



## **DIRETORIA-EXECUTIVA**

### **Resolução nº 12, de 10 de abril de 2026**

*Estabelece o Plano de Recuperação de Desastres de Tecnologia da Informação (TI) no âmbito da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev.*

**A Diretora-Presidente da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev**, no uso de suas atribuições legais, previstas no artigo 57, inciso IX do Estatuto e no artigo 44, inciso XIX do Regimento Interno; e, considerando o artigo 53, inciso X do Estatuto e artigo 27, inciso X do Regimento Interno, registra que a Diretoria-Executiva, em sua 413ª Reunião Ordinária, ocorrida em 10 de abril de 2026, RESOLVE:

Art. 1º. Fica estabelecido o Plano de Recuperação de Desastres de Tecnologia da Informação (TI) no âmbito da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev, conforme ANEXO I.

Art. 2º. Esta Resolução entra em vigor na data da sua aprovação.

 Assinado de  
forma digital  
por ELISANGELA  
HESSSE:65468627  
000

**Elisângela Hesse**

Diretora-Presidente

**FUNDAÇÃO DE PREVIDÊNCIA COMPLEMENTAR  
DO SERVIDOR PÚBLICO DO ESTADO DO RIO GRANDE DO SUL**



## ANEXO I

### PLANO DE RECUPERAÇÃO DE DESASTRES DE TECNOLOGIA DA INFORMAÇÃO (TI)

#### 1 APRESENTAÇÃO

- 1.1. Fica aprovado o Plano de Recuperação de Desastres de Tecnologia da Informação (TI) no âmbito da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev.
- 1.2. O plano tem como objetivo esclarecer o procedimento para a rápida recuperação dos sistemas e dados críticos da RS-Prev em caso de desastre, assegurando a continuidade dos serviços de Tecnologia da Informação.

#### 2 DEFINIÇÕES

- 2.1. *Backup*: Cópia de segurança dos dados.
- 2.2. *DRP*: Plano de recuperação de desastres de Tecnologia da Informação.
- 2.3. *Emergência*: situação séria, de aparição súbita, que causa ou ameaça perigo à vida, ao patrimônio ou ao meio ambiente.
- 2.4. *Evento*: situação com possibilidade de ocorrência que, caso se materialize, pode gerar perdas diretas e/ou indiretas, além de eventualmente resultar em situações de emergência.
- 2.5. *Failover*: Mecanismo de troca automática para sistema reserva.
- 2.6. *RPO*: Idade máxima dos dados que podem ser perdidos.
- 2.7. *RTO*: Tempo máximo aceitável para recuperação.
- 2.8. *TI*: Tecnologia da Informação

#### 3 PLANO DE PLANO DE RECUPERAÇÃO DE DESASTRES DE TI

A recuperação de desastres depende de um plano sólido para colocar sistemas e infraestrutura essenciais em funcionamento após uma interrupção, idealmente em minutos.



### 3.1. Elementos de recuperação de desastres de TI

O DRP da RS-Prev aborda três elementos diferentes para recuperação:

3.1.1. Prevenção: busca garantir que os sistemas sejam os mais seguros e confiáveis possível, usando ferramentas e técnicas para evitar que um desastre ocorra. Como controle preventivo são realizados *backup* de dados críticos e monitoramento contínuo de ambientes em busca de erros de configuração e violações de conformidade.

3.1.2. Detecção: busca saber quando uma resposta é necessária, a fim de detectar ou descobrir eventos indesejados na hora em que eles acontecem.

3.1.3. Correção: busca planejar possíveis cenários de desastres de TI a fim de garantir operações de backup para reduzir o impacto e implementar procedimentos de recuperação para restaurar dados e sistemas rapidamente se for necessário.

A recuperação de desastres envolve a replicação e o *backup* seguros de dados e cargas de trabalho essenciais para um local secundário ou vários locais de recuperação de desastres. Um local de recuperação de desastres pode ser usado para recuperar dados do *backup* mais recente ou de um momento anterior. Pode-se voltar a usar um local de recuperação de desastre se o local principal e os sistemas falharem devido a um evento imprevisível até que o principal seja restaurado.

### 3.2. Tipos de recuperação de desastres de TI

Estão estruturados para atual estrutura de TI da Fundação, pequeno porte, entre elas:

3.2.1. *Backups*: os dados são copiados para um sistema externo secundário ou enviados para um local externo secundário

3.2.2. *Backup* como serviço (*BaaS*): provedor terceirizado que oferece backups regulares de dados.

3.2.3. Recuperação de desastres como serviço (*DRaaS*): os dados e a infraestrutura de TI são armazenados em *backup* e hospedados na infraestrutura em nuvem de um provedor terceirizado. O provedor implementa e orquestra o DRP durante uma crise.



3.2.4. *Snapshots* pontuais: dados, arquivos ou um banco de dados inteiro são replicados em um momento específico. Os *snapshots* podem ser usados para restaurar dados, desde que a cópia seja armazenada em um local não afetado pelo evento.

3.2.5. *DRP* virtual: as operações e os dados são armazenados em *backup*, ou uma réplica completa da infraestrutura de TI é criada e executada em máquinas virtuais externas (VMs).

3.2.6. Local de recuperação de desastres: é o local que a Fundação pode usar temporariamente após um evento de desastre, que contém *backups* de dados, sistemas e outras infraestruturas de tecnologia.

### **3.3. Etapas de recuperação de desastres de TI**

3.3.1. Avaliação de riscos: Identifica-se as possíveis ameaças e vulnerabilidades que possam interromper os sistemas de TI e as operações comerciais.

3.3.2. Análise de impacto nos negócios: Determina-se o impacto de possíveis interrupções nas funções comerciais críticas, incluindo perdas financeiras, danos à reputação e violações de conformidade.

3.3.3. Planejamento de *DRP*: Registram-se as etapas a serem seguidas antes, durante e depois de um evento de desastre. O plano inclui funções e responsabilidades claras, procedimentos de recuperação e protocolos de comunicação. Na estratégia de recuperação de desastres inclui-se requisitos detalhados de resposta a emergências, operações de *backup* e procedimentos de recuperação, de forma a garantir a continuidade de negócios. O plano está associado ao plano de contingência para mitigar o impacto além da infraestrutura e dos sistemas de TI, permitindo que todas as áreas de negócios retomem as operações normais o mais rápido possível.

3.3.4. Implementação: A implantação é realizada configurando sistemas de *backup* e replicação, mecanismos de *failover* e estabelecendo canais de comunicação. O tempo de recuperação (RTO) é o período máximo aceitável em que sistemas e aplicativos podem ficar inativos sem causar danos significativos a operação. Já o ponto de recuperação (RPO) é a idade máxima dos dados que precisam ser recuperados para retomar as operações



após um evento grave, isto é, define a frequência de *backups*. A recuperação de desastres na nuvem reduz a maioria, se não todos, os fatores de riscos.

3.3.5. Teste e manutenção: Anualmente é realizado teste para garantir a eficácia e identificar possíveis falhas. O plano é atualizado conforme necessidade para refletir as mudanças no ambiente de TI e nos requisitos de negócios.

#### **4. REFERÊNCIAS**

4.1. ABNT NBR ISO/IEC 27031 DE 01/2023 – Tecnologia da informação – Técnicas de segurança – Diretrizes para a prontidão para a continuidade de negócios da tecnologia da informação e comunicação.

4.2. ABNT NBR Isso 22301 DE 06/2024 – Segurança e resiliência – Sistema de gestão de continuidade de negócios – Requisitos.

4.3. Plano de Contingências RS-Prev.

4.4. Política de Segurança da Informação da RS-Prev.

4.5. Manual de Gestão de Emergências e Preparação para Desastres – ICA.

#### **5. DISPOSIÇÕES FINAIS**

O plano entra em vigor na data de sua aprovação e tem validade por tempo indeterminado.