DIRETORIA-EXECUTIVA

Resolução n° 09, de 27 de junho de 2025

Estabelece o Plano de Contingência 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 374ª Reunião Ordinária, ocorrida em 27 de junho de 2025, RESOLVE:

Art. 1º. Fica estabelecido o Plano de Contingência 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 HESSE:65468627000

Elisângela Hesse

Diretora-Presidente

ANEXO I

PLANO DE CONTINGÊNCIA

1 APRESENTAÇÃO

1.1 Fica aprovado o Plano de Contingência no âmbito da Fundação de Previdência Complementar do Servidor Público do Estado do Rio Grande do Sul – RS-Prev.

O plano tem como objetivo fornecer diretrizes e orientações gerais a dirigentes, colaboradores e partes interessadas, a fim de promover a manutenção ou a retomada das atividades em caso de interrupção operacional.

1.2 Além das orientações do Plano de Contingência (PCO), devem ser consultados os seguintes planos, observadas as suas respectivas responsabilidades:

1.3.1 Plano de Emergência (PAE): procedimentos imediatos para emergências, como incêndios e desastres, com foco em evacuação, primeiros socorros e resposta rápida. (Elaborado com base no PPCI do condomínio).

1.3.2 Plano de Gerenciamento de Crises (PGC): estratégias para resposta aos cenários de crises que possam ameaçar a administração ou a reputação institucional, incluindo comunicação interna e externa, com diretrizes para administrar, neutralizar ou eliminar os impactos até a superação da crise. (Elaborado por empresa de comunicação terceirizada).

1.3.3 Plano de Resposta a Incidentes de Segurança (PRIS): procedimentos para tratamento de incidentes que envolvam violação de segurança, especialmente aqueles relacionados a dados pessoais, como acessos não autorizados, vazamentos, perdas, destruição, alteração ou qualquer forma de tratamento inadequado ou ilícito, que possam gerar riscos aos direitos dos titulares e impactos à operação ou à reputação institucional. (Elaborado pelo Comitê LGPD).

2 DEFINIÇÕES

2.1. Ambiente de contingência: soluções alternativas que podem ser acionadas em caso de falha no ambiente principal. Pode incluir *backup de data centers*, sistemas redundantes, servidores externos ou locais remotos.

2.2. Atividades prioritárias: aquelas que devem ser priorizadas após um incidente para mitigar os impactos. Podem ser classificadas como: críticas, vitais, essenciais, urgentes e fundamentais.

2.3. Contingência: capacidade em continuar a entregar serviços em um nível aceitável previamente definido após incidentes de interrupção.

2.4. Crise: período prolongado dos impactos do incidente e de busca de solução.

2.5. 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.

2.6. Evento disruptivo: incidente natural ou causado pelo homem, que causa um desvio não planejado e negativo na entrega dos serviços e operações de negócio.

2.7. Gestão de continuidade de negócios: processo através do qual identificam-se ameaças potenciais e os possíveis impactos nas operações, e se prepara para os incidentes, com ações estruturadas para mitigação dos riscos e gerenciamento da crise.

2.8. Incidente de segurança com dados pessoais: evento adverso que compromete as propriedades de confidencialidade, integridade, disponibilidade e autenticidade da segurança de dados pessoais.

2.9. Incidente: evento de pequeno, médio ou grande porte, que pode levar à interrupção de negócios, perdas, emergências ou crise.

2.10. Interrupção: incidente que resulta em desvios negativos na entrega esperada de serviços de acordo com os objetivos da Fundação.

2.11. *Patch*: programa de computador criado para atualizar ou corrigir um *software*.

Plano de contingência: conjunto de procedimentos documentados que orientam a continuidade de negócio e como restaurar um nível pré-definido de operação e manutenção da entrega do serviço após a interrupção ou durante a crise.

2.12. Plano de f*ailover*: um conjunto de procedimentos e recursos utilizados para garantir a disponibilidade contínua de seus sistemas e serviços em caso de falhas ou interrupções.

2.13. Risco: é medido a partir da ponderação entre a probabilidade de ocorrência do evento e respectivo nível de impacto.

3 AVALIAÇÃO DE RISCOS PARA CONTINGÊNCIA

O objetivo da avaliação é identificar possíveis riscos que possam interromper os processos críticos da Fundação. Molda o escopo geral de contingência, fornecendo uma lista de eventos possíveis e consequências associadas que devem ser abordados em um plano de mitigação de riscos.

EVENTOS DISRUPTIVOS: Exemplos de eventos disruptivos que podem afetar processos críticos e motivo pelos quais os planos de contingência devem ser acionados:

Eventos Disruptivos	Possíveis causas
Desastres naturais	• Alagamentos ou inundações provocados por chuvas intensas; • Danos causados por descargas atmosféricas; • Deslizamentos de terra que afetem a infraestrutura;
Epidemias ou outros riscos médicos	• Falta de acesso a equipamentos de proteção ou medicamentos essenciais; • Pandemias globais; • Surto de doenças contagiosas na equipe;
Incêndios e explosões	• Armazenamento inadequado de materiais inflamáveis. • Curto circuitos na rede elétrica;

	• Falha em sistemas de segurança contra incêndios.
Falta de eletricidade, de rede de telecomunicações e de *data center*	• Falha de concessionária de energia elétrica; • Problemas com fornecedores de TIC e telecomunicações; • Falha na prestadora de serviço de *data center;* • Rompimento de cabos de interconexão decorrente da execução de obras públicas, desastres ou acidentes.
Fatores humanos, como erros de funcionários, atos criminosos e fraudes	• Atos internos de má-fé, como sabotagem ou fraude; • Erros ao operar equipamentos sensíveis; • Falhas em seguir procedimentos de segurança.
Riscos de TIC, como terrorismo cibernético, vírus e ataques *hacker*	• Ataques de *ransomware;* • *DDoS (Distributed Denial of Service)* - Ataque Distribuído de Negação de Serviço) que tornem os sistemas inacessíveis; • Disseminação de *malware* na rede; • Invasão por *hackers* com roubo/sequestro de dados.

4 ESTRATÉGIAS DE RECUPERAÇÃO E CONTINGÊNCIA

Algumas das soluções para contingência incluem: trabalhos manuais; terceirização; recuperação de desastres para TIC; reestruturação de equipe alternativa e instalações alternativas.

4.1 TREINAMENTO E TESTES DE CONTINGÊNCIA: A eficácia do Plano de Contingência depende da capacitação dos envolvidos e da realização periódica de testes para

validar os procedimentos estabelecidos. Os treinamentos poderão ser conduzidos por equipes especializadas, internas ou externas, e poderão incluir exercícios presenciais, treinamentos *online* e simulações controladas.

4.1.1 Capacitação periódica: instrução sobre procedimentos de contingência para dirigentes e colaboradores.

4.1.2 Simulações práticas: realização de testes para avaliar a eficácia dos planos de resposta a incidentes, recuperação de dados e restauração de sistemas críticos.

4.1.3 Testes de infraestrutura: verificação da redundância de TIC, capacidade do ambiente de trabalho remoto e integridade dos *backups*.

4.2 ATIVOS DO PLANO DE CONTINGÊNCIA: São os recursos fundamentais que garantem o suporte à continuidade de negócio. Para isso, neste tópico, são mapeados os ativos que integram a infraestrutura necessária para a disponibilidade dos serviços de TIC e das atividades prioritárias, considerando a estrutura predial, dispositivos (*hardwares*) e sistemas (*softwares*).

Em um imóvel condominial, a responsabilidade pela infraestrutura predial compartilhada — como sistemas de combate a incêndio, segurança estrutural, proteção elétrica das áreas comuns e demais itens vinculados ao edifício — é da administração do condomínio, conforme previsto na convenção condominial. Cabe à Fundação zelar, acompanhar e demandar as providências necessárias para garantir que tais condições estejam adequadas e aderentes às exigências operacionais e legais.

4.2.1 Infraestrutura predial: Fundamental para garantir a continuidade das operações essenciais. Sua manutenção e cuidado asseguram condições adequadas para o funcionamento seguro e eficiente de equipamentos e processos críticos. Deve contemplar medidas para combate a incêndios, prevenção de alagamentos,

segurança física contra invasões ou roubos, climatização e proteção das instalações elétricas.

Em situações de contingência, quando o ambiente predial principal se torna indisponível, e, sendo o local secundário a residência dos dirigentes e colaboradores, exige-se que a infraestrutura suporte adequadamente o acesso remoto para a continuidade das atividades.

4.2.2 Sistema de energia elétrica: O fornecimento de energia elétrica é essencial para garantir o funcionamento das operações na sede, onde está localizada a infraestrutura de TIC primária e demais operações internas. A dependência de energia está diretamente associada ao funcionamento dos servidores locais, estações de trabalho, sistemas de comunicação, climatização e demais ativos operacionais.

O prédio sede, por não possuir geradores próprios ou fontes alternativas locais, depende da concessionária de energia e dos sistemas de suporte prediais disponibilizados pelo condomínio. Este ativo é considerado essencial, uma vez que falhas no fornecimento de energia impactam diretamente a continuidade dos processos operacionais, especialmente os que dependem da infraestrutura de TI local.

4.2.3 Ativos de comunicação de dados: O *data center* que sustenta a operação da rede de comunicação de dados é externo, operado por uma empresa especializada. Nele estão localizados os principais dispositivos computacionais responsáveis pelo armazenamento de dados, processamento e serviços centrais, como: *link* de internet externo; *firewall*; roteadores; *switches core*; servidores e *storage*.

Na sede encontram-se os equipamentos de conexão responsáveis pela distribuição e acesso à rede. Esses dispositivos interligam as atividades locais ao *data center* externo e suportam o tráfego de dados entre os usuários e os serviços centralizados. A comunicação é viabilizada por uma infraestrutura que inclui: anel e derivações de fibra óptica; *switches* de distribuição, *switches* de acesso; pontos de acesso w*i-fi*; cabeamento de rede; computadores, *notebooks*, *smartphones* e outros dispositivos (*endpoints*).

A manutenção da infraestrutura de rede é essencial para garantir a continuidade operacional. Esse processo envolve estratégias preventivas, como análises de especificações técnicas, processos de aquisição bem estruturados, monitoramento contínuo e substituição periódica de equipamentos críticos.

Os equipamentos de rede instalados na sede desempenham um papel fundamental, já que quaisquer falhas nesses componentes afetam diretamente o funcionamento global das operações internas. Devido à dependência da infraestrutura de TIC da sede, uma falha nos equipamentos centrais pode dificultar não apenas os trabalhos locais, mas também o acesso remoto e o funcionamento de serviços essenciais. Embora o *data center* externo forneça suporte para armazenamento e processamento de dados em situações emergenciais, ele depende de uma conexão funcional com a sede para operar plenamente como ponto de contingência.

Dessa forma, a robustez e a continuidade operacional demandam que tanto a infraestrutura interna quanto a comunicação com o *data center* externo sejam protegidas por medida preventivas, incluindo redundância de conexões, uso de *backups* sincronizados e planos de *failover* automáticos.

4.2.4 Sistemas e dados: Utiliza uma variedade de serviços de tecnologia da informação voltados para o suporte às suas funções administrativas e operacionais,

essenciais para a gestão dos benefícios previdenciários. A continuidade e eficiência desses serviços dependem de estratégias específicas que variam conforme o tipo de sistemas e o seu fornecedor. Os sistemas básicos de infraestrutura de rede, em geral, são disponibilizados por fabricantes de *hardware* ou adquiridos como soluções independentes. Já os sistemas voltados às atividades administrativas e operacionais são contratados de fornecedores especializados. A adoção de ações direcionadas para cada categoria de sistema é indispensável à continuidade, sem prejuízo das práticas gerais de manutenção e gestão da infraestrutura tecnológica.

4.2.4.1 Sistemas básicos de rede e infraestrutura: fundamentais para o funcionamento da infraestrutura de TIC, permitindo a operação contínua dos serviços administrativos e operacionais. Esses sistemas são responsáveis por garantir a conectividade e o gerenciamento de dados necessários à gestão previdenciária e podem ser classificados em três categorias:

a) Serviços de *hardware*: *softwares* necessários para o desempenho dos dispositivos físicos, como servidores e computadores. Incluem sistemas operacionais fornecidos por fabricantes ou obtidos como *softwares* livres;

b) Serviços de infraestrutura: sistemas destinados ao monitoramento da rede, segurança cibernética (*firewall*), *backups*, banco de dados e virtualização;

c) Serviços aos usuários: soluções acessadas diretamente pelas áreas administrativas e operacionais, como servidores de arquivos e sistemas de gestão.

4.2.4.2 Sistemas fornecidos por terceiros: os sistemas contratados podem ser instalados localmente, hospedados em servidores ou em nuvem. Sistemas locais dependem integralmente da infraestrutura de TIC da Fundação, enquanto os sistemas hospedados externamente exigem conectividade estável com a *internet*. Exemplos incluem:

a) Local: soluções para gestão financeira e contábil;

b) Servidores: soluções para gestão de documentos e arquivos, sistemas de *backup* e recuperação de desastres;
c) Nuvem: plataformas de comunicação e colaboração, sistemas de controle de acesso e ponto eletrônico, *google workspace*, *Microsoft 365*.

4.2.4.3 Dados: os dados coletados e processados pelos sistemas são ativos digitais para a operação. Esses dados, armazenados em bancos de dados e servidores de arquivos sustentam as atividades administrativas e operacionais relacionadas à gestão previdenciária. A segurança, integridade e disponibilidade dessas informações são essenciais para a operação e requerem mecanismos de proteção robustos, como *backups* regulares e monitoramento constantes.

4.2.5 Medidas preventivas: As medidas de prevenção abaixo listadas consideram apenas os eventos sobre os quais a Fundação julga ter gerência e possibilidade de mitigação. A responsabilidade por medidas de prevenção para eventos de desastres naturais, incêndios e falhas em serviços de eletricidade recai sobre terceiros.

Fatores humanos	
Atos de má-fé	Código de Ética e de Conduta, de conhecimento obrigatórios por dirigentes e colaboradores.
Erros e falhas ao seguir procedimentos de segurança	Divulgação de instruções de trabalho e comunicação proativa da TIC.
Epidemias ou outros riscos de saúde	
Surtos de doenças contagiosas	Prover informações e incentivos para campanhas de vacinação públicas.
Acesso remoto para situações de contingência	

Rede privada virtual (VPN)	Permissão de acesso seguro aos sistemas internos da Fundação a partir de locais remotos.
Infraestrutura de TIC na nuvem	Hospedagem de sistemas essenciais em servidores *cloud* para garantir disponibilidade.
Dispositivos móveis corporativos	*Notebooks* ou *tablets* configurados para trabalho remoto.
Suporte técnico remoto	Equipe capacitada para resolver problemas à distância.

4.3 PLANO DE CONTINGÊNCIA OPERACIONAL – PCO: é um conjunto de cenários de inoperância previamente definidos e respectivos procedimentos alternativos planejados para manter a continuidade das atividades prioritárias. Inserido no PCO, o Plano de Recuperação de Desastres – PRD é um conjunto de cenários de desastre (incidente maior com interrupção de negócios) previamente definidos e de respectivos procedimentos de reação, estruturados para possibilitar que as atividades prioritárias retomem o nível de operação dentro de prazo tolerável. Abaixo as ações que deverão ser seguidas a fim de mitigar os riscos dos seguintes eventos disruptivos:

- **Falha no *firewall***

Responsável: Diretoria de Administração e Equipe de TIC

Contatos internos: TIC da RS-Prev (Bruno Mendonça - informatica@rsprev.com.br), andressa-manczak@rsprev.com.br e Rafael Rocha Luzardo (rafael-luzardo@rsprev.com.br).

Contatos externos: Suporte da INTELINOVE (chamados@intelinove.com.br).

Objetivo: Proteger a rede corporativa contra ataques cibernéticos, acessos não autorizados e proporcionar a disponibilidade de serviços críticos por meio da configuração, monitoramento e manutenção do *firewall*.

O que fazer: Analisar qual falha está ocorrendo e se for critico ou relacionado ao Hardware, solicitar um novo equipamento e realizar o *restore* das configurações.
Antes do incidente: a) realizar *backups* automáticos e monitorar *logs* regularmente; b) atualizar frequentemente a política de segurança e *patches* do *firewall.*
Durante o incidente: isolar a ameaça e acionar o suporte técnico.
Após o incidente: revisar políticas de segurança, aplicar *patches* e atualizar os registros do plano.

- **Falha em equipamento crítico de TIC**

Responsável: Diretoria de Administração e Equipe de TIC
Contatos internos: TIC da RS-Prev (Bruno Mendonça - informatica@rsprev.com.br), Andressa Manczak (andressa-manczak@rsprev.com.br) e Rafael Rocha Luzardo (rafael-luzardo@rsprev.com.br).
Contatos externos: Se houver, acionar a garantia com a empresa.
Objetivo: Buscar o funcionamento contínuo dos ativos de TIC, minimizando os impactos de falhas e maximizando a disponibilidade por meio de inspeções regulares, manutenções corretivas e preventivas.
O que fazer: Analisar qual a falha e se houver acionar a garantia do equipamento, e/ou procurar reparar a máquina e usar máquinas backups.
Antes do incidente: a) monitorar os ativos de TIC para detectar falhas antes de tornarem-se problemas graves; b) realizar manutenções preventivas.
Durante o incidente: diagnosticar o problema, substituir componentes defeituosos e restaurar o funcionamento de equipamentos.
Após o incidente: inspecionar os equipamentos, registrar as ações tomadas e atualizar o plano de manutenção preventiva.

- **Falha em servidor crítico de TIC**

Responsável: Diretoria de Administração e Equipe de TIC

Contatos internos: TIC da RSPREV (Bruno Mendonça - informatica@rsprev.com.br), Andressa Manczak (andressa-manczak@rsprev.com.br) e Rafael Rocha Luzardo (rafael-luzardo@rsprev.com.br).

Contatos externos: Suporte ao Cliente - SC1 (sc1@procergs.rs.gov.br).

Objetivo: Gerenciar e manter servidores, redes e sistemas de TIC para propor a continuidade dos serviços, a segurança dos dados e a disponibilidade dos sistemas essenciais.

O que fazer: Analisar a falha e a depender do problema critico solicitar a empresa acesso a um novo servidor com as mesmas características do anterior.

Antes do incidente: realizar manutenção preventiva dos servidores e redes, realização de *backups* regulares e monitoramento contínuo.

Durante o incidente: Diagnosticar a falha no servidor ou na rede, ativar redundância e realizar a recuperação do sistema.

Após o incidente: Validar a restauração do serviço e monitorar os sistemas para garantir estabilidade.

- **Falta de acesso ao sistema de folha de pagamentos**

Responsável: Diretoria de Administração

Contatos internos: Ana Paula Morfan (ana-morfan@rsprev.com.br), Rafael Rocha Luzardo (rafael-luzardo@rsprev.com.br), Andressa Manczak (andressa-manczak@rsprev.com.br) e Elisangela Hesse (elisangela-hesse@rsprev.com.br).

Contatos externos: PRP – Mayara Lopes (mayara.lopes@prpsolucoes.com.br), Cristiane Rosa (cristiane.rosa@prpsolucoes.com.br), José Antônio Prattes (jose.antonio@prpsolucoes.com.br).

Objetivo: Promover a continuidade do processamento e pagamento dos salários e benefícios durante a indisponibilidade do sistema de folha de pagamento, adotando soluções alternativas e ações de contingência para minimizar os impactos operacionais.

O que fazer: Contatar os responsáveis pelo sistema.

Antes do incidente: a) viabilizar que a equipe possa acessar o sistema por meio de VPN e máquinas virtuais a partir de qualquer local com internet; b) manter um canal direto com a empresa terceirizada para notificar falhas e solicitar exportações manuais de dados, se necessário; c) armazenar periodicamente relatórios resumidos com dados de pagamento em um ambiente seguro e acessível (*OneDrive*), como medida emergencial para cálculos manuais.

Durante o incidente: coordenar com a empresa terceirizada e utilizar dados locais ou *backups* para emergências.

Após o incidente: atualizar os registros, inclusive em sistema.

- **Indisponibilidade do sistema financeiro e paralisação do expediente financeiro**

Responsável: Diretoria de Administração e Diretoria de Investimentos

Contatos internos: Rafael Luzardo (rafael-luzardo@rsprev.com.br), Sibeli Monteiro Pereira (sibeli-pereira@rsprev.com.br), Filipe Jeffman dos Santos (filipe-santos@rsprev.com.br).

Contatos externos: Agencia Banrisul (ag_central_pjuridica@banrisul.com.br).

Gerentes de conta Banrisul: Eliara Kaminski (eliara_kaminski@banrisul.com.br); Ivolmar luttjohann Jacques ((51) 99610-1448, ivolmar_jacques@banrisul.com.br); Agencia Caixa Econômica Federal (ag2822rs06@caixa.gov.br); Gerente de conta Caixa Econômica Federal (Filipe Caurio (51) 99466-7340).

Objetivo: Propor a continuidade das operações financeiras críticas em caso de falha sistêmica, indisponibilidade de rede ou ausência de pessoal-chave, garantindo o cumprimento de pagamentos, remessas, devoluções, atualizações em sistemas e comunicação com as partes interessadas.

O que fazer:

Antes do incidente: a) manter *backup* atualizado e seguro das obrigações financeiras, registro e relatórios operacionais, em planilhas locais e na nuvem (*OneDrive*), com acesso controlado; b) estabelecer fluxo manual para consolidação de pagamentos

com base nesses registros; c) manter equipamentos com dispositivos de segurança bancários atualizados.

Durante o incidente: a) verificar documentação de pagamentos *online*, operacionalizar resgates/aplicações dos investimentos; b) efetuar os pagamentos e c) registrar em controle manuais (planilhas).

Após o incidente: atualizar os registros, inclusive em sistema.

- **Dificuldades de acesso a sistemas para arrecadação de contribuições**

Responsável: Diretoria de Seguridade

Contatos internos: Elisângela Hesse (eliangela-hesse@rsprev.com.br); Kelly Cristina Lippert (kelly-lippert@rsprev.com.br); Evelyne Thamara Kunrath (evelyne-kunrath@rsprev.com.br).

Contatos externos: Coordenador do Comitê Gerencial do RHE - Paulo Ricardo da Silveira Hoff – Procergs (paulo-hoff@procergs.rs.gov.br - 0800 648 48 48).

Objetivo: Adotar medidas para sustentar a continuidade das atividades de arrecadação, minimizando os impactos no fluxo de caixa.

O que fazer:

Antes do incidente: a) viabilizar que a equipe possa acessar o sistema por meio de VPN e máquinas virtuais a partir de qualquer local com internet; b) preparar planilhas locais ou em nuvens (O*neDrive*) para registro temporário das contribuições e c) alinhar com patrocinadores o envio de dados em planilhas físicas.

Durante o incidente: receber dados dos patrocinadores, registrar manualmente as contribuições e manter controle rigoroso das operações.

Após o incidente: reconciliar os dados manuais com os sistemas oficiais e ajustar os registros para evitar inconsistências.

- **Risco de inadimplência fiscal devido à indisponibilidade de sistemas**

Responsável: Diretoria de Seguridade

Contatos internos: Elisângela Hesse (elisangela-hesse@rsprev.com.br); Kelly Cristina Lippert (kelly-lippert@rsprev.com.br); Evelyne Thamara Kunrath (evelyne-kunrath@rsprev.com.br).

Contatos externos: Sócio-Diretor da PRP Soluções - Jaques Callegaro (jaques.callegaro@prpsolucoes.com.br , 51 3085-6161).

Objetivo: Adotar medidas para propor a continuidade das atividades relacionadas à preparação, transmissão e validação das declarações fiscais, como EFD-Reinf e e-Financeira, mesmo em cenários de indisponibilidade temporária da rede corporativa, de modo a mitigar riscos de atrasos no cumprimento das obrigações fiscais e preservar a conformidade regulatória.

O que fazer:

Antes do incidente: a) viabilizar que a equipe possa acessar o sistema por meio de VPN e máquinas virtuais a partir de qualquer local com internet; b) utilizar *backups* locais e em servidores externos para armazenar relatórios críticos, como os de eventos tributáveis, resgates e contribuições, garantido acesso mesmo sem a rede corporativa; c) em caso de indisponibilidade prolongada, acionar a consultoria contratada para assumir temporariamente a geração e envio das declarações fiscais.

Durante o incidente: solicitar que a consultoria contratada assuma funções críticas, como a transmissão de dados e validação de declarações fiscais.

Após o incidente: a) validar as declarações e relatórios processados externamente, integrando-os ao sistema corporativo.

- **Prejuízo à gestão da conformidade e ao controle documental**

Responsável: Diretoria Presidência e Equipe de TIC

Contatos internos: Elisângela Hesse (elisangela-hesse@rsprev.com.br); Miréia Nicolini Gomes (mireia-nicolini@rsprev.com.br); Bruno Mendonça Toledo Silva (informatica@rsprev.com.br).

Contatos externos: Luiz Fernando Vale Cunda - Canal de Suporte ao Cliente da Procegs (sc1@procergs.rs.gov.br, 0800 648 48 48).

Objetivo: Implementar mecanismos que viabilizem a continuidade das atividades de conformidade documental dos colegiados, mesmo em situações de indisponibilidade dos sistemas ou de acesso restrito aos registros eletrônicos.

O que fazer:

Antes do incidente: a) viabilizar que a equipe possa acessar o sistema por meio de VPN e máquinas virtuais a partir de qualquer local com internet; b) utilização de *backup* regular para garantir a preservação das informações críticas, como termos de posse e registros de mandatos.

Durante o incidente: utilizar documentos físicos e registros manuais para continuidade do controle de mandatos e certificações, comunicando prontamente eventuais atrasos aos dirigentes.

Após o incidente: atualizar o arquivamento de documentos e sistemas de controle.

- **Indisponibilidade de rede ou internet em reuniões de colegiados, por períodos prolongados**

Responsável: Diretoria Presidência

Contatos internos: Elisângela Hesse (elisangela-hesse@rsprev.com.br); Miréia Nicolini Gomes (mireia-nicolini@rsprev.com.br).

Contatos externos: Presidente do Conselho Deliberativo - José Guilherme Kliemann, (jose-kliemann@ipe.rs.gov.br, 51 99550-2632) e Presidente do Conselho Fiscal - Fernando Boklis (fernando-boklis@planejamento.rs.gov.br, 51 99968-4871).

Objetivo: viabilizar a continuidade das reuniões e o registro das atas de forma eficaz, mesmo na ausência de acesso à internet ou à rede corporativa, seja no dia da reunião ou durante períodos prolongados de desconexão.

O que fazer:

Antes do incidente: a) assegurar que todos os documentos críticos para as reuniões estejam acessíveis em plataformas de nuvem (O*neDrive*) e *backups off-line*; b) promover redundância de contratos de acesso à internet.

Durante o incidente: promover a condução das reuniões presenciais ou por meios alternativos e registrar as atas *off-line*.

Após o incidente: atualizar arquivamento de documentos e restaurar as atas digitais, integrando-as aos sistemas de armazenamento da Fundação assim que a rede for restaurada.

- **Indisponibilidade da sede e ferramentas de TIC na condução das operações de caixa (investimentos) e ataque cibernético**

Responsável: Diretoria de Administração

Contatos internos: Ana Paula Morfan (ana-morfan@rsprev.com.br), Rafael Rocha Luzardo (rafael-luzardo@rsprev.com.br), Andressa Manczak (andressa-manczak@rsprev.com.br) e TIC da RS-Prev (Bruno Mendonça - informatica@rsprev.com.br).

Contatos externos: Fundação Atlântico - Hélio Monteiro ((21) 96817-7966), Síndico do Prédio - Luiz Vencato ((51) 99936-2828).

Objetivo: sustentar a continuidade operacional, mesmo em cenários de comprometimento dos sistemas, e preservar a segurança dos dados críticos.

O que fazer: Se os sistemas forem em sites, poderá ser realizado remotamente sem que ocorra algum impacto. Se forem sistemas locais, se o prédio possuir energia também poderá ser feito remotamente sem haver impactos. Se houver ataques cibernéticos procurar contato com a empresa responsável pelo sistema.

Antes do incidente: a) utilizar *backups off-line* atualizados para recuperação de dados críticos; b) treinar a equipe de TIC para atuar em condições de contingência manual; c) em caso de incidente que envolvam violação de segurança, especialmente aqueles relacionados a dados pessoais, como acessos não autorizados, vazamentos, perdas, destruição, alteração ou qualquer forma de tratamento

inadequado ou ilícito, que possam gerar riscos aos direitos dos titulares e impactos à operação ou à reputação institucional, seguir o Plano de Resposta a Incidentes de Segurança (PRIS).

Durante o incidente: conter o ataque, isolar os de sistemas comprometidos e ativação de procedimentos manuais.

Após o incidente: atualizar sistemas, validar a integridade dos dados e revisar as medidas de segurança.

5 REFERÊNCIAS

5.1 Gerenciamento de Continuidade de Negócios na Administração Pública – Fundação Escola Nacional de Administração Pública – ENAP

5.2 Gestão de Continuidade de Negócios – *Global Technology Audit Guide (GTAG)*

5.3 Guia de Boas Práticas para Planos de Continuidade de Negócios – ABRAPP

5.4 Guia de Resposta a Incidentes de Segurança – Programa de Privacidade e Segurança da Informação – Ministério da Gestão e da Inovação em Serviços Públicos

5.5 Norma ABNT NBR ISO 22301.

5.6 Norma ABNT NBR ISO 22313.

5.7 Norma ABNT NBR ISO 22317.

5.8 Resolução MPAS/CGPC nº 13/2004.

6 DISPOSIÇÕES FINAIS

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