



MANUAL DE BACKUP E RESTAURAÇÃO DE DADOS

1. OBJETIVO

Visando a assegurar o acesso e a proteção das informações eletrônicas do CRCPR, se estabelece o presente Manual de *Backup* e Restauração de Dados, que observa, criteriosamente, o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.

2. RESPONSÁVEL

O responsável/administrador pelo *backup* do CRCPR será o coordenado de TIC, que será responsável pelos procedimentos de configuração, execução, monitoramento e testes dos procedimentos de *backup* e *restore*.

O administrador de *rede* será o assistente de informática.

3. DIRETÓRIO DE ARMAZENAMENTO

O CRCPR possui diretórios de armazenamento físicos, nas dependências do órgão. Em que pese grande parte trate de dados físicos, poucos setores possuem arquivos fechados à chave, mas, em alguns casos, não há o hábito de mantê-los efetivamente chaveados.

Quanto ao armazenamento de arquivos físicos, os *backups* são realizados através do *Software Veem Backup & Replication 10*.

4. ROTINAS DE BACKUP

Os *backups* são realizados automaticamente, através do *Software Veem Backup & Replication 10*, com a seguinte estratégia:

Servidor	Horário	Frequência
Banco de Dados	a cada 1 hora	Diária
Servidor de Arquivos	a cada 6 horas	Diária
Servidor Active Directory	17:00	Diária
Servidor Folha de Pagamento	18:00	Diária
Servidor de Imagens (imprensa)	00:00	Diária



<i>Servidores Linux (Portal do CRCPR, Sistemas Web, E-mail corporativo, Envio de lista de e-mails)</i>	<i>19:00</i>	<i>Diária</i>
<i>Servidores Windows (Antivirus Corporativo, Aplicativos remoto, Suporte HelpDesk, Sistemas Web, Serviço de Impressão, Mensageiro Corporativo, Sincronismo Office 365 nuvem, Serviço de Atualização de Servidores e Desktops).</i>	<i>20:00</i>	<i>Diária</i>
<i>Cópia de segurança de todas as máquinas virtuais, em equipamento localizado em outro andar do prédio do CRCPR.</i>	<i>18:00</i>	<i>Diária</i>
<i>Backup Tape</i>	<i>05:00</i>	<i>Semanal (Domingo)</i>

5. LOCAIS DE ARMAZENAMENTO

5.1. Local 01 - Para o primeiro local de *backup* é utilizado repositório no próprio servidor que está instalado e configurado o *Software Veem Backup & Replication 10*, conforme abaixo:

- Servidor HPE Proliant DL380 Gen10
- 2 discos de 480 GB SSD SFF (2.5"), SATA 6 Gb, Hot Plug, para sistema operacional;
- 12 discos de 4 TB LFF (3.5"), SAS 12 Gb, 7,2k rpm, Hot Plug, totalizando 48 TB de área bruta, sendo 32,7 TiB de área líquida considerando RAID 6 (9+2) + 1 disco para spare

5.2. Local 02 - Equipamento instalado em outra sala dentro da sede do CRCPR em Curitiba, em local distante do *DataCenter*, onde são realizadas as cópias de segurança dos backups do Local 01, conforme abaixo:

- Servidor HPE Proliant ML30 Gen10
- 4 discos de 8 TB LFF (3.5"), SATA 12 Gb, 7,2k rpm, Hot Plug, totalizando 32 TB de área bruta, sendo 21,6 TiB de área líquida considerando RAID 5 (3+1);

5.3. Local 03 - Backup realizado em Fita LTO-7, semanalmente, e armazenado em local fora da sede do CRCPR, conforme abaixo:





- HPE Autoloader 1/8 G2 FC LTO-7
- 1 drive Ultrium 15000 (LTO7) com capacidade de 6/15TB;

6. VOLUME E TEMPO DE CONSERVAÇÃO DOS DADOS

O volume de *backups* realizados são:

Local 01 – Espaço disponível 32,7TB, utilizado para backups 22,8TB

Local 02 – Espaço disponível 21,7TB, utilizado 12,6TB

Local 03 – Espaço disponível 8 Fitas LTO-7, com capacidade para até 48/120TB

Os *backups* são conservados da seguinte maneira:

Backup	Pontos de recuperação	Tempo armazenamento
<i>Banco de Dados</i>	999	41 dias
<i>Servidor de Arquivos</i>	240	60 dias
<i>Servidor Active Directory</i>	60	60 dias
<i>Servidor Folha de Pagamento</i>	90	90 dias
<i>Servidor de Imagens</i>	45	45 dias
<i>Servidores Linux</i>	45	45 dias
<i>Servidores Windows</i>	45	45 dias
<i>Cópia de Segurança</i>	20	20 dias
<i>Backup Tape</i>	30	30 semanas

Ao final do prazo, os *backups* são excluídos automaticamente.

7. TESTE DE VALIDAÇÃO DAS CÓPIAS

Os testes de validação de cópias serão realizados exclusivamente em caso de falha percebida e confirmada dos *backups*, conforme mensagens de alerta do *software* conferidos diariamente pelo administrador de *backup*.

8. ADMINISTRADOR DE BACKUP

O administrador do *backup* será responsável pela política e procedimentos relativos aos serviços de *backup* e *restore*, bem como, de guardar as mídias móveis e assegurar o cumprimento das normas aplicáveis.



São atribuições do administrador de *backup*:

- Propor modificações visando ao aperfeiçoamento da política de *backup*;
- Criar e manter os *backups*;
- Configurar a ferramenta de *backup*;
- Criar e testar *scripts*;
- Criar e manter mídias;
- Testar o *backup* e *restore*;
- Criar notificações e relatórios;
- Verificar periodicamente os relatórios gerados pela ferramenta de *backup*;
- Restaurar os *backups* em caso de necessidade;
- 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;
- Fazer manutenções periódicas dos dispositivos de *backup*;
- Fazer o carregamento das mídias necessárias para os *backups* programados;
- Fazer o armazenamento das mídias de *backup* em cofre próprio.
- Todo e qualquer dispositivo que armazene dados deverão ser considerados para sua inclusão no *backup*.

O administrador de *backup* poderá delegar algumas dessas funções ao administrador de rede, conforme a necessidade, mediante descrição do cargo.

9. ARQUIVOS DE *BACKUP*

O administrador do *backup* definirá quais diretórios e arquivos serão incluídos no *backup*, tendo como prioridade:

- Arquivos de configurações de sistemas operacionais e aplicativos instalados em servidores;
- Arquivos de *log* dos aplicativos, inclusive *log* da ferramenta de *backup* e *restore*;
- Informações e configurações de banco de dados;
- Arquivos de usuários (documentos e e-mails);

O administrador de *backup* definirá quais diretórios e arquivos não serão incluídos na rotina, tendo como referência:

- Arquivos do sistema operacional ou de aplicações que podem ser recolocados através de uma nova instalação;





- Arquivos temporários;
- Arquivos salvos nas unidades locais das estações de trabalho;
- Arquivos da área de transferência;
- Arquivos particulares dos usuários.

Para os aplicativos e/ou bancos de dados devem ser seguidas as recomendações sugeridas pelo desenvolvedor e/ou fabricante.

Os procedimentos de *backup* deverão ser atualizados quando houver:

- Novas aplicações desenvolvidas;
- Novos locais de armazenamento de dados ou arquivos;
- Novas instalações de bancos de dados;
- Novos aplicativos instalados;
- Outras informações que necessitem de proteção através de backups deverão ser informadas ao Administrador de *Backup*.

10. OPERAÇÃO DE BACKUP

- O *backup* deverá ser monitorado pelo administrador de *backup* e pelo administrador de rede;
- Para todos os *backups* realizados com sucesso, será gerado um extrato automatizado pela própria ferramenta de *backup*, confirmando a execução do mesmo;
- Para os *backups* que apresentarem falhas, o administrador de *backup* deverá criar um relatório de "Acompanhamento de *backup*", no qual deverá constar a data, os horários de início e término, os objetos e os clientes de backup, a causa da falha, a ação corretiva adotada e qual parte do backup ficou comprometida.

11. RECUPERAÇÃO DE BACKUPS

Os *backups* do CRCPR contêm informações confidenciais, dados pessoais e pessoais sensíveis de colaboradores, beneficiários e participantes, portanto, apenas o administrador de *backup* e o administrador de Rede poderão realizá-la.





Os usuários que necessitarem recuperar arquivos devem contatar o administrador de *backup* e registrar a solicitação através do e-mail [helpdesk](#). O gestor do solicitante da recuperação deverá encaminhar *e-mail* ao setor de TI ratificando o requerimento.

Serão mantidos registros de todos os arquivos cuja restauração foi solicitada, juntamente às informações relativas ao solicitante, nome do arquivo, data da versão restaurada, data e hora da solicitação e autorização do gestor do solicitante.

Os bancos de dados também serão restaurados pelo Administrador de Backup, por conterem dados pessoais que demandam proteção.

Quaisquer procedimentos programados nos servidores e que impliquem riscos de funcionamento ou em quaisquer dispositivos de armazenamento do CRCPR, somente deverão ser executados após a realização do backup dos seus dados.

O descarte das mídias de *backup* inservíveis ou inutilizáveis deverá ser feito mediante proposta apresentada pelo administrador de backup e aprovada pela equipe de trabalho.

12. TEMPO DE RESTAURAÇÃO

Após a solicitação de restauração de arquivo ou banco de dados, caberá ao administrador de *backup* definir o período de recuperação, levando-se em consideração a complexidade do arquivo.

Data da última atualização: 29 de outubro de 2021.

