IMPRENSA OFICIAL ELETRÔNICA

SANTA FÉ DO SUL

Quinta-feira, 14 de dezembro de 2023 | www.santafedosul.sp.gov.br | Ano III | Edição nº 450

SUMÁRIO

PODER EXECUTIVO

Atos Oficiais

Resoluções

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
TRABALHANDO POR VOCÊ

SECRETARIA DE ADMINISTRAÇÃO E PLANEJAMENTO
DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO
RESOLUÇÃO N.º 002, DE 13 DE DEZEMBRO DE 2023

Institui a Política de Gestão de Riscos de Tecnologia da Informação da Prefeitura Municipal de Santa Fé do Sul.

A **SECRETARIA DE ADMINISTRAÇÃO E PLANEJAMENTO** por meio do **DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO**, no uso de suas atribuições legais e regimentais,

Considerando a necessidade de instituir política de gestão de riscos de Tecnologia da Informação formalmente instituída;

Considerando a busca pela melhoria do Índice de Eficiência na Gestão Pública Municipal IEG-M, em especial a dimensão I-GOV TI;

R E S O L V E:

Art. 1º Fica instituída a Política de Gestão de Riscos de Tecnologia da Informação da Prefeitura Municipal de Santa Fé do Sul.

Art. 2º Esta Política deverá compor o Plano Diretor de Tecnologia da Informação da Prefeitura Municipal de Santa Fé do Sul.

Art. 3º Esta resolução entra em vigor na data de sua publicação, revogando disposições em contrário.

Jorge Renato Caetano Rondina Stefanoni
DIRETOR DO DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Gilvan Cesar de Melo
DIRETOR-GERAL DE ADMINISTRAÇÃO E PLANEJAMENTO

POLÍTICA DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO

Versão 1.0

ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
13 DE DEZEMBRO DE 2023

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL TRABALHANDO POR VOCÊ

POLÍTICA DE GESTÃO DE RISCOS DE TECNOLOGIA DA INFORMAÇÃO

Evandro Farias Mura
Prefeito Municipal

Gilvan Cesar de Melo
Diretor-Geral de Administração e Planejamento

Jorge Renato Caetano Rondina Stefanoni
Diretor do Departamento de Tecnologia da Informação

Equipe Técnica de Elaboração
Enio Rodrigo Marconcini
João Augusto de Araujo Abrantes
Jorge Renato Caetano Rondina Stefanoni
Willyan Wilson Milan

ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
13 DE DEZEMBRO DE 2023

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
TRABALHANDO POR VOCÊ

SUMÁRIO

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
TRABALHANDO POR VOCÊ

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
13/12/2023	1.0	Política de Gestão de Riscos de Tecnologia da Informação	Equipe Técnica de Elaboração

HISTÓRICO DE REVISÃO

ID DA VERSÃO	DATA DA MUDANÇA	AUTOR

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
TRABALHANDO POR VOCÊ

1 INTRODUÇÃO

A gestão de riscos, medida preventiva a nível estratégico, possibilita a administração pública o aprimoramento da eficiência, princípio fulcrado no art. 37/CF, e ponto central da administração pública gerencial, inclusive cabendo ressaltar que diversos textos jurídicos expressam a relevância do planejamento na administração pública para o alcance da eficiência, cita-se Lei Federal nº 14.133, de 01 de abril de 2021 – Nova Lei de Licitações.

Entre os princípios norteadores da gestão de riscos apresenta-se a salvaguarda da ininterruptabilidade e qualidade na prestação do serviço público, ao alçar o planejamento a tônica central para persecução dos objetivos do executivo municipal e atendimento às necessidades dos munícipes, antecipando-se a cenários que podem afetar o volume e frequência dos serviços públicos.

Salienta-se ainda que a administração pública gerencial busca adaptar princípios como governança corporativa, *compliance,* ética e *Environmental, Social and Governance* (ESG) a esfera pública, logo, dirimir riscos é essencial, iniciando-se com a elaboração de planejamento, priorizando ações preventivas e padronizando ações corretivas para sanar inconformidades.

Conhecer o nível de maturidade e identificar os aspectos da gestão de riscos que necessitam ser aperfeiçoados nas organizações públicas constitui um subsídio relevante para que a Prefeitura Municipal de Santa Fé do Sul planeje, execute, monitore e qualifique seus serviços internos e externos.

Desta forma, considerando que para a Prefeitura Municipal de Santa Fé do Sul, a informação é um ativo essencial para execução de suas atividades, logo a obtenção, armazenamento e manipulação de dados pelos diferentes meios de suporte, armazenamento e comunicação, devem ter suas vulneráveis a fatores internos e externos protegidas de comprometimento, inclusive sendo tal iniciativa contemplada nas Leis Federais nº 12.527, de 18 de novembro de 2011e nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados, regulamentada no município pelo Decreto nº 5.316, de 08 de dezembro de 2022, alterado pelo Decreto nº 5.333, de 16 de dezembro de 2022, o

estabelecimento de Política de Gestão de Riscos complementarmente a Política de Segurança da Informação, como parte integrante do Plano Diretor de Tecnologia da Informação, parte de um sistema estratégico de gestão, alinhado as boas práticas, visa garantir níveis adequados de proteção às informações da instituição ou sob a sua responsabilidade.

O plano de gestão de riscos é um esquema dentro da estrutura de gestão de riscos que especifica a abordagem, os recursos a serem aplicados para gerenciar riscos e os componentes de gestão, incluindo procedimentos, práticas, sequência e cronologia das atividades e atribuição de responsabilidades.

As principais referências para a elaboração deste plano foram a NBR ISO/IEC 27005:2022 e NBR ISO/IEC 31000:2018.

2 PROCESSO METODOLÓGICO

Com o objetivo de antecipar-se a problemas relacionados à tecnologia da informação que possam de alguma forma impactar nas funções desempenhadas pela Administração Pública, o Departamento de Tecnologia da Informação elaborou a Política de Gestão de Riscos de Tecnologia da Informação adotando como processo metodológico as ferramentas: brainstorming, matriz de impacto x probabilidade, diagrama de Ishikawa e 5w2h.

Inicialmente foi realizado um brainstorming entre os membros do Departamento de Tecnologia da Informação em ação conjunta com os membros da Secretaria de Administração e Planejamento afim de suscitar os possíveis riscos que a Administração Pública incorre na área de Tecnologia da Informação em decorrência de suas atividades regulares, sazonais e esporádicas.

Suscitados os riscos inerentes aos processos, subprocessos e atividades de tecnologia da informação foram estes critérios avaliados por meio da classificação qualitativa de probabilidades e impactos, correlacionados na matriz de impacto x probabilidade, elencando os riscos segundo suas severidades. Em face desse processo, foi

possível elaborar um plano de ação por meio da ferramenta 5w2h para cada um dos riscos suscitados.

Quanto a aplicação da matriz de impacto x probabilidade argumenta-se que foram aplicados em escala de Likert, com escala de 1-5, sendo que a dimensão Impacto buscou determinar o quão significante determinado evento de risco é para a continuidade dos procedimentos planejados, sendo classificados os resultados conforme demonstrado no Quadro 1:

Quadro 1: Escala qualitativa de impacto.

CLASSIFICAÇÃO	DESCRIÇÃO	NÍVEL
Insignificante	Impacto nos objetivos são irrelevantes.	1
Relativo	Impacto nos objetivos são mínimos e reversíveis.	2
Moderado	Impacto nos objetivos são medianos.	3
Expressivo	Impacto significante nos objetivos, com possibilidade remota de recuperação	4
Irreversível	Impacto máximo nos objetivos sem possibilidade de recuperação.	5

Discorre-se que, enquanto os dados apresentados pela análise qualitativa dos impactos avaliaram o grau de dano apresentado na ocorrência de um evento, a escala de probabilidade analisou com que frequência este evento ocorre, logo, a frequência de ocorrência do evento de risco identificado, possibilitou prever a maior ou menor preocupação em enfrentá-lo.

Os dados inerentes a escala de probabilidade foram apresentados no quadro 2:

Quadro 2: Escala de probabilidade.

CLASSIFICAÇÃO	DESCRIÇÃO	PERCENTUAL	NÍVEL
Muito baixa	É improvável que aconteça	Até 10%	1
Baixa	Esporadicamente ocorrerá – até uma vez ao ano	De 11% a 30%	2
Possível	Ocorrerá mais de uma vez ao ano	De 31% a 50%	3
Alta	Frequentemente ocorrerá – mensalmente	De 51% a 70%	4

Muito alta	Ocorrerá cotidianamente – diariamente ou semanalmente	De 71% a 100%	5

Feitas as análises conforme os quadrantes impacto e probabilidade foi possível escaloná-los na Matriz de Impacto x Probabilidade, de forma a conjugar os dois critérios. A conjugação do impacto e da probabilidade permitiu a confirmação do nível de risco da atividade verificada e auxiliou na determinação da aceitação ou urgência da correção deste risco, sendo expresso o grau de severidade pela multiplicação do Impacto x Probabilidade e apresentado os resultados em forma numérica e em escalas distintas de cores.

A exemplificação da Matriz de Impacto x Probabilidade segue demonstrada no Quadro 3:

Quadro 3: Matriz Impacto x Probabilidade

		PROBABILIDADE				
		1 Muito baixa	2 Baixa	3 Possível	4 Alta	5 Muito Alta
IMPACTO	5 Irreversível	**5**	**10**	**15**	**20**	**25**
	4 Expressivo	**4**	**8**	**12**	**16**	**20**
	3 Moderado	**3**	**6**	**9**	**12**	**15**
	2 Relativo	**2**	**4**	**6**	**8**	**10**
	1 Insignificante	**1**	**2**	**3**	**4**	**5**

Risco baixo | Risco moderado | Risco alto | Risco crítico

O resultado do diagrama de cálculo de risco indicará qual o nível de risco a que está exposta a organização em razão do evento identificado. Sendo realizada posteriormente a aplicação do Diagrama de Ishikawa para compreender o evento, causa e consequência do risco, sendo posteriormente proposta uma ação tomando como base a ferramenta 5w2h.

A correlação entre o Diagrama de Ishikawa e a ferramenta 5w2h segue expressa no Quadro 4:

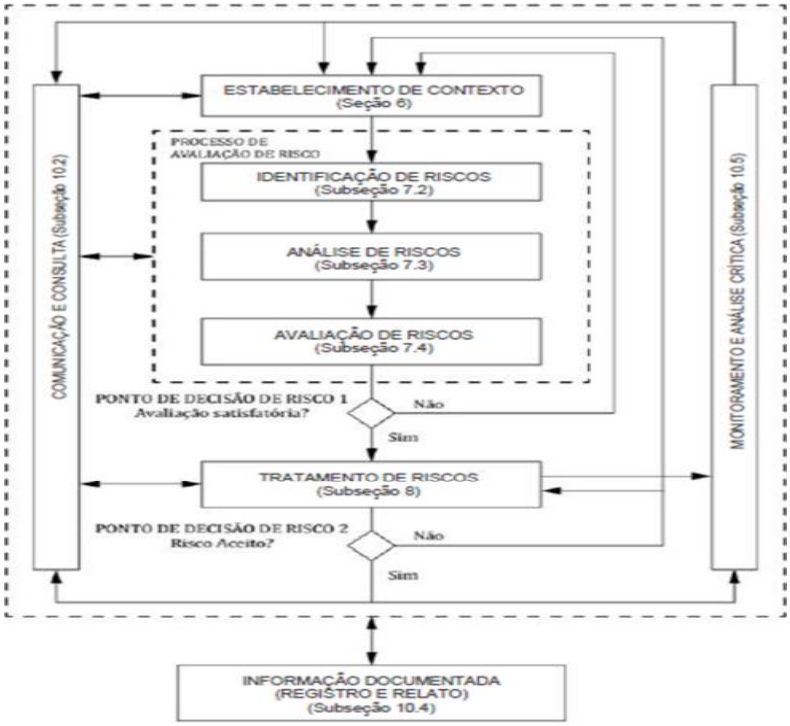
Quadro 4: Diagrama de Ishikawa e 5w2h.

ID	DESCRIÇÃO			P	I	PXI	AÇÃO PROPOSTA		
	EVENTO	CAUSA	CONSEQUÊNCIA				DESCRIÇÃO	METAS	ÍNDICE

Com o resultado obtido se elaborou um plano de ação para ser aplicado pelos servidores do Departamento de Tecnologia da Informação tanto preventiva como corretivamente, caso necessário.

O processo metodológico segue aquele descrito na NBR ISO/IEC 27005:2022 combinado com NBR ISO/IEC 31000:2018 conforme figura 1:

Figura 1: Fluxograma do processo metodológico.



PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
TRABALHANDO POR VOCÊ

3 ESCOPO

Os procedimentos inerentes a esta Resolução se aplicam as seguintes áreas organizacionais:

ÁREA ORGANIZACIONAL	DESCRIÇÃO
Departamento de Tecnologia da Informação	O Departamento de Tecnologia da Informação, departamento pertencente conforme Lei Complementar nº 80, de 17 de dezembro de 2002 a estrutura administrativa da Secretaria de Planejamento é responsável pelo suporte, manutenção preventiva, corretiva, e implantação de tecnologias de software, hardware e infraestrutura de redes.
GRUPO ORGANIZACIONAL	**DESCRIÇÃO**
Diretor do Departamento de Tecnologia da Informação Cargo criado pela Lei Complementar nº 81, de 17 de dezembro de 2002	Planeja, coordena, promove a execução de todas as atividades da unidade de acordo com a sua área de atuação e subordinação, orientando, controlando e avaliando os resultados, para assegurar o desenvolvimento normal das atividades.
Administrador de Rede Cargo criado pela Lei Complementar nº 96, de 28 de setembro de 2005 que altera a Lei Complementar nº 81, de 17 de dezembro de 2002	Administra ambiente computacional, definindo parâmetros de utilização de sistemas, implantando e documentando rotinas e projetos e controlando os níveis de serviço de sistemas operacionais, banco de dados e redes. Fornece suporte técnico no uso de equipamentos e programas computacionais e no desenvolvimento de ferramentas e aplicativos de apoio para usuários, orienta na criação de banco de dados de sistemas de informações geográficas, configura e instala recursos e sistemas computacionais, gerencia a segurança do ambiente computacional.
Assistente de Informática	Presta assistência na administração da rede de computadores e suporte aos usuários nos aspectos de hardware e software, montando, fazendo reparos,

Cargo criado pela Lei Complementar nº 96, de 28 de setembro de 2005 que altera a Lei Complementar nº 81, de 17 de dezembro de 2002	configurando equipamentos e treinando pessoal para a utilização dos aplicativos diversos. Presta suporte aos usuários da rede de computadores, envolvendo a montagem, reparos e configurações de equipamentos e na utilização do hardware e software disponíveis. Participa do processo de análise dos novos softwares e do processo de compra de softwares aplicativos. Elabora pequenos programas para facilitar a interface usuário-suporte. Efetua os back-ups e outros procedimentos de segurança dos dados armazenados. Cria e implanta procedimentos de restrição do acesso e utilização da rede, como senhas, eliminação de drives, etc; e prepara relatórios de acompanhamento do trabalho técnico realizado.
Técnico em T.I. Cargo criado pela Lei Complementar n° 377, de 13 de Outubro de 2022, que altera a Lei Complementar nº 81, de 17 de dezembro de 2002	Atende chamados de suporte dos usuários da rede de computadores, envolvendo a montagem, reparos e configurações de equipamentos e na utilização do hardware, softwares disponíveis e pontos de rede. Efetua a manutenção e conservação dos equipamentos do parque de computadores, telefonia IP e na rede de comunicação.
Empresas terceiradas de Tecnologia da Informação	Empresas contratadas para prestação de serviço relacionados a área de Tecnologia da Informação

4 IDENTIFICAÇÃO DOS PROCESSOS DE TECNOLOGIA DA INFORMAÇÃO

A primeira etapa da elaboração de gestão de riscos é a identificação e mapeamento dos processos de Tecnologia da Informação e a definição do nível de criticidade, considerando seu impacto e probabilidade para os objetivos estratégicos da instituição.

A partir dos macroprocessos institucionais foram definidos os processos de Tecnologia da Informação da Prefeitura Municipal de Santa Fé do Sul. A partir desses processos foram definidos pelo Departamento de Tecnologia da Informação os processos gerais.

A definição dos processos de Tecnologia da Informação é de suma importância, pois é a partir deles que serão verificados os processos críticos e a que se deve dar maior relevância na Gestão de Riscos de Tecnologia da Informação.

A Tabela 3 fornece os macroprocessos em que a Tecnologia da Informação atua e processos definidos de cada setor

Tabela 3: Processos de Tecnologia da Informação.

ID	PROCESSO	RESPONSÁVEL	SETOR ENVOLVIDO	ESCOPO
01	Gestão estratégica	Secretaria de Administração e Planejamento	Departamento de Tecnologia da Informação	PPA, LDO e LOA
02	Gestão do departamental	Diretor do Departamento de Tecnologia da Informação	Departamento de Tecnologia da Informação	Demandas gerais do Departamento de Tecnologia da Informação
03	Implantação de soluções	Diretor do Departamento de Tecnologia da Informação e Administrador de Redes	Departamento de Tecnologia da Informação	Implantação de soluções de tecnologia, software e hardware.
04	Elaboração de projetos de Tecnologia da Informação	Equipe de membros do PDTI	Departamento de Tecnologia da Informação	Análise de necessidades para criação de projetos que visam melhorias de T.I.
05	Gestão de contratos	Diretor do Departamento de Tecnologia da Informação	Departamento de Tecnologia da Informação	Gestão dos contratos relacionados ao Departamento de Tecnologia da Informação.
06	Fiscalização de contratos	Administrador de Redes	Departamento de Tecnologia da Informação	Fiscalização da execução dos contratos relacionados ao Departamento de Tecnologia da Informação.

07	Manutenção corretiva em computadores	Assistente de Informática	Departamento de Tecnologia da Informação	Órgãos públicos da Administração Municipal e Secretarias Municipais.
08	Manutenção preventiva em computadores	Assistente de Informática	Departamento de Tecnologia da Informação	Órgãos públicos da Administração Municipal e Secretarias Municipais.
09	Substituição de componentes dos computadores	Assistente de Informática	Departamento de Tecnologia da Informação	Órgãos públicos da Administração Municipal e Secretarias Municipais.
10	Suporte ao uso dos computadores	Assistente de Informática	Departamento de Tecnologia da Informação	Órgãos públicos da Administração Municipal e Secretarias Municipais.
11	Suporte ao uso de impressoras e scanners	Assistente de Informática	Departamento de Tecnologia da Informação	Órgãos públicos da Administração Municipal e Secretarias Municipais.
12	Manutenção e suporte de servidores	Administrador de Redes	Departamento de Tecnologia da Informação	Acompanhamento, manutenção e suporte aos servidores do Departamento de T.I.
13	Implantação de ambientes e servidores de virtualização	Administrador de Redes	Departamento de Tecnologia da Informação	Implantação e atualização dos servidores de virtualização do Departamento de T.I.
14	Comunicação externa	Diretor do Departamento de Tecnologia da Informação	Departamento de Tecnologia da Informação	Órgãos públicos da Administração Municipal e Secretarias Municipais.
15	Gerenciamento de senhas do sistema	Diretor do Departamento de Tecnologia da Informação e Administrador de Redes	Departamento de Tecnologia da Informação	Criação, alteração, exclusão de senhas de acesso ao servidor de compartilhamento de arquivos
16	Gerenciamento de contas de email	Diretor do Departamento de Tecnologia da	Departamento de Tecnologia da Informação	Criação de contas de e-mail, alteração e exclusão de senhas de e-mails.

		Informação e Administrador de Redes		
17	Elaboração e manutenção do Plano Diretor de Tecnologia da Informação	Equipe de membros do PDTI	Departamento de Tecnologia da Informação	Elaboração e manutenção dos documentos do PDTI.
18	Elaboração de Políticas Públicas de Tecnologia da Informação	Equipe de membros do PDTI	Departamento de Tecnologia da Informação	Elaboração e manutenção dos documentos de Políticas Públicas de Tecnologia da Informação.
19	Aquisição de equipamentos de Tecnologia da Informação	Equipe de membros do PDTI	Departamento de Tecnologia da Informação	Análises para aquisição de equipamentos.
20	Avaliação de especificações técnicas de equipamentos de Tecnologia da Informação	Equipe de membros do PDTI	Departamento de Tecnologia da Informação	Avaliar as especificações técnicas de equipamentos relacionados a Tecnologia da Informação.
21	Elaboração de especificação e requisitos de Tecnologia da Informação	Equipe de membros do PDTI	Departamento de Tecnologia da Informação	Analisar, elaborar e manter especificações tecnológicas para o Departamento de Tecnologia da Informação.
22	Elaboração de termos de referência de objetos de Tecnologia da Informação	Equipe de membros do PDTI	Departamento de Tecnologia da Informação	Elaborar o termo de referência e as especificações técnicas para aquisição de objetos relacionados a Tecnologia da Informação.
23	Execução e controle das políticas de Backup	Diretor do Departamento de Tecnologia da Informação e	Departamento de Tecnologia da Informação	Elaborar, testar, acompanhar, e analisar a execução das políticas de backup.

		Administrador de Redes		

5 ANÁLISE E AVALIAÇÃO DE RISCOS

Uma vez definido o escopo, os limites e a organização do processo de gestão de riscos de segurança da informação, é possível então, passar para a fase de análise/avaliação de riscos. Nesta fase são identificadas as ameaças, os controles existentes e que devem ser implementados, as vulnerabilidades e ameaças relacionadas. Assim que as ameaças e vulnerabilidades são levantadas é possível identificar e categorizar os riscos envolvidos e realizar o planejamento de tratamento necessário.

Com os resultados da Análise/Avaliação de riscos será possível direcionar e determinar ações gerenciais e prioridades para a gestão de riscos de segurança da informação, e assim, conseguir implementar controles para proteção para estes riscos. Esta deverá ser repetida periodicamente para conseguir contemplar mudanças que podem influenciar nos resultados.

A Figura 14 fornece o Processo de Análise/Avaliação de Riscos apresentado na Norma NBR ISO/IEC 27005:2008. Este processo é dividido em três fases (identificar riscos, estimar riscos dentro da análise de riscos e avaliar os riscos).

A Identificação dos Riscos determina os eventos que possam causar perda para a organização. A identificação consiste de 5 (cinco) etapas:

1. Identificar Ativos: ativo é considerado algo de valor para a organização e que, consequentemente, precisa ser protegido. A identificação dos ativos geralmente é feita por entrevista, no final obtêm-se uma lista de componentes e responsáveis.

2. Identificar Ameaças: esta fase tem o objetivo de verificar incidentes passados, identificando ameaças e suas fontes.

3. Identificar Controles Existentes: identificar controles planejados evitando custos e retrabalhos com duplicação de controles, e assegurando que estes controles estejam funcionando adequadamente.

4. Identificar Vulnerabilidades: tem como objetivo criar uma lista de vulnerabilidades associada aos ativos, ameaças e controles.

5. Identificar Consequências: analisar consequências e prejuízos caso um incidente venha a ocorrer.

5.1 ATIVOS INDETIFICADOS

Nesta fase foram identificados os ativos conforme quadro abaixo apresentado e analisadas suas ameaças, vulnerabilidades, controles existentes e consequências:

ATIVO	QUANTIDADE	LOCAL INSTALADO	RESPONSÁVEL	AMEAÇA	CONSEQUÊNCIA	CONTROLE
Computadores completos	335	Geral	Departamento de T.I.	Obsolescência, oscilação elétrica, falha de hardware, exposição a malwares, falta de peças de reposição, indisponibilidade de peças de reposição, problema estrutural do prédio,	Indisponibilidade	Sob demanda
	118	Geral	Contrato HAIP		Indisponibilidade	Sob demanda
Servidores	06	Sala T.I.	Departamento de T.I.	Impossibilidade de extensão de garantia	Indisponibilidade	Garantia estendida, plano de substituição.
Switches	70	Geral	Departamento de T.I.	Obsolescência, falha de hardware causada por oscilação elétrica	Indisponibilidade	Estoque para imediata substituição
Roteadores	60	Geral	Contrato FibraOn	Obsolescência, falha de hardware	Indisponibilidade	Reserva para imediata substituição

				causada por oscilação elétrica		
Firewalls	02	Sala T.I.	Contrato HD Tecnologia	Falha de segurança lógica da rede	Indisponibilidade	Possui alta disponibilidade (H.A) com 2 dispositivos ativos.
Impressoras	291	Geral	Responsabilidade de cada setor que possui suas impressoras	Obsolescência, falha de hardware causada por oscilação elétrica	Indisponibilidade	Manutenção corretiva, necessário PDTI elaborar plano de locação
Access Point WiFi	25	Geral	Contrato ITC	Obsolescência, falha de hardware causada por oscilação elétrica	Indisponibilidade	Sob demanda

5.2 AMEAÇAS IDENTIFICADAS

Nesta etapa foi realizado mapeamento dos registros de incidentes ocorridos, consequências, ameaças e demais registros que tenham sobre o fato.

INCIDENTE	CONSEQUÊNCIA	CAUSA	OBSERVAÇÃO
Malwares	Indisponibilidade, perda de dados, vazamento e/ou roubo de dados, instalação de vírus, backdoor e bots.	E-mail ou pendrive	Identificado por meio de relatórios da ferramenta de controle de antivírus que, os casos em que os computadores foram expostos à ameaças relacionadas a malwares, foram através de emails contendo anexos ou links falsos, e uso de unidades removíveis, como pendrive, HDs externos ou smartphones conectados na porta USB para carregamento da bateria.

Computador: Falha no disco	Indisponibilidade e perda de dados	Obsolescência, desgaste natural por uso, defeito de fábrica.	Requer peças de reposição em estoque para imediata substituição. Pode causar perda de dados, uma vez que ocasionalmente um disco com falha não permite ter acesso aos dados nele gravado.
Computador: falha na memória RAM	Indisponibilidade	Obsolescência, defeito de fábrica.	Requer peças de reposição em estoque para imediata substituição.
Computador: falha na placa-mãe	Indisponibilidade	Obsolescência, defeito de fábrica, oscilação elétrica.	Requer peças de reposição em estoque para imediata substituição.
Computador: falha na fonte de alimentação	Indisponibilidade	Desgaste natural por uso, defeito de fábrica, oscilação elétrica.	Requer peças de reposição em estoque para imediata substituição.
Computador: falha do hardware em geral	Indisponibilidade	Obsolescência, defeito de fábrica, desgaste natural por uso, oscilação elétrica.	Requer peças para reposição e/ou computador completo para imediata substituição.
Computador: falha de software S.O.	Indisponibilidade	Falha causada por erros do próprio sistema, falha causada por erros de hardware, falha causadas por aplicativos de terceiros.	Ocasionalmente não é possível identificar a causa da falha. A ação padrão tomada é realizar backup dos dados, realizar a reinstalação do sistema operacional, e restaurar os backups dos dados do usuário.
Computador: falha de software aplicativo	Indisponibilidade temporária	Falha causada por erros no próprio software aplicativo.	Remoção e reinstalação completa do aplicativo.
Computador: falha de periférico (mouse, teclado ou monitor)	Indisponibilidade temporária	Desgaste natural por uso, defeito acidental (ex: derrubar bebidas).	Requer peças de reposição em estoque para imediata substituição.
Falha de Switch	Indisponibilidade isolada	Falha do equipamento, falha causada por oscilação elétrica.	Requer peças de reposição em estoque para imediata substituição.
Falha de Roteador	Indisponibilidade isolada	Falha do equipamento, falha causada por oscilação elétrica.	Requer peças de reposição em estoque para imediata substituição.
Cabeamento de Rede	Indisponibilidade isolada	Defeito de cabo ou conector.	Refazer a conectorização dos cabos
Servidor de arquivos: exclusão	Indisponibilidade e violação de integridade	Usuário ocasionalmente exclui acidentalmente arquivos importantes no servidor de	Arquivos no servidor possuem backups. Arquivos no computador podem ou não ser

acidental de arquivo		arquivos ou no próprio computador.	recuperados, através do uso de softwares de terceiros.
Servidores: falha de hardware	Indisponibilidade crítica	Obsolescência, desgaste natural do equipamento.	Imprescindível que o equipamento esteja no período de garantia ou possuir garantia estendida, para substituição do equipamento em falha.
Servidores: falha de disco	Indisponibilidade crítica	Obsolescência, desgaste natural do equipamento.	Imprescindível que o equipamento esteja no período de garantia ou possuir garantia estendida, para substituição do equipamento em falha.
Servidores: falha de software S.O.	Indisponibilidade crítica	Falha causada por erros do próprio sistema, falha causada por erros de hardware, falha causadas por aplicativos de terceiros.	Promover a atualização do S.O. para versões atualizadas.
Servidores: falha elétrica, falta de energia.	Indisponibilidade crítica	Falta de energia	Uso de nobreaks nos equipamentos essenciais.
Nobreaks dos servidores	Indisponibilidade crítica	Obsolescência das baterias, desgaste dos relês.	Realizar manutenções periódicas nos nobreaks.
Falha de Firewall	Indisponibilidade geral a rede, telefonia e Internet.	Obsolescência, desgaste natural do equipamento.	Equipamentos de firewall em alta disponibilidade (H.A.) para evitar indisponibilidade em caso de falha.
Indisponibilidade de Link dedicado	Indisponibilidade de acesso à Internet	Problemas enfrentados pelas operadoras que fornecem Internet	Links redundantes de operadoras distintas, com configuração de *failover* em funcionamento nos firewalls.
Rede MAN fibra: rompimento	Indisponibilidade de sistemas e telefonia	Rompimento de fibra causada por eventos externos.	Rompimento causado por tráfego de caminhões na cidade, causado por podadores de árvores.
Rede WiFi	Indisponibilidade de acesso à Internet em dispositivos móveis de trabalho.	Falha de equipamento, falha de Internet.	Apenas a rede WiFi e Hotspots são afetados.
Falha elétrica: falta de energia	Indisponibilidade geral	Falha no fornecimento de elétrico por parte da concessionária de energia.	Estuda-se um plano de uso de geradores.

5.3 CONTROLES EXISTENTES

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL TRABALHANDO POR VOCÊ

Nesta etapa serão identificados os sistemas de controle existentes e quais são a abrangência de atuação e os benefícios diretos e indiretos obtidos.

ID	CONTROLE	DESCRIÇÃO	APLICAÇÃO DIRETA	APLICAÇÃO INDIRETA
01	Antivírus corporativo.	Proteção contra malwares	Computadores dos usuários.	Segurança dos computadores e da rede
02	Filtro de conteúdo Web.	Filtro de conteúdo com base em categorias	Computadores dos usuários. Ação preventiva que visa bloquear o acesso a conteúdo web que estão listados em categorias inadequadas para o perfil corporativo da Prefeitura.	Segurança dos dados
03	Firewall	Firewall de rede/borda e rede interna/DMZ.	Proteção geral de rede.	Segurança dos dados
04	Controle de dispositivos removíveis.	Bloqueio de unidades de discos removíveis (pendrive e hd externo)	Computadores das unidades básicas de saúde.	Segurança dos dados
05	Controle de dispositivos removíveis.	Bloqueio de unidades de armazenamento de smartphones	Todos os computadores da rede.	Segurança dos dados
06	Redundância de link dedicado de Internet.	Link de Internet fornecido por 2 empresas distintas, que não	Toda rede de Internet dos órgãos públicos.	Garantia de acesso aos sistemas web.

		compartilhem entre si infraestrutura nem operadora/backbone.		
07	Redundância dupla abordagem de fibra para link dedicado.	Pelo menos 1 link dedicado de Internet possui dupla abordagem: o provedor entrega o link através de 2 cabos de fibra, para redundância. Minimiza os riscos de indisponibilidade.	Toda rede de Internet dos órgãos públicos.	Garantia de acesso aos sistemas web.
08	Redundância dupla abordagem de fibra LAN2LAN.	Locais críticos e estratégicos a rede LAN2LAN possui dupla abordagem de cabo de fibra, para redundância. Minimizar riscos de indisponibilidade em órgãos públicos críticos.	Garantia de acesso à órgãos públicos essenciais.	Garantia de atendimento aos munícipes que são atendidos por estes órgãos públicos.
09	Estoque mínimo de peças sobressalentes.	Ter em estoque, os principais componentes que podem apresentar falhas, para imediata substituição.	Todos os computadores da rede.	Funcionário público/usuário do equipamento.

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
TRABALHANDO POR VOCÊ

5.4 VULNERABILIDADES IDENTIFICADAS

Nesta etapa foram identificadas as vulnerabilidades, primeiramente ao que tange a ao impacto resultante e posteriormente a probabilidade de ocorrência, permitindo assim a elaboração da matriz de impacto x probabilidade.

ID	RISCO	IMPACTO	PROBABILIDADE	I X P
01	Malwares.	5	1	5
02	Falha de disco (HD ou SSD) em computadores dos usuários.	3	4	12
03	Falha de disco no servidor de arquivos: arquivos de principais documentos de trabalho.	4	1	4
04	Falha de disco no servidor de arquivos: arquivos diversos, PDFs, fotos, imagens vetoriais e projetos CAD.	5	1	5
05	Falha estrutural de prédio, dano físico ao computador por causa de vazamento de água.	5	1	5
06	Falha em switch.	2	3	6
07	Falha em roteador.	2	3	6
08	Falha em componentes do computador.	2	4	8

5.5 CONSEQUÊNCIAS IDENTIFICADAS

Por fim realizou-se a análise das consequências por meio das ferramentas utilizadas Diagrama de Ishikawa e 5w2h utilizadas de forma concomitante, permitindo estipular um plano de ação para a solução das inconformidades, caso necessário.

PREFEITURA DA ESTÂNCIA TURÍSTICA DE SANTA FÉ DO SUL
TRABALHANDO POR VOCÊ

ID	DESCRIÇÃO			I	P	IXP	AÇÃO PROPOSTA		
	EVENTO	CAUSA	CONSEQUÊNCIA				DESCRIÇÃO	METAS	ÍNDICE
01	Malware	Pendrive e e-mail	Indisponibilidade	5	1	5	Manutenção do contrato do software antivírus Kaspersky Endpoint Security for Business.	Renovar em 2027 por 10 anos, com base na nova Lei de Licitações.	Serviço
02	Falha de hardware, computador	Obsolescência, desgaste	Indisponibilidade	3	4	12	Requer peças para substituição.	Manter em estoque as peças necessárias para reposição rápida.	Serviço
03	Falha de hardware, servidor	Obsolescência, desgaste	Indisponibilidade	4	1	4	A garantia estendida irá garantir a substituição de peças, quando houver falhas de hardware.	Renovação da garantia estendida dos servidores.	Serviço
04	Falha de switch	Obsolescência, desgaste		3	4	12	Requer peças para substituição.	Manter em estoque as peças necessárias para reposição rápida.	Serviço
05	Falha de roteador	Obsolescência, desgaste		3	4	12	Requer peças para substituição.	Manter em estoque as peças necessárias para reposição rápida.	Serviço
06	Obsolescência de computador	Obsolescência, desgaste	Indisponibilidade	3	4	12	Manutenção do contrato de locação de computadores	Renovar em 2024 por 10 anos, com base na nova	Serviço