc/pve/qemu-server**: Contém os arquivos de configuração das máquinas virtuais KVM.
3. **/etc/pve/lxc**: Contém os arquivos de configuração dos contêineres LXC.
4. **/var/lib/vz**: Contém os discos e imagens de disco das máquinas virtuais e contêineres. Esta pasta é importante para backup, pois contém os dados das VMs e contêineres.
5. **/var/lib/rrdcached**: Ainda contém os arquivos de dados RRD usados para gráficos de monitoramento.
6. **/var/lib/pve-cluster**: Esta pasta contém dados de configuração do cluster Proxmox, se você estiver usando um cluster.

O backup da virtualizadora é feito por meio do cliente Bácula vinculado a ferramenta de backup da Reitoria.

O Backup offsite provido pela Reitoria utiliza fitas LTO como mídia de armazenamento, sendo disponibilizado ao campus o espaço total de 3TB do referido volume.

8.5. Arquivos de Configuração de ativos

Vide seção 8.2 e 8.4 e seção privada no repositório https://github.com/iff-cordeiro-ctic

8.6. Servidor de Arquivos

Vide seção 8.2

8.7. Mídia de Armazenamento Utilizada

O Backup offsite provido pela Reitoria utiliza fitas LTO como mídia de armazenamento, sendo disponibilizado ao campus o espaço total de 3TB do referido volume.

Realizado, obedecendo à seguinte rotina:

Backup GFS (Grandfather-Father-Son), usando backups full e incremental em diferentes intervalos para criar uma estratégia de retenção de dados ao longo do tempo. Aqui estão as características típicas dos tipos de backup (full ou incremental) para os níveis mensal, semanal e diário:

1. Backup Mensal (Avô):
   - Tipo: Full
   - Características: Um backup completo de todos os dados é feito uma vez por mês.
   - Retenção: 730 dias.
   - Objetivo: Captura uma imagem completa dos dados em um determinado ponto no tempo para fins de longo prazo e conformidade.

2. Backup Semanal (Pai):
   - Tipo: Full

- Características: Um backup completo realizado no início da semana (full), seguido de backups incrementais nos dias subsequentes.
- Retenção: 730 dias.
- Objetivo: Captura uma imagem mais recente e abrangente dos dados, permitindo uma recuperação rápida e eficiente em caso de perda de dados.

3. Backup Diário (Filho):
- Tipo: Incremental
- Características: Apenas as alterações desde o último backup são copiadas.
- Retenção: 730 dias.
- Objetivo: Captura as alterações diárias nos dados, minimizando o tempo e os recursos necessários para fazer backup e restaurar dados regularmente.

Essa combinação de backups full e incrementais em diferentes intervalos oferece uma estratégia robusta para garantir a disponibilidade e integridade dos dados ao longo do tempo, equilibrando a eficiência de armazenamento com a capacidade de recuperação rápida e granular em diferentes pontos no tempo.

8.8. Réplica Off-Site

Por padrão, o backup do Centro de Referência de Cordeiro é realizado offsite, utilizando a ferramenta fornecida pela Reitoria. Nesse contexto, a exportação do backup para o storage de backup off-site não é aplicável. Portanto, a inclusão do ANEXO I não se faz necessária.

ANEXO I – AGENDAMENTO DA RÉPLICA OFF-SITE

Servidor	Dom	Seg	Ter	Qua	Qui	Sex	Sáb	Hora BKP	Hora Rsync	Cluster	Ambiente

ANEXO II – FORMULÁRIO DO ESQUEMA DE BACKUP

<NOME DO BANCO DE DADOS>				
Descrição do Esquema de Backup				
<Descrever a estratégia de backup>				
Informação do BD				
Versão				
Localização do BD (IP):				
Sistema Operacional:				
Cliente de Backup				
Software de Backup:	<bacula>			
Tipo de Agente Necessário:	<bacula-client>			
Script ou Ferramenta adicional				
Nomenclatura dos Volumes				
Banco	<db_name> sql			
Moodle	dump_moodle<versao>.sql			
OJS	Ojs.sql			
Atom	dump_atom.sql			
Mídia Físicas (Fita Magnética)				

Agendamento da Política Diária				
Tipo de Backup	**Banco de Dados**			
	Dados		**Binários**	
	Disco	**Fita**		
Full	<frequência temporall + horário>	<frequência temporall + horário>		
Incremental	-	-		
Diferencial	-	-		

Retenção do Backup						
	Full		**Incremental**		**Diferencial**	
	Disco	**Fita**	**Disco**	**Fita**	**Disco**	**Fita**
Retenção (tempo em que o backup será mantido)	<frequência temporal>	<frequência temporal>				
RPO (tempo máximo de perda de dados)	<frequência temporal>	<frequência temporal>				
RTO (tempo estimado para a restauração)	<frequência temporal>	<frequência temporal>				

Esquema de Teste e Validação				
	Recuperação	**Validação**	**Responsável**	**Periodicidade**
Observações				

ANEXO III – MODELO DE FORMULÁRIO PARA TESTES DE RESTAURAÇÃO E VALIDAÇÃO DE BACKUP

Banco de Dados								
	Restauração				Validação			
Grupo de Backup	Responsável	Tipo de Mídia	Data	Resultado	Responsável	Data	Resultado	OBS
			25/01/2024	ok		25/01/2024	ok	

Sistema Operacional								
	Restauração				Validação			
Grupo de Backup	Responsável	Tipo de Mídia	Data	Resultado	Responsável	Data	Resultado	OBS

REPOSITÓRIO PÚBLICO DESTA POLÍTICA	
Atualizações no Github	https://github.com/iff-padua-ctic/politica-backup.git

HISTÓRICO DE VERSÕES

Data	Versão	Descrição
03/05/2024	1.0	Estabelecimento do modelo de Plano de Backup.