P O R T A R I A Nº 203/2024/ ANGRAPREV

A DIRETORA - PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA SOCIAL DO MUNICÍPIO DE ANGRA DOS REIS – ANGRAPREV, no uso da atribuição que lhe confere o Anexo I, Inciso I, alínea "l", da Lei nº 4037, de 21 de Dezembro de 2021, e considerando os despachos exarados nos autos do Processo Administrativo nº 2024033403 do Instituto de Previdência Social do Município de Angra dos Reis - ANGRAPREV, 16 de Setembro de 2024,

R E S O L V E :

APOSENTAR a servidora **SANDRA SUELI FERNANDES,** Médica, Matrícula 7022, Referência 2000, Padrão I, do Grupo Funcional da Saúde, da Parte Permanente da Prefeitura Municipal de Angra dos Reis, com base no Artigo 19 da Lei Complementar nº 014, de 21 de dezembro de 2021, com redação dada pela Lei Complementar nº 016 de 23 de agosto de 2022 e pela Lei Complementar nº 021, de 19 de dezembro de 2023.

REGISTRE - SE, PUBLIQUE-SE E CUMPRA-SE

MUNICÍPIO DE ANGRA DOS REIS, 11 DE OUTUBRO DE 2024

LUCIANE PEREIRA RABHA
DIRETORA - PRESIDENTE

P O R T A R I A Nº 204 /2024/ ANGRAPREV

DISPÕE SOBRE O PLANO DE RECUPERAÇÃO DE DESASTRES EM TECNOLOGIA DA INFORMAÇÃO E DÁ OUTRAS PROVIDÊNCIAS.

A DIRETORA-PRESIDENTE DO INSTITUTO DE PREVIDÊNCIA SOCIAL DE ANGRA DOS REIS - ANGRAPREV, no uso de suas atribuições legais,

R E S O L V E :

Art. 1º - Ficam aprovadas as normas de procedimentos referentes ao Plano de Recuperação de Desastres em Tecnologia da Informação a serem implementadas no âmbito do ANGRAPREV, nos termos do regulamento que passa a integrar a presente Portaria.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação, revogadas as disposições em contrário.

REGISTRE - SE, PUBLIQUE-SE E CUMPRA-SE

MUNICÍPIO DE ANGRA DOS REIS, 14 DE OUTUBRO DE 2024

LUCIANE PEREIRA RABHA
DIRETORA- PRESIDENTE

1. INTRODUÇÃO E CONCEITUAÇÃO

O ANGRAPREV têm a necessidade de utilização de um sistema de informação, seja para auxílio no gerenciamento dos processos de negócio ou até mesmo para auxiliar nas tomadas de decisões. Por este motivo, o instituto passa cada vez mais a ser dependente desses sistemas, tendo a responsabilidade de assegurar a disponibilidade do mesmo, tanto para manter os processos sempre disponíveis quanto para prestação de serviços críticos para os segurados.

Incidentes, falhas e sinistros podem acontecer com qualquer órgão público a qualquer momento, e como resultado, podem parar todas as operações de negócio por horas ou dias, ocasionando uma possível perda de receita (investimentos) e produtividade, com impacto negativo na confiança dos segurados do RPPS. Ter um plano de ação em TI caso aconteça qualquer interrupção - seja ela causada por hackers, incêndio, falta de energia, desastre natural ou outro tipo de crise -, é extremamente importante para manter a confiabilidade e a rentabilidade de qualquer negócio.

O ANGRAPREV não possui um Plano de Recuperação de Desastres (PRD), e, atualmente isto é indispensável para que os processos críticos da entidade não fiquem indisponíveis, mantendo a normalidade das operações. Todos os processos de negócios do ANGRAPREV são gerenciados através de um único Enterprise Resource Planning (ERP), compras, investimentos, dados dos segurados e fornecedores, estoque, chamados e outros processos e, caso venha a ocorrer algum tipo de desastre, o instituto não possui nenhum plano estratégico para disponibilizar rapidamente o ERP de forma que não prejudique o seu funcionamento. Melhor dizendo, se o ERP para o ANGRAPREV também para.

Acredita-se que com a implementação de um Plano de Recuperação de Desastres - PRD e seus devidos testes e treinamentos, o mesmo possui a capacidade de minimizar efetivamente as consequências negativas de um desastre se aplicado corretamente.

A elaboração de um PRD é um meio o qual traz uma estratégia de recuperação pronta para o ANGRAPREV no momento em que um incidente gere uma interrupção do funcionamento, seja qual for o

caráter deste incidente, natural, propositalou mesmo acidental.

2. OBJETIVOS

O objetivo geral da aplicação de um PRD com foco no ERP, no âmbito do ANGRAPREV, visa a redução dos efeitos resultantes de qualquer interrupção dos processos, garantindo o retorno da operação no menor tempo possível. Para que esse objetivo seja alcançado, estão sendo criados os seguintes objetivos específicos: estudar normas de TI; descrever Sistema de Gestão de Segurança da Informação (SGSI); explicar Gestão de Riscos; conceituar Plano de Continuidade de Negócios (PCN) e Plano de Recuperação de Desastres (PRD); avaliar estratégias de continuidade e; apresentar a aplicação do PRD.

3. REFERENCIAL TEÓRICO

Aqui são apresentados os embasamentos teóricos referente a esta Portaria, sendo eles: normas de TI, SGSI, gestão de riscos, PCN, PRD e estratégias.

3.1. NORMAS DE TECNOLOGIA DA INFORMAÇÃO

Esta Portaria tem a finalidade de harmonizar um conjunto de melhores práticas, levando em consideração estudos, históricos e conhecimentos operacionais, e deve ser aplicada para objetivos específicos. O ANGRAPREV tem o dever de determinar as melhores práticas que devem ser aplicadas (ABNT NBR ISO/IEC 27002, 2013).

Na Figura 1 são apresentadas algumas normas brasileiras e também do National Institute of Standards and Technology (NIST), ambas com relações a TI e que servirão de apoio no desenvolvimento do projeto, tanto para análises quanto para a elaboração do PRD.

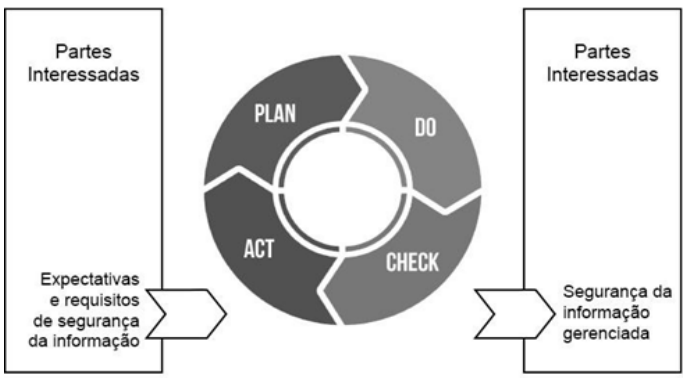
Figura 1 - Principais normas relacionadas a TI

a) ABNT NBR ISO 31000 (2018): estabelece princípios e orientações genéricas sobre gestão de riscos;
b) ABNT NBR ISO/IEC 22301 (2020): está relacionada a gestão da continuidade de negócios e é relevante a todos os modelos e tamanhos de organizações que tem como objetivo estabelecer, implementar, manter e melhorar o sistema de informação;
c) ABNT NBR ISO/IEC 27001 (2013): especifica requisitos para a implementação de controles de segurança adaptados para as necessidades específicas de organizações ou suas partes;
d) ABNT NBR ISO/IEC 27002 (2013): estabelece um guia prático para desenvolver os procedimentos necessários de segurança da informação e práticas de gestão da segurança da informação;
e) ABNT NBR ISO/IEC 27005 (2019): oferece as melhores práticas para o processo de gestão de riscos de uma organização, tratando particularmente os requisitos de um SGSI;
f) NIST SP 800-30 (2012): oferece orientações para a realização de avaliação de riscos dos sistemas de informação e organizações;
g) NIST SP 800-34 (2010): fornece orientações, recomendações e considerações para a contingência dos sistemas de informações;
h) NIST SP 800-37 (2018): apresenta diretrizes para execução do quadro de gestão de riscos para sistemas de informação com o objetivo de prover instruções para a realização das atividades de categorização, seleção, controle, implementação, avaliação, autorização e monitoramento dos controles de segurança.

3.2. SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

A norma ABNT NBR ISO/IEC 27001 descreve que a adoção de um SGSI deve ser uma decisão estratégica para uma organização, visto que a especificação e a implementação são influenciadas pelas suas necessidades e objetivos. É recomendável que a implementação de um SGSI seja escalonada conforme as necessidades da organização, por exemplo, um cenário simples exige uma solução de um SGSI simples (ABNT NBR ISO/IEC 27001, 2013). A norma, responsável por providenciar um modelo completo que trata desde o princípio até a melhoria contínua de um SGSI, faz a utilização da metodologia Plan-Do-Check-Act (PDCA), que é aplicada para estruturar todos os processos do SGSI.

Figura 2 - Plan-Do-Check-Act (PDCA)



Fonte: Adaptado de ABNT NBR ISO/IEC 27001 (2013).

O ANGRAPREV, em busca de soluções de segurança da informação, deve seguir as diretrizes das normas nacionais e internacionais, projetar um SGSI de acordo com seus requisitos, aprovar a gestão e implementá-lo com ajuste contínuo para torná-lo efetivo no atendimento dos desafios dinâmicos de segurança e conformidade.

3.3. GESTÃO DE RISCOS

Para identificar as necessidades do ANGRAPREV em relação aos requisitos de segurança da informação e para criar um SGSI que seja eficaz, é necessária uma abordagem sistemática de gestão de riscos de segurança da informação (ABNT NBR ISO/IEC 27005, 2019).

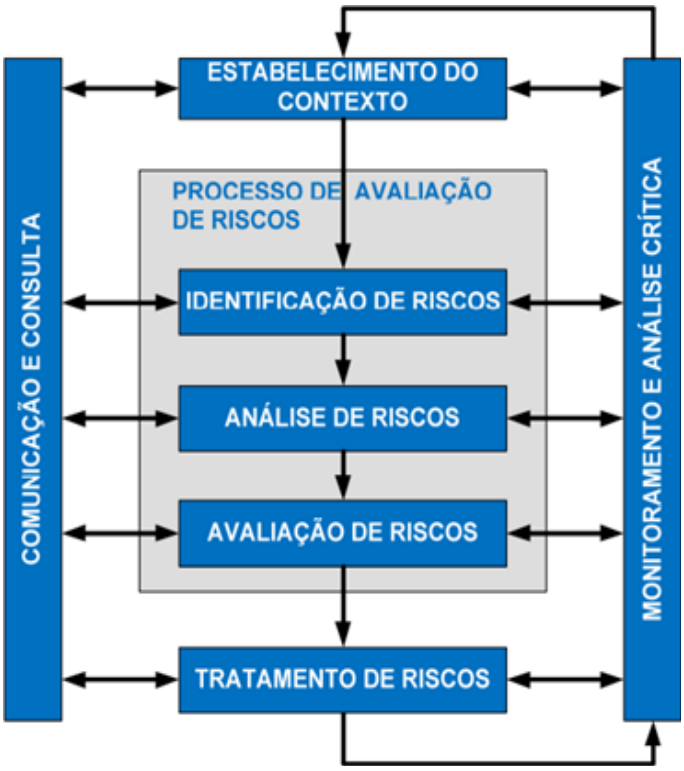
Figura 3 - Diagrama de equação do risco de segurança da informação

Conforme visto na Figura 3, o risco é a hipótese de que as ameaças explorem as vulnerabilidades, causando impactos aos negócios. Esses impactos podem ser limitados por medidas de segurança, responsável pela proteção dos ativos, impedindo ou dificultando que as ameaças explorem as vulnerabilidades, diminuindo, assim, o risco.

De um modo geral, a gestão de riscos é um método voltado para o controle dos riscos e abrange um conjunto de atividades específicas que tem como objetivo garantir a boa governança, sem que os riscos e surpresas indesejáveis atrapalhem seus objetivos e metas.

A gestão de riscos é composta por sete etapas, conforme Figura 4.

Figura 4 - O processo de gestão de riscos



3.4. PLANO DE CONTINUIDADE DE NEGÓCIOS

Espera-se que os responsáveis pela gestão do ANGRAPREV e em especial de TI, tenham a devida atenção aos ativos críticos, que servem de base de suporte da entidade.

Consequentemente, pensar em como assegurar a continuidade dos serviços em caso de algum evento que interrompa a operação de um ou mais processos de negócio, se torna uma tarefa essencial para a gestão da segurança da informação.

O foco está em garantir a continuidade dos processos e informações cruciais para a sobrevivência da entidade, no menor tempo possível, com o objetivo de minimizar os efeitos resultantes de um desastre.

O PCN é um processo, cujo planejamento tem como objetivo assegurar que o ANGRAPREV resista a um desastre ou qualquer atividade imprevista que provoque danos aos ativos críticos, pondo em risco qualquer processo de negócio. De acordo com a norma NIST SP 800-34, o plano pode ser elaborado englobando somente os processos críticos do negócio ou pode compor todos os processos do ANGRAPREV (NIST SP 800-34, 2010).

A metodologia a ser adotada no PCN pode pressupor a criação e administração de planos específicos, sendo eles: Plano de Contingência Operacional (PCO), Plano de Administração de Crises (PAC) e PRD. O PRD, em específico, trata-se de procedimentos

previamente definidos para cenários de desastres, ou seja, conjunto de procedimentos para garantir que as atividades críticas retornem à operação dentro do prazo preestabelecido após a ocorrência de um desastre.

3.5. **PLANO DE RECUPERAÇÃO DE DESASTRES**

O PRD é um plano de ação, que tem como principal objetivo restaurar, no menor tempo possível e mesmo com desempenho reduzido, os serviços de TI que sustentam os processos críticos da entidade. A preparação é a peça-chave para um PRD bem-sucedido, por isso é preciso desenvolver uma documentação que abrange ações bem planejadas a serem adotadas antes, durante e após um desastre.

O plano é acionado após o acontecimento de um desastre, podendo ser voluntário (hackers, incendiários etc.), involuntário (acidentes, falta de energia etc.) ou natural (terremotos, enchentes, incêndios naturais etc.).

Conforme citado no Item3.4, o PCN apresenta uma abordagem completa para o ANGRAPREV, assegurando desde um grande desastre - um incêndio, por exemplo -, até problemas com fornecedores. Já no planejamento do PRD, somente alguns itens críticos foram levados em consideração, tendo como exemplo este projeto, o servidor de banco de dados e da aplicação do ERP do ANGRAPREV.

A norma NIST SP 800-37 (2018), descreve o PRD como um plano de informação do sistema com foco projetado para restaurar a funcionalidade do sistema, aplicação ou infra estrutura de instalação de computadores em um site alternativo após uma emergência, e complementa informando que se aplica a grandes rupturas, geralmente físicas, para os serviços que negam o acesso a infra estrutura de instalação principal para um período prolongado.

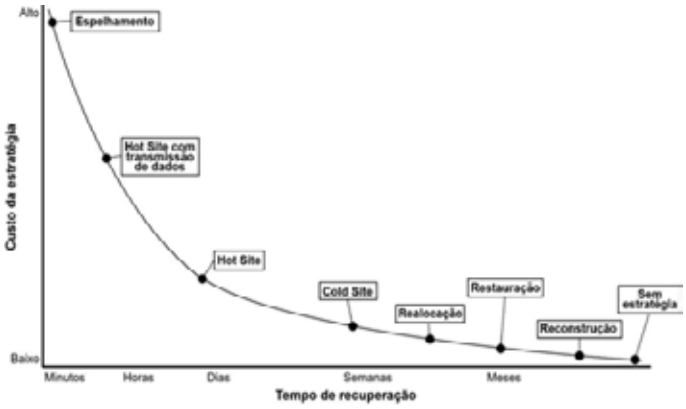
3.6. **ESTRATÉGIAS DE CONTINUIDADE**

Conforme a norma NIST SP 800-34, a estratégia de recuperação é desenvolvida através da análise dos resultados obtidos da avaliação de riscos e fornece direção na maneira com que a estratégia de continuidade possa ser executada (NIST SP 800-34, 2010).

A Diretoria de TI, define e orienta a escolha das múltiplas estratégias para a recuperação dos processos e componentes de negócio, dentro dos prazos de recuperação definidos. Com a possibilidade de múltiplas combinações e cada uma com seus benefícios, é difícil agradar todos os gestores, isto é, não existe uma solução correta nem errada, o responsável pelo PCN deve comparar os fatores existentes e o nível de risco que a organização está disposta a correr. As estratégias mais satisfatórias são aquelas que tem a melhor relação custo X benefício, são as que reduzem os riscos e exposições e que também atendem às exigências do negócio e não só de TI.

Independente da estratégia escolhida, o objetivo final deve ser o mesmo, garantir uma recuperação eficiente dos processos de negócio da empresa de acordo com a análise obtida na gestão de riscos e seu tipo de negócio. Na Figura 5, são apresentadas algumas das estratégias de continuidade existentes, levando em consideração o tempo de restauração e o custo.

Figura 5 – Custo da estratégia X tempo de recuperação



4. **METODOLOGIA**

Aqui está apresentado toda a metodologia que se fez necessária para a elaboração de um Plano de Recuperação de Desastres focado no ERP do ANGRAPREV.

4.4. ETAPAS

De acordo com o PRD proposto, serão aplicadas somente no servidor DE BANCO DE DADOS AS ETAPAS APRESENTADAS ABAIXO:

4.4.1 CARACTERIZAÇÃO DO ATIVO

A caracterização do ativo é o passo inicial e é tão importante quanto os outros, pois permite identificar as limitações, recursos e informações do ativo. O responsável de TI deve disponibilizar as seguintes informações: informações de hardwares e softwares; usuários que fazem uso do ativo; missão do ativo, descrevendo os processos realizados pelo mesmo; sensibilidade e criticidade do ativo; políticas de segurança; controles operacionais; e relatórios (NIST SP 800-30, 2012). Conforme apresentado no Quadro 1.

Quadro 1 - Caracterização do ativo

CARACTERIZAÇÃO DO ATIVO	
IDENTIFICAÇÃO	**MANAGER**
Missão	Hospedar o banco de dados e prover acesso Ao ERP da organização
Usuários ativos	Em média 40 usuários simultâneos
Monitoramento de uso	Através da ferramenta Zabbix,gerenciado Por empresa terceirizada
Responsáveis pela manutenção e suporte	DBA e Analista de TI
Controle de acesso	Permissões de acordo com os níveis de Acesso por usuário
Consequências do ativo para aorganização	Afeta todos os processos
Registros de incidentes ocorridos anteriormente	Não é feito relatório, porém nunca ocorreu
Procedimentos documentados de operação, manutenção e suporte	Não existe nada documentado
Formato de operações da manutenção e alteração	Não existe nada documentado
Seguro contra roubo,furto,incêndio ou desastre natural	Sim
Treinamento para administradores e usuários	Não
Criticidade	Muitoalta
Sensibilidade	Muitoalta
Proprietário	Diretoria deTI
Sos executados	Por se tratar do ERP, é responsável por Executar todos os processos da organização
Informações de hardware	DellPower EdgeR630, 2 processadores Intel XeonE5-2670v32.30GHz, 64GBRAM,2x SSD 960GB e 6xHD 480GB

4.4.2. IDENTIFICAR AS AMEAÇAS

Para essa etapa, é necessário reunir dados obtidos através de análises e relatórios de incidentes, dos responsáveis pelo ativo ou dos usuários, de catálogos externos de ameaças, dentre outros documentos, com o objetivo de levantar informações que indiquem potenciais ameaças para o ativo. Deve-se também coletar informações que podem apontar prováveis ameaças relativas ao ativo que não haviam sido identificadas até o momento (ABNT NBR ISO/IEC 27005, 2019).

É fundamental classificar as ameaças e a probabilidade da existência dela para o ativo, de acordo com o apresentado na Tabela 1.

Tabela 1 - Classificação das ameaças

Categoria	**Classificação de Existência**		
Humanas/Ambientais/Naturais	**Muito baixa**	**Moderada**	**Muito alta**
Falha não intencional		X	
Falha de hardware		X	
Falha de software		X	
Falha de conectividade		X	
Falha de fornecimento de energia		X	
Falha no controle de temperatura		X	
Terrorismo cibernético			X
Espionagem		X	
Sabotagem		X	
Atividade criminosa–Roubo de dados			X
Queda de raios		X	
Fogo		X	
Infestação de pragas/insetos	X		

Fonte: Adaptado de NIST SP 800-30 (2012).

4.4.3. IDENTIFICAR AS VULNERABILIDADES

Com a finalização da identificação das ameaças, é importante elaborar uma tabela das possíveis vulnerabilidades, capazes de afetar diretamente os serviços da organização, conforme apresentado no Quadro 2.

Quadro 2: Identificação de Vulnerabilidades

Ameaça	**Vulnerabilidade**	**Comentário**
Falha não intencional	Falta de treinamento para analistas	Funcionários não recebem treinamento
Falha de hardware	Falta de peças de reposição,equipamento sem garantia ou fora de linha do fabricante	Nunca houve ocorrência
Falha de software	Falta de aplicação de atualizações	Nunca houve ocorrência

Falha de conectividade	Falta de equipamentos de rede reservas para substituição em caso de falhas	Em caso de falta, a comunicação com o servidor será perdida
Falha de Fornecimento de energia	Falta de energia ou nobreak com autonomia reduzida	Caso a energia não volte até 1 hora, será necessário o desligamento do ativo
Falha no controle de temperatura	Queima de ar-condicionado	Em caso de falha,existe um ar-condicionado redundante
Terrorismo cibernético	Falta de especialista em firewall	Tentativas de ataques e acessos não autorizados
Espionagem	Acessoremoto concedido para Terceiros responsáveis pela manutenção	Acessos não monitorados
Sabotagem	Funcionários com privilégios avançados	Número de administradores elevado
Atividade criminosa - Roubo de dados	Extração de dados confidenciais	Roubo de dados pelos funcionários ou criminosos
Queda de raios	Falha no supressor de surto	Raios podem provocar oscilações que causem danos
Fogo	Combate a incêndio feito manualmente	Não possui sistema automático de combate a incêndios,somente detector de fumaça e temperatura
Infestação de pragas/insetos	Falta de dedetização	Nunca houve ocorrência

Fonte: Adaptado de NIST SP 800-30 (2012).

4.4.4. DETERMINAR AS PROBABILIDADES

O objetivo desta etapa é realizar a classificação das probabilidades de explorar as potenciais ameaças através das vulnerabilidades identificadas para o ativo na etapa anterior. Portanto, deve-se montar uma tabela para classificar as probabilidades como muito baixa, baixa, moderada, alta e muito alta, conforme apresentado na Tabela 2.

Quadro 2: Identificação de vulnerabilidades

Ameaça	**Vulnerabilidade**	**Probabilidade**				
		Muito baixa	**Baixa**	**Moderada**	**Alta**	**Muito alta**
Falha nãointencional	Falta de treinamento paraanalistas				X	
Falha de hardware	Falta de peças de reposição, Equipamentos em garantia ou fora de linha do fabricante		X			
Falha de software	Falta de aplicação deatualizações		X			
Falha de conectividade	Falta de equipamentos de rede reservas para substituição em caso defalhas		X			
Falha de fornecimento de energia	Falta de energia ou nobreakcom autonomia reduzida				X	
Falha no controlede temperatura	Queima de ar-condicionado		X			
Terrorismo cibernético	Falta de especialista emfirewall				X	
Espionagem	Acesso remoto concedido-Para terceiros responsáveis pela manutenção			X		
Sabotagem	Funcionários com privilégiosavançados		X			
Atividade criminosa–Roubode dados	Extração de dados confidenciais		X			
Queda de raios	Falha no supressor de surto		X			
Fogo	Combate a incêndio feitomanualmente		X			
Infestação depragas/insetos	Falta de dedetização	X				

Fonte: Adaptado de NIST SP 800-30 (2012).

4.4.5. ANÁLISE DE IMPACTOS

O objetivo da análise de impacto é mostrar os eventos negativos que podem levar a danos ou perdas dos recursos de informação, proporcionando ao ANGRAPREV margem de impacto em alguns casos. Portanto, é necessário conduzir uma avaliação combinada

de ameaças, vulnerabilidades e impactos, identificar aspectos relevantes e determinar onde aplicar esforços para eliminar ou reduzir as probabilidades de ameaças e vulnerabilidades, com o propósito de evitar possíveis problemas no funcionamento dos negócios da entidade (NIST SP 800-37, 2018).

Portanto, deve-se identificar os níveis de impactos consequentes das ameaças, classificando-os em níveis, muito baixo, baixo, moderado, alto e muito alto, conforme elaborado na Tabela 3.

Tabela 3 - Análise de Impacto

Ameaça	Impacto				
	Muito baixo	Baixo	Mode-rado	Alto	Muito alto
Falha não intencional			X		
Falha de hardware					X
Falha de software			X		
Falha de conectividade					X
Falha de fornecimento de energia					X
Falha no controle de temperatura				X	
Terrorismo cibernético			X		
Espionagem		X			
Sabotagem		X			
idade criminosa–Roubo de dados		X			
Queda de raios		X			
Fogo				X	
Infestação de pragas/insetos		X			

Fonte: Adaptado de NIST SP 800-30 (2012).

A análise de impacto também pode ser medida através da elaboração de um questionário, que deve ser respondido pelo responsável do ativo em questão. O objetivo do questionário é conceituar o impacto adverso em relação à DEGRADAÇÃO OU PERDA DOS FUNDAMENTOS DA SEGURANÇA DA INFORMAÇÃO, confidencialidade, integridade e disponibilidade.

O questionário realizado com o Diretor de TI, responsável pelo ativo analisado, é apresentado no Quadro 3.

Quadro 3: Questionário do Impacto do Ativo

Questionário do Impacto do Ativo	
1.Período de utilização:	Dias: todos os dias úteis Horas: 06h às 20h
2.Este ativo é obrigatório para o funcionamento da organização:	Sim
3.Período de pico de utilização:	Meses: todos Dias: 1 23 45 67 25 262728 29 3031 Horas: 06h às22h
4.Tempo de inoperância tolerável:	30minutos
5.Período de inoperância específico para manutenções:	Dias úteis: 23h às 05h Finais de semana e feriados: 24h
6.Quanto de perda a paralisação deste ativo causaria a empresa(valor estimado):	30minutos:R$10.000,00 1hora: R$20.000,00 2horas: R$40.000,00 3horas: R$60.000,00 4horas: R$80.000,00 5horas: R$110.000,00 6horas: R$200.000,00 1dia: R$480.000,00
7.A indisponibilidade deste ativo resultaria em algum tipo de multa:	Sim,atendimentos feitos fora do SLA gerariam multas.
8.A indisponibilidade deste ativo evitaria disponibilizar algum serviço aos clientes: Sesim,quais:	Sim. Portal do Cliente, envio de faturas, peças e material de consumo.
9.A indisponibilidade deste ativo causaria qual Impacto a imagem da organização:	Grande perda financeira e perda de confiança dos clientes.
10.A indisponibilidade deste ativo causaria qual Impacto aos colaboradores:	Grande perda de produtividade e retrabalhos.

4.4.6. Análise de Riscos

Após todos os dados levantados nas etapas anteriores, por fim, é realizada a análise de riscos. É imprescindível que nessa fase de análise de riscos, seja levado em consideração todas as ameaças identificadas na etapa de identificação de ameaças, e também, os dados apurados nas etapas de identificação das vulnerabilidades e análise de impacto, que são necessários para a elaboração da matriz de risco.

O objetivo da análise de riscos é estabelecer o nível do risco, mediante o cálculo da probabilidade de uma ameaça explorar uma vulnerabilidade e da dimensão do impacto na presença de um evento adverso, sendo assim, a função do cálculo para determinar o peso do risco é a multiplicação dos valores atribuídos para a probabilidade de ocorrer ameaças pelo tamanho do impacto após a exploração da ameaça (NIST 800-30, 2012).

Para determinar o peso do risco, foi desenvolvida uma matriz de risco conforme apresentado na Tabela 4.

Ameaças	**Probabilidade** Muitobaixa=0.1 Baixa =0.2 Moderada=0.5 Alta=0.8 Muitoalta=1.0	x	**Impacto** Muito baixo = 4 Baixo =20 Moderado=79 Alto = 95 Muitoalto=100	=	**Peso do risco** Muito baixo = 0-4 Baixo = 5-20 Moderado = 21-79 Alto = 80-95 Muito alto = 96-100
Falha não intencional	0.8	x	79	=	63,2
Falha de hardware	0.2	x	100	=	20
Falha de software	0.2	x	79	=	15,8
Falha de conectividade	0.2	x	100	=	20
Falha de fornecimento de energia	0.8	x	100	=	80
Falha no controle de temperatura	0.2	x	79	=	15,8
Terrorismo cibernético	0.8	x	20	=	16
Espionagem	0.5	x	20	=	10
Sabotagem	0.2	x	20	=	4
Atividade criminosa – Roubo de dados	0.2	x	20	=	4
Queda de raios	0.2	x	20	=	4
Fogo	0.2	x	95	=	19
Infestação de pragas/insetos	0.1	x	20	=	2

Fonte: Adaptado de NIST SP 800-30 (2012).

O ANGRAPREV possui suas próprias características, objetivos e planos específicos, em razão disso, precisa encontrar o nível de risco mais adequado para operar. Dentro desse cenário, a análise de riscos é a ferramenta perfeita para mensurar a situação de segurança atual.

5.CONSIDERAÇÕES FINAIS

O modelo proposto de PRD nesta Portaria, tem como base as normas e boas práticas de segurança da informação.

A implementação de um Plano de Recuperação de Desastres deve minimizar os impactos de um desastre, possibilitando ao ANGRAPREV reagir de forma rápida e segura em casos de eventos negativos.

Assim, os responsáveis pelo TI, devem realizar a implantação do PRD no ANGRAPREV, através da elaboração de planos, aplicação das medidas de segurança contra os prováveis riscos que o ANGRAPREV possa ser afetado, por meio das etapas de caracterização do ativo, identificação das ameaças e vulnerabilidades, determinação das probabilidades e análise dos impactos e riscos, com a possibilidade de restaurar as atividades após um evento negativo de maneira planejada e organizada.

P O R T A R I A Nº 205/ 2024/ ANGRAPREV

DISPÕE SOBRE OS PROCEDIMENTOS PARA DIGITALIZAÇÃO DE DOCUMENTOS E PROCESSOS E DÁ OUTRAS PROVIDÊNCIAS.

A Diretora-Presidente do Instituto de Previdência Social de Angra dos Reis - ANGRAPREV, no uso de suas atribuições legais,

R E S O L V E :

Art. 1º - Ficam aprovadas as normas de procedimentos referentes a Digitalização de Documentos e Processos a serem implementadas no âmbito do ANGRAPREV, nos termos do regulamento que passa a integrar a presente Portaria.

Art. 2º - Esta Portaria entra em vigor na data de sua publicação, revogadas as disposições em contrário.

REGISTRE - SE, PUBLIQUE-SE E CUMPRA-SE

MUNICÍPIO DE ANGRA DOS REIS, 14 DE OUTUBRO DE 2024

LUCIANE PEREIRA RABHA
DIRETOR - PRESIDENTE

I - INTRODUÇÃO E CONCEITUAÇÃO

A digitalização de documentos e processos promove a melhoria no acesso e na difusão da informação. A adoção de procedimentos de digitalização implica tanto no conhecimento dos princípios da Arquivologia, quanto no cumprimento das atividades inerentes, como a captura de imagem, apresentação, armazenagem e preservação de originais.

Nesse sentido, a Diretoria Administrativa, a Diretoria de Tecnologia da Informação e a Chefia de Gabinete da Presidência do ANGRAPREV, visando ao atendimento dos dispositivos legais, ao