IDENTIFICAÇÃO DA NECESSIDADE DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS PARA O NÚCLEO DE TECNOLOGIA DA POLÍCIA RODOVIÁRIA FEDERAL DE SANTA CATARINA E SUBSÍDIOS PARA O DESENVOLVIMENTO

Jean Paulo da Silveira

Resumo: A Polícia Rodoviária Federal (PRF), assim como todas as instituições e organizações em evolução, investe muito em tecnologia. Praticamente todos os procedimentos realizados hoje pela PRF são informatizados, sejam tarefas administrativas ou operacionais. Os serviços de Tecnologia da Informação (TI) oferecidos pela instituição Federal afetam tanto o público interno quanto o externo, ou seja, servidores e sociedade. Prover TI para a PRF de Santa Catarina (SC) cabe ao Núcleo Tecnologia da Informação e Comunicação de Santa Catarina (NUTIC/SC), portanto o núcleo deve estar preparado para imprevistos que possam vir a acontecer, por isso a elaboração do plano de continuidade de negócios (PCN) para o NUTIC/SC é essencial para o perfeito funcionamento da PRF de SC. Nesta pesquisa foi possível identificar ativos importantes e algumas deficiências que precisam de maior atenção.

Palavras-chave: Plano de Continuidade de Negócios, Tecnologia da Informação, Polícia Rodoviária Federal.

1 INTRODUÇÃO

A Polícia Rodoviária Federal, conta em seu quadro de servidores os policiais e os agentes administrativos, sendo aqueles com requisito de entrada a formação de nível superior em qualquer área e estes a conclusão do nível médio, portanto existe um efetivo com conhecimentos variados. O NUTIC/SC é um núcleo pertencente à PRF e é responsável por gerir toda a tecnologia e comunicação utilizada pelos policiais e servidores administrativos. A rápida evolução e a complexidade em se trabalhar com TI, assim como os poucos servidores formados na área, afetam diretamente a gestão e operacionalização do NUTIC/SC.

A gama de serviços dependentes de tecnologia na PRF é enorme. Alguns dos serviços oferecidos pelo órgão para o público externo conforme consta no Portal da PRF: Sistema Nacional de Alarmes, sistema em que o usuário que tem um veículo furtado/roubado comunica no portal da PRF o ocorrido e todos os policiais rodoviários federais recebem o comunicado; Declaração de Acidente de Trânsito, documento oficial emitido pela PRF, cuja elaboração é feita pelos próprios envolvidos na ocorrência de acidente; Boletim de Acidente de Trânsito, sistema em que o usuário envolvido no acidente pode imprimir o boletim de acidente realizado pelos agentes oficiais, inclusive é possível solicitar a retificação do boletim; muitos outros serviços são disponibilizados e podem ser solicitados no portal[1] da PRF.

Para que todos os serviços possam estar disponíveis, o policial necessita de todo um apoio tecnológico para que possa desenvolver suas atividades: consultar veículos e pessoas abordadas, elaborar o boletim de acidente de trânsito, realizar auto de infração de trânsito, recolher documentos e veículos, prestar apoio ao cidadão necessitado na rodovia federal e realizar diversos procedimentos administrativos internos.

A falta de servidores com formação específica e de padronização nas ações, faz com que o núcleo trabalhe apenas aguardando o incidente ocorrer para poder solucioná-lo, sem uma política de continuidade de negócios e sem documentação de resoluções de problemas, contando apenas com o conhecimento do servidor em tentar resolver o mais rápido possível.

1 www.prf.gov.br

A pesquisa levantou informações sobre o NUTIC/SC para que se pudesse conhecer os serviços disponibilizados e quais devem possuir uma resiliência maior, haja vista o seu grau de importância. Também foram obtidos dados sobre documentação e segurança da informação referente ao núcleo.

A metodologia utilizada foi uma pesquisa pura buscando as melhores práticas já estudadas e documentadas para continuidade de negócios, mas também aplicada, pois foi necessário uma investigação dos problemas que ocorrem no NUTIC/SC. Como a pesquisa ocorreu diretamente sobre os fatos, ela foi basicamente empírica em cima dos relatos dos servidores e também na consulta de documentos produzidos com algumas soluções a certos problemas. Como o presente projeto visa esclarecer quais ativos importantes sofrem incidentes constantemente no NUTIC/SC, o aprofundamento do estudo foi em cima de uma pesquisa explicativa, com procedimento de dados bibliográficos, já que vai se fundamentar ações em gestão de continuidade de negócios de TI.

O método utilizado para a coleta de dados foi a pesquisa-ação, haja vista que os dados vieram dos servidores do NUTIC/SC da PRF de Santa Catarina, sendo estes os sujeitos da pesquisa, atualmente o NUTIC/SC conta com 11 colaboradores. A pesquisa ocorreu no próprio Núcleo de Tecnologia da Informação e Comunicação da Polícia Rodoviária Federal de Santa Catarina. A técnica utilizada para coleta de dados foi de forma informal com os colaboradores do NUTIC/SC, haja vista que o pesquisador é servidor do núcleo, facilitando essa coleta.

O objetivo desta pesquisa é identificar quais serviços oferecidos pelo núcleo de TI são mais importantes e que sofrem maior indisponibilidade. Os subsídios para o desenvolvimento de um Plano de Continuidade de Negócios, servirá de base para que os servidores e colabores do NUTIC/SC tenham uma orientação para seguir na construção do PCN, melhorando a resiliência dos serviços e evitando assim que a atividade-fim venha a sofrer com a interrupção de atividades essenciais. Tais informações serão elencadas no decorrer desta pesquisa.

2 O PLANO DE CONTINUIDADE DE NEGÓCIOS

2.1 IMPORTÂNCIA DE UM PLANO DE CONTINUIDADE DE NEGÓCIOS

O plano de continuidade de negócios busca dar um norte nos momentos de crise, orienta os envolvidos no processo no restabelecimento ao funcionamento normal da empresa. A ideia é amenizar ou até mesmo eliminar o impacto negativo que uma indisponibilidade pode trazer para a organização.

Conforme Marinho (2008, p.47), um plano de continuidade de negócios tem por objetivo manter as atividades corporativas após algum tipo de incidente, reduzindo perdas e prejuízos durante a indisponibilidade. Exemplifica que quando o usuário ligar para o SAC, ao invés do atendente informar que não poderá realizar o atendimento porque está sem acesso ao sistema, o mesmo vai anotar todos os dados de forma manual e realizar o atendimento, mesmo que de forma mais lenta. O PCN permite elaborar estratégias para que a empresa possa continuar atendendo em caso de algum incidente ocorrer.

Um PCN organiza e prepara a empresa para poder agir em diversas situações indesejadas, com isso podendo responder aos incidentes de forma planejada, tentando dessa forma fazer com os clientes da empresa sejam impactados da menor forma possível. A organização deve estar preparada para tudo, independente da sua atividade, senão vai deixar de existir no primeiro incidente que ocorrer e suspender os serviços oferecidos aos seus usuários.

A instituição que investe em um PCN adquire confiança dos envolvidos, demonstra para todos que é uma organização forte e estruturada, que mesmo que surjam problemas, e sempre surgirão, estará pronta para responder de forma rápida e planejada. Quando acontecer algo que afete as empresas do mesmo ramo, as que conseguirem manter seus serviços funcionando, mesmo que de forma um pouco mais precária do que a habitual, conseguirão sobreviver, enquanto as outras, em sua maioria, sucumbirão.

McCarthy (2014,p.5-6) relata que mesmo com um planejamento que almeje abordar todos os assuntos, é impossível conseguir documentar todas as hipóteses que podem ocorrer, e, ainda, mesmo as que estão planejadas podem não apresentarem soluções corretas. Afirma que quando uma crise aparece em uma organização sem

planejamento, não há nem o encarregado do problema e as equipes entram em desespero. Para Marinho (2008, p.49) quanto mais rápido a empresa retornar a sua normalidade após um incidente, mais competitiva ela será, enquanto outros fornecedores estiverem tentando retornar os seus serviços, a empresa que estiver oferecendo o mesmo produto conquistará os clientes pela disponibilidade, sendo este um grande diferencial competitivo.

McCarthy tenta ratificar a importância do PCN, relatando que mesmo que a empresa esteja preparada e com certo planejamento, as coisas podem sair do controle quando um incidente surgir. Marinho explica que a indisponibilidade decorrente de um problema pode ser a exclusão de uma organização do mercado.

Ambos os autores buscam destacar a importância de um PCN para a empresa, deve haver o planejamento e uma equipe especializada deve estar pronta para agir quando houver necessidade, isso dará clareza para que os funcionários saibam o que fazer nos momentos difíceis, dessa forma a instituição demonstra sua capacidade para superar as diversas crises que possam aparecer, tornando-se competitiva com as empresas do mesmo ramo.

Um PCN não necessariamente conseguirá deixar os serviços com 100% de disponibilidade, porém de forma estruturada e com uma equipe treinada, o serviço pode ser restaurado muito mais rápido do que os concorrentes que não possuírem. Em organizações públicas, principalmente nas de segurança pública em que se trabalha em missão crítica, a falta de um serviço pode influenciar em salvar uma vida ou não.

Em um Plano de Continuidade de Negócios é impossível contemplar todos os eventos negativos que podem ocorrer em uma organização, portanto o esforço do PCN deve concentrar suas forças em tentar identificar os processos críticos da instituição e com isso definir as prioridades do planejamento. O levantamento de informações deve ser realizado com pessoas que têm pleno conhecimento da empresa, identificando em que serviços a empresa não pode apresentar indisponibilidade.

O desenvolvimento de um PCN não irá ter o devido apoio se não for levado à alta gestão da empresa a importância que ele terá para manter a estabilidade do negócio. Os diretores devem dar total apoio financeiro para que se possa contar com pessoas especializadas para desenvolver o PCN e também para colocar em prática o

plano de contingência no momento em que o evento negativo ocorrer, sem contar que o planejamento deve ter constantes atualizações.

Os profissionais responsáveis pelo desenvolvimento do Plano de Continuidade dos Negócios devem possuir experiência no assunto, inclusive o serviço podendo ser terceirizado, mas o ideal é que a própria empresa tenha o seu funcionário que construa e atualize o planejamento constantemente, podendo ele ser o coordenador das ações quando uma crise aparecer. Esse funcionário pode realizar treinamentos periódicos para atualizar os empregados de como se comportar em uma situação de instabilidade na organização, indicando a quem procurar e intervenções rápidas que possam diminuir o prejuízo até que o PCN seja colocado em prática.

Para Filho (2013, p.64) as perdas de uma empresa serão medidas na quantidade de interrupções de serviços críticos e nos estragos e potenciais perdas decorrentes delas. Portanto, é fundamental que seja identificado o maior número possível de riscos que possam afetar as atividades críticas da empresa, para isso deve-se analisar as vulnerabilidades e ameaças aos ativos críticos da organização.

Segundo Silva Coelho, Araújo e Bezerra (2014, p.151-152) a preocupação dos dirigentes na continuidade dos negócios deve ser constante, conscientizar a alta gestão sobre um plano de contingência é extremamente importante e deve ser tratado como estratégico. Informam ainda que o Plano de Continuidade de Negócios é de responsabilidade dos dirigentes da organização, devem ser apoiados por especialistas que os auxiliarão, mas não podem ser responsabilizados pela total implementação.

Marinho (2008, p.77) relata que o profissional responsável no momento de crise deve ser resiliente para conseguir ser eficiente e eficaz. Não basta seguir o plano após o incidente, pois se deve manter a ansiedade controlada para que não influencie nas atividades de recuperação. Para que a resiliência torne-se um atributo, o treinamento deve ser constante para que a repetição faça as atividades se tornarem um reflexo mecânico. O profissional deve se sentir seguro nas suas ações, sem se preocupar na avaliação que irá receber após solucionar o problema.

Para desenvolver um plano consistente é preciso conhecer bem os problemas que serão resolvidos, segundo McCarthy (2014,p.42)

> Acima de tudo, antes de dedicar qualquer segundo de seu tempo à tarefa, é preciso considerar que problema você está resolvendo. Que risco à empresa requer esse esforço? Isso o ajudará a desenvolver um escopo para o risco e para o esforço resultante necessário à sua resposta. Quem será afetado se esse risco ocorrer e qual será o impacto se não houver resposta? Você já conhece a execução baseada em requisitos. Que requisitos são relevantes a esse risco ou crise? Há leis relacionadas a essa crise? Você tem que saber o suficiente sobre o problema para justificar não só seu tempo, mas o tempo que solicitará dos outros para a criação do Plano de Resposta a Incidentes.

O Plano de Continuidade de Negócios busca dar um viés para os envolvidos na resolução de uma crise, objetivando continuar com as atividades como se nada tivesse ocorrido, de forma estruturada e planejada. A organização que tem um PCN eficiente demonstra estar à frente dos concorrentes e isso se tornará evidente na primeira crise que afetar as empresas do mesmo ramo. Conhecer as ações críticas da instituição, assim como obter informações com funcionários que têm o conhecimento pleno do funcionamento das atividades dará base para o plano adequar-se a realidade da empresa. O PCN deve ser considerado estratégico para a organização e precisa do apoio da alta direção, inclusive para ter financiamento e disponibilizar pessoas qualificadas para estarem envolvidas com a construção, atualização e implementação do PCN.

O plano deve ser planejado para toda a organização, entretanto há áreas que tem uma importância estratégica. O setor de Tecnologia da Informação (TI) está presente em praticamente todas as empresas privadas e órgãos públicos. Seja qual for a atividade da empresa, provavelmente TI fornecerá subsídios para o desempenho dela, por isso, ter uma indisponibilidade em TI causará algum tipo de prejuízo as demais ações da organização. Manter a área de TI resiliente é fundamental para a estabilidade da empresa, nada adianta a instituição produzir seus produtos se não poderá vender, pois, na maioria das vezes, depende necessariamente de um sistema informatizado para efetuar as transações.

Segundo Marinho (2018, p.75) desde 1999 o setor de Tecnologia da Informação é que coordena o projeto do Plano de Continuidade de Negócios, mesmo que a atividade da empresa não tenha ligação direta com TI. Relata que a informática é parte essencial para escalabilidade e rentabilidade da organização, e quanto mais a instituição oferecer serviços, maior a necessidade dos envolvidos reconhecerem a importância da TI para os negócios.

Quanto mais importante for a organização, mais ela deve ter um PCN bem planejado e atualizado. Em uma instituição de segurança pública em que vidas dependem de agilidade no atendimento, manter os serviços de TI e comunicação funcionando é fundamental. No caso da Polícia Rodoviária Federal a tecnologia da informação e comunicação são gerenciados pelo mesmo setor, desde o momento em que um usuário da rodovia liga para o 191, a TI gerencia a entrada dessa ligação via VOIP e encaminha ao despacho de ocorrência tudo passando pela rede interna da instituição, inclusive o acionamento da viatura para atendimento é via rádio comunicação, a qual também é gerenciada pelo mesmo setor.

Na construção do PCN, coletar informações com os funcionários do núcleo de TI é essencial para que se obtenha os detalhes dos serviços oferecidos pelo setor e que são vitais para organização, buscando desenvolver um plano de resposta a incidentes dos serviços de tecnologia condizentes com a realidade da organização, trabalhando em cima das especificidades apresentadas pelos envolvidos com a TI da instituição.

2.2 COLETA DE DADOS PARA SUBSIDIAR O PCN

O questionário, anexo 1, foi aplicado de forma online nos dias 18 e 19 de Junho de 2018 com os servidores efetivos e terceirizados do Núcleo de Tecnologia da Informação e Comunicação da Polícia Rodoviária de Santa Catarina. Foram no total 11 respostas de forma individual, as quais era possível escolher apenas uma alternativa. Como resultado, os seguintes dados foram obtidos:

- Avaliação dos serviços oferecidos pelo NUTIC/SC?
  - 45,5% - Quase nunca indisponíveis;
  - 36,4% - Indisponibilidade eventuais;
  - 18,2% - Às vezes indisponíveis.
- Recuperação dos serviços oferecidos pelo NUTIC/SC após um incidente?
  - 63,6% - Rápida;
  - 36,4% - Média.
- Avaliação sobre segurança da informação no NUTIC/SC?

- 27,3% - Ruim;
- 27,3% - Boa;
- 27,3% - Ótima;
- 18,2% - Razoável.

- Avaliação da documentação de resolução de problema no NUTIC/SC?
  - 81,8% - Pouco documentada;
  - 9,1% - Bem documentada;
  - 9,1% - Totalmente documentada.
- Avaliação dos serviços do NUTIC/SC que sofrem maior indisponibilidade?
  - 18,2% - Radiocomunicação;
  - 18,2% - Voip;
  - 18,2% - Internet concessionária;
  - 18,2% - Internet fornecedora;
  - 9,1% - Proxy;
  - 9,1% - Acesso ao SISP;
  - 9,1% - Fibra da concessionária.
- Serviços essenciais ao serviço da Polícia Rodoviário Federal?
  - 54,5% - Internet – Empresa fornecedora;
  - 27,3% - Radiocomunicação;
  - 9,1% - Virtualizador;
  - 9,1% - Fibra concessionária.
- Interferência externa que afeta os serviços do NUTIC/SC?
  - 63,6% - Falta de energia;
  - 27,3% - Interrupção da internet – Empresa da internet;
  - 9,1% - Interrupção da internet – Concessionária.

2.3 ANÁLISE DOS DADOS

Com o resultado do questionário aplicado com os funcionários do NUTIC/SC foi possível identificar aspectos referentes à disponibilidade, importância e

documentação dos serviços oferecidos pelo núcleo de TI da PRF de Santa Catarina, assim como a segurança da informação.

Os colaboradores do NUTIC/SC, em sua maioria, informaram que ocorre as vezes e eventualmente indisponibilidade dos serviços, mas quase metade do efetivo relata que raramente os serviços apresentam indisponibilidade, porém alguns sistemas precisam estarem sempre disponíveis, haja vista que a Polícia Rodoviária Federal serve a sociedade em todo o território brasileiro e a comunicação entre os usuários da rodovia e a polícia, inclusive entre os próprios policiais, depende do uso da tecnologia.

Outra informação verificada é que a maioria do núcleo indica que a recuperação dos serviços após um incidente ocorre de forma rápida, sendo que a maioria também relatou que a resolução dos problemas é pouca documentada, com isso percebe-se que a grande maioria das resoluções está restrita a alguns funcionários, seja em anotações próprias ou em seu próprio conhecimento. O núcleo de TI da PRF resolve problemas recorrentes de forma rápida, porém um pouco menos da metade acredita que a solução ocorre de forma moderada, sendo estes problemas um pouco mais complexos e precisam de pesquisas para solucionar, sendo que a falta de documentação eleva o tempo de resposta aos incidentes, sem contar a falta de padronização para resolver problemas semelhantes.

Observou-se que um pouco mais da metade do efetivo acredita que os procedimentos para garantir a segurança da informação no núcleo são ótimos ou bons, porém quase metade também relata que a segurança é ruim ou razoável, sendo que em um núcleo que é responsável por diversas informações confidenciais, a segurança da informação é fundamental para o bom andamento do serviço policial.

Nos serviços gerenciados pelo NUTIC/SC, de acordo com as respostas, é notável a importância da internet que é fornecida por uma empresa terceirizada, afetando diretamente o desempenho da PRF, todavia foi identificado que a internet sofre muita indisponibilidade. A ausência da internet gera automaticamente a cessação de serviços como Voip, Proxy, acesso aos sistemas corporativos, comunicação entre a fibra da concessionária da rodovia e as unidades operacionais, entre outros.

Nas rodovias concessionadas de Santa Catarina, a utilização da fibra para transporte de dados é fundamental para reduzir custos e melhorar o desempenho do

tráfego de informações na rede interna da PRF. A concessionária oferece uma banda na fibra para que a polícia utilize, porém, a grande indisponibilidade da rede de dados das unidades que ficam no trecho concessionado se dá pelo rompimento de fibras decorrente, na maioria das vezes, por obras que ocorrem constantemente na rodovia.

O Voip é de grande importância para a comunicação na PRF/SC, pois é ele quem gerencia as ligações para o número de emergência 191 e toda a comunicação telefônica da instituição, inclusive a nível nacional. A sua indisponibilidade ocorre pela ausência da internet, problema no servidor ou inconsistências na programação da central.

A radiocomunicação que é para uso em missão crítica, atualmente por usar o sinal analógico, apresenta diversas falhas e pouca cobertura para o uso policial. Basicamente não há mais investimento nessa tecnologia e a migração para o rádio digital deve ser priorizada. As equipes mantêm a comunicação com aplicativos de mensagens e via Voip para amenizar a ausência da comunicação por rádio.

O não funcionamento do Proxy, que é utilizado em todas as unidades da PRF de Santa Catarina, afeta diretamente o trabalho policial, haja vista que o uso é obrigatório e sua interrupção causa problemas de comunicação com a internet, e como todos os sistemas da PRF são informatizados, o policial fica impossibilitado de fornecer um serviço de qualidade a sociedade.

Servidor de arquivos, Active Directory, firewall, monitoramento da rede, banco de dados, DHCP, DNS, virtualizador e Storage apresentam indisponibilidades eventuais e são serviços que rodam no Data Center da PRF/SC, sendo que a interrupção de qualquer um deles gera problemas específicos, os quais acabam afetando a atividade-fim da PRF.

Um problema que é a realidade de várias empresas, principalmente as que trabalham com Tecnologia da Informação é a falta de energia, no NUTIC/SC esse problema foi identificado pela maioria dos funcionários como sendo a maior interferência causadora das interrupções dos serviços. Também foi identificado a falta de internet como sendo um obstáculo externo que afeta os serviços do núcleo.

3 ETAPAS DO PCN

3.1 ANÁLISE E AVALIAÇÃO DO RISCO

Após a definição do contexto da organização, deve-se partir para a avaliação dos riscos. Utilizando como base os ativos identificados na pesquisa e o conhecimento do pesquisador, foram identificadas ameaças que podem vir a deixar ativos inoperantes. Na Tabela 1 pode-se observar algumas ameaças referente aos ativos identificados. No Anexo 2 é possível visualizar todo o levantamento de ameaças.

Tabela 1 – Identificação das ameaças

Nº	Ativo	Tipo	Ameaças
1	Link Internet/MPLS	Falhas técnicas	Erro no roteamento – Empresa (1A)
2	Link Internet/MPLS	Segurança	Rede WIFI com acesso à rede interna (2A)
6	Radiocomunicação	Dano físico	Queima de equipamentos (6A)
14	Servidor de Arquivos	Localização	Produção e Backup nos mesmos lugares (14A)

3.2 ANÁLISE DOS CONTROLES EXISTENTES

O controle serve para que se possa ter uma noção do que existe implantado na organização, buscando identificar quais ativos precisam de maior atenção. Na Tabela 2 foi elencado a análise de alguns controles. O levantamento completo poderá ser visualizado no Anexo 3.

Tabela 2 – Identificação dos controles existentes

Ativo	Ameaça	Controle	Implantado		
			Sim	Não	Parcial
Link Internet/MPLS	1A	Contato com o responsável pelas rotas	X		
Link Internet/MPLS	2A	Rede wifi e intranet serem redes distintas		X	
Radiocomunicação	6A	Equipamentos reservas			X

Servidor de Arquivos	14A	Colocar backup em outra Cidade		X	

3.3 IDENTIFICAÇÃO DAS VULNERABILIDADES

Na Tabela 3 foi levantado a identificação de algumas vulnerabilidades correspondentes as ameaças dos ativos. No anexo 4 é possível observar todas as vulnerabilidades encontradas.

Tabela 3 – Identificação das vulnerabilidades

Ameaça	**Vulnerabilidade**	**É vulnerável**		
		Sim	**Não**	**Parcial**
Erro no roteamento – Empresa (1A)	Poucos servidores da terceirizada aptos a mexer com a tabela de roteamento			X
Rede WIFI com acesso a rede interna (2A)	Usuário externo acessar a rede interna via WIFI	X		
Queima de equipamentos (6A)	Sem equipamentos para reposição	X		
Produção e Backup nos mesmos lugares (14A)	Risco de dano ao data center			X

3.4 IDENTIFICAÇÃO DAS CONSEQUÊNCIAS

Serão elencados cenários que podem vir a ocorrer e quais ativos sofrerão consequências decorrentes destes eventos. Na Tabela 4 é possível ver exemplos que servirão para a análise de riscos. Todos os ativos serão considerados como valor máximo por já terem sido identificados no questionário aplicado. No anexo 5 encontra-se a tabela completa.

Tabela 4 – Identificação das consequências

Cenário do Incidente	**Ativo Afetado**	**Consequências**

Rompimento de fibra da empresa fornecedora MPLS	Link Internet/MPLS	Unidades ficam sem acesso
Invasão da rede	Servidor de Arquivos	Acesso aos arquivos confidenciais Exclusão dos arquivos
Prédio da sede sem energia	Radiocomunicação	Sem comunicação na região da Grande Florianópolis
Dano no Virtualizador	Servidor Arquivos	Sem acesso aos arquivos

3.5 AVALIAÇÃO DO RISCO

Na Tabela 5 foram catalogadas algumas ameaças que deverão ser tratadas considerando a importância do ativo, se existe ou não controle, se há vulnerabilidade e consequências relevantes ao negócio da organização. No anexo 6 é possível visualizar toda a tabela de avaliação do risco.

Tabela 5 – Avaliação do Risco

Ameaça	**Afeta Ativo Importante**		**Existe Controle**			**Há Vulnerável**			**Há Consequências**		**Tratar?**	
	S	**N**	**S**	**N**	**P**	**S**	**N**	**P**	**S**	**N**	**S**	**N**
Erro no roteamento – Empresa (1A)	X		X					X	X			X
Rede WIFI com acesso a rede interna (2A)	X			X		X			X		X	
Queima de equipamentos (6A)	X				X	X			X		X	
Produção e Backup nos mesmos lugares (14A)	X			X				X	X		X	

3.6 TRATAMENTO DOS RISCOS

3.6.1 CONTROLES E JUSTIFICATIVAS

Nessa etapa será descrito a forma de controle para cada ameaça identificada e a justificativa para a adoção dessa medida. Na Tabela 6 alguns exemplos de controle e justificativa e no anexo 7 todo o levantamento.

Tabela 6 – Controles e justificativas

Ameaça	Controle	Justificativa
Rede WIFI com acesso a rede interna (2A)	Não permitir acesso à rede interna pelo WIFI.	Evitar acesso externo à rede intranet e servidores.
Queima de equipamentos (6A)	Aquisição de equipamentos que eventualmente costumam ficar inoperantes	Equipamentos em que a troca seja fácil, a equipe do NUTIC/SC pode realizar a troca e subir o serviço.
Produção e Backup nos mesmos lugares (14A)	Levar o servidor de backup para outra Cidade.	Garantir a integridade dos arquivos

3.6.2 PLANO DE TRATAMENTO DE RISCOS

Na Tabela 7 segue exemplos do plano de tratamento para identificar quais recursos serão necessários, assim como os responsáveis e data de início e fim da implantação de cada controle. No anexo 8 é possível observar todo o pano de tratamento de riscos.

Tabela 7 – Plano tratamento de riscos

Controle	Recursos Necessários	Responsável	Início/fim
Centralizar as rotas em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de ausência do responsável.	Capacitação	Técnico de redes e Servidor PRF	01/09/2018 a 31/12/2018
Não permitir acesso à rede interna pelo WIFI.	Implementar controladora	Técnico de redes e	01/09/2018 a

		Servidor PRF	15/10/2018
Aquisição de equipamentos que eventualmente costumam ficar inoperantes.	Recurso financeiro	Gerente do Rádio Digital	01/09/2018 a 30/06/2019
Levar o servidor de backup para outra Cidade.	Local disponível e infraestrutura	Chefe NUTIC/SC e Servidor PRF	01/09/2018 a 31/12/2018

3.7 ANÁLISE DE IMPACTOS

Nesta etapa serão definidos impactos na atividade do Policial Rodoviário Federal após a interrupção de um serviço. O processo de análise de impactos é baseado no pesquisar, que é Policial Rodoviário Federal, com experiência no serviço operacional e administrativo no Núcleo de Tecnologia da Informação e Comunicação da Polícia Rodoviária Federal.

As seguintes informações serão importantes:

- A maioria dos procedimentos operacionais realizados pelos policiais precisam ser inseridos em sistemas informatizados, sendo que um plantão tem 24 horas e até o final do serviço. As consultas a veículos e pessoas ocorrem em sistemas online;

- O procedimento de fiscalização necessita de acesso dos telefones móveis à internet, em grandes centros é possível, na ausência do WIFI, utilizar os dados da operadora, porém, em diversas unidades, a falta do WIFI por mais de 1 hora afeta a fiscalização dos policiais.

- As repetidoras de rádio digital, em locais críticos e estratégicos para a PRF, não poderão ficar inoperante por mais de 4 horas, nos demais, é aceitável uma indisponibilidade de até 6 horas;

- Os núcleos e delegacias acessam os arquivos do servidor de arquivos durante todo o período compreendido entre 08 horas até as 17 horas,

portanto a indisponibilidade nesse horário não poderá ser maior que 3 horas.

- O proxy como é utilizado para a conexão das máquinas de todas as unidades, não deve ficar fora por mais de 1 hora, o mesmo acontece com o firewall que controla toda a rede e sua indisponibilidade afetaria todos os serviços, já o Active Directory pode ficar fora por até 8h sem que venha a afetar os serviços, apenas novos logins e novas máquinas no domínio.

3.8 ANÁLISE DE IMPACTOS E TEMPO DE INDISPONIBILIDADE ACEITÁVEIS

Nesta etapa, de acordo com as informações levantadas pelo pesquisador, será estipulado um tempo médio aceitável de indisponibilidade das atividades e que não causará um impacto muito forte na organização. Na Tabela 8 é possível identificar algumas análises e no anexo 9 está a tabela completa.

Tabela 8 – Plano tratamento de riscos

Recurso	Impacto	Tempo admissível
Acesso à internet	Policiais sem atualizar sistemas informatizados. Usuários da rodovia sem conseguir imprimir documentos nas unidades. Fiscalização de veículos e pessoas prejudicada.	1 hora
Radiocomunicação	Policiais sem comunicação rápida em situações de emergência, afetando inclusive, salvamento de pessoas.	4 horas em locais estratégicos 6 horas nos demais locais

4 CONCLUSÕES

É possível identificar a importância de um Plano de Continuidade de Negócios em qualquer organização, a sobrevivência de uma instituição, seja ela privada ou pública, depende da sua importância para os clientes ou sociedade, de quanto ela consegue ser útil quando se precisa dela, portanto um plano que organize e fortaleça suas atividades é vital para o sucesso.

A Polícia Rodoviária Federal é um órgão federal que tem como visão de futuro ser reconhecida pela sociedade brasileira por sua excelência e efetividade e para que isso ocorra, haja vista a grande dependência por tecnologia e comunicação em sua atividade, o setor responsável pela TI e comunicação deve estar preparado para os diversos tipos de eventos negativos que possam vir a ocorrer.

Foi verificado que o núcleo de tecnologia da informação e comunicação da PRF de Santa Catarina precisa melhorar sua política de segurança da informação e os procedimentos de documentação de suas ações. O alto índice de indisponibilidade de alguns serviços oferecidos também precisa ser corrigido.

Os ativos identificados fornecem recursos para que a atividade administrativa e operacional da PRF possam ser exercidas com excelência, são sistemas de uso emergencial, missão crítica e ainda assim apresentam alguma indisponibilidade. As ameaças identificadas para os ativos são passíveis de controle, porém são muitas e precisam ter os riscos gerenciados.

Um Plano de Continuidade de Negócios é necessário e fundamental para o Núcleo de Tecnologia da Informação e Comunicação da Polícia Rodoviária Federal, assim como definir políticas de segurança, fornecendo para os policiais um serviço estável e confiável.

REFERÊNCIAS

SILVA COELHO, Flávia Estélia ; ARAÚJO, Luiz Geraldo Segadas; BEZERRA, Edson Kowask. **Gestão da Segurança da Informação**. Rio de Janeiro: Escola Superior de Redes, 2014. 198 p.

GESTÃO de Riscos. Rio de Janeiro: Brasiliano, 2012. Disponível em: <http://www.brasiliano.com.br>. Acesso em: 05 abr. 2018.

FILHO, Felício Cestari. **ITIL** v3 : Fundamentos. Rio de Janeiro: Escola Superior de Redes, 2012. 176 p.

BEZERRA, Edson Kowask . **Gestão de Riscos de TI**: NBR 27005. Rio de Janeiro: Escola Superior de Redes, 2013. 156 p.

MARINHO, Fernando. **Plano de Continuidade de Negócios**. Rio de Janeiro: Elsevier, 2018. 123 p.

MCCARTHY, N.K. **Resposta a Incidentes de Segurança em Computadores**. Original. ed. Nova York: Bookman, 2014. 208 p.

MCCARTHY, N.K. **Resposta a Incidentes de Segurança em Computadores**. Original. ed. Nova York: Bookman, 2014. 208 p.

ANEXO 1

Continuidade dos serviços NUTIC/SC

Formulário para obter informações sobre a disponibilidade e continuidade dos serviços de TI oferecidos pelo NUTIC/SC para o funcionamento do aparato tecnológico da PRF/SC.

1. Como você avalia a disponibilidade dos serviços oferecidos pelo NUTIC/SC? *

Marcar apenas uma oval.

- Sempre indisponíveis
- Maioria das vezes indisponíveis
- As vezes indisponíveis
- Indisponibilidade eventuais
- Quase nunca indisponíveis
- Sem indisponibilidade

2. Como você avalia a recuperação dos serviços oferecidos pelo NUTIC/SC após um incidente? *

Marcar apenas uma oval.

- Lenta
- Moderada
- Rápida

3. Como você avalia a segurança da informação no NUTIC/SC? *

Marcar apenas uma oval.

- Não existe
- Ruim
- Razoável
- Boa
- Ótima

4. Como você avalia a documentação de resolução de problemas do NUTIC/SC? *

Marcar apenas uma oval.

- Inexistente
- Pouco documentada
- Documentada, mas desorganizada
- Bem documentada

- Totalmente documentada

5. Escolha 1 serviço oferecido pelo NUTIC/SC que você identifica que sofre maior indisponibilidade. *

- Internet - Empresa Fornecedora
- Internet - Concessionária
- Voip
- Radiocomunicação
- Servidor de Arquivos
- Active Directory - AD
- Proxy
- Firewall
- Monitoramento da rede
- WIFI
- Bancos de Dados
- DHCP
- DNS
- SGPP
- VIrtualizador
- Storage
- Telefonia móvel
- Página de abertura de chamados do NUTIC/SC
- Acesso ao Bem Te Vi
- Acesso ao SISP
- Outro:

6. Dos serviços oferecidos pelo NUTIC, escolha 1 que você acredita ser essencial ao serviço

Policial Rodoviário Federal?

- Internet - Empresa Fornecedora
- Internet - Concessionária
- Voip
- Radiocomunicação
- Servidor de Arquivos
- Active Directory - AD
- Proxy
- Firewall
- Monitoramento da rede
- WIFI
- Bancos de Dados

- DHCP
- VIrtualizador
- Storage
- Telefonia Móvel
- Página de abertura de chamados do NUTIC/SC
- Acesso ao Bem Te Vi
- Acesso ao SISP
- Outro:

7. Escolha 1 interferência externa ao núcleo que afetam diretamente os serviços oferecidos pelo NUTIC/SC? *

- Falta de energia
- Falta de água
- Interrupção da internet - Empresa de Internet
- Interrupção de internet - Concessionária
- Roedores danificando cabos de rede
- Trovoadas/tempestades
- Indisponibilidade do LDAP
- Receber doação de equipamentos fora do padrão do NUTIC/SC
- Interferência externa nas decisões do NUTIC/SC
- SISP - Acesso e senhas
- DETRANNET
- Bem Te Vi
- Greve de ônibus
- Outro:

ANEXO 2 – IDENTIFICAÇÃO DAS AMEAÇAS

Nº	Ativo	Tipo	Ameaças
1	Link Internet/MPLS	Falhas técnicas	Erro no roteamento – Empresa (1A)
			Erro de configuração de IP – Empresa (1B)
			Erro no roteamento - NUTIC/SC (1C)
			Problemas no roteador Firewall - NUTIC/SC (1D)
2	Link Internet/MPLS	Segurança	Rede WIFI com acesso a rede interna (2A)
3	Link Internet/MPLS	Dano físico	Rompimento de fibra ou problema no rádio enlace (3A)
4	Fibra da concessionária	Dano físico	Rompimento de fibra (4A)
5	Fibra da concessionária	Recurso humano	Limitação de conhecimento técnico a apenas 1 funcionário (5A)
6	Radiocomunicação	Dano físico	Queima de equipamentos (6A)
			Falta de energia (6B)
7	Radiocomunicação	Falhas técnicas	Configurações impróprias para o bom funcionamento da rede de rádio (7A)
8	Radiocomunicação	Manutenção	Estações espalhadas pelo Estado inteiro (8A)
9	Radiocomunicação	Segurança	Locais vulneráveis a furto (9A)
10	Telefonia Voip	Falhas técnicas	Erro configuração do servidor (10A)
			Loop na rede (10B)
11	Telefonia Voip	Dano físico	Dano no servidor (11A)
12	Telefonia Voip	Recurso humano	Conhecimento técnico em apenas 2 servidores para o Brasil inteiro (12A)
13	Servidor de Arquivos	Falhas técnicas	Manipulação errada dos usuários dos arquivos e pastas (13A)
14	Servidor de Arquivos	Localização	Produção e Backup nos mesmos lugares (14A)

15	Servidor de Arquivos	infra-estrutura	Pouco espaço de armazenamento livre (15A)
16	Servidor de Arquivos	Segurança	Usuários acessando pastas de setores em que ele não está mais (16A)
17	Proxy	Falhas técnicas	Erro de configuração (17A)
18	Proxy	Dano físico	Dano no servidor (18A)
19	Active Directory	Falhas técnicas	Erro de configuração (19A)
20	Active Directory	Segurança	Muitos Administradores de domínio (20A)
			Existe apenas o AD principal (20B)
			Sem atualizações de sistemas (20C)
21	Active Directory	Dano físico	Dano no servidor (21A)

ANEXO 3 – ANÁLISE DOS CONTROLES EXISTENTES

Ativo	Ameaça	Controle	Implantado		
			Sim	Não	Parcial
Link Internet/MPLS	1A	Contato com o responsável pelas rotas	X		
Link Internet/MPLS	1B	Contato com o responsável	X		
Link Internet/MPLS	2A	Rede wifi e intranet serem redes distintas		X	
Link Internet/MPLS	3A	Rotas alternativas		X	
Fibra da concessionária	4A	Rotas alternativas			X
Fibra da concessionária	5A	Documentação e manutenção nos roteadores pela equipe NUTIC/SC		X	
Radiocomunicação	6A	Equipamentos reservas			X
Radiocomunicação	7A	Treinamentos e suporte da empresa fornecedora dos equipamentos			X
Radiocomunicação	8A	Empresa terceirizada de manutenção		X	
Radiocomunicação	9A	Solução de segurança dos sites		X	
Telefonia Voip	10A	Pessoas habilitadas e autorizadas a alterarem a programação			X
Telefonia Voip	10B	Spanning Tree Protocol nos switches		X	
Telefonia Voip	11A	Servidor redundante			X
Telefonia Voip	12A	Habilitar servidores do Nutic/SC			X
Servidor de Arquivos	13A	Auditoria dos arquivos e pastas			X
Servidor de Arquivos	14A	Colocar backup em outra Cidade		X	
Servidor de Arquivos	15A	Adquirir novo storage		X	
Servidor de Arquivos	16A	Gerencia de usuários constante			X
Proxy	17A	Capacitar servidores		X	
Proxy	18A	Servidor redundante		X	
Active Directory	19A	Capacitar servidores		X	
Active Directory	20A	Somente servidores capacitados como administradores			X
Active Directory	20B	AD redundante		X	

Active Directory	20C	Realizar todas as atualizações críticas		X	
Active Directory	21A	Servidor redundante		X	

ANEXO 4 – IDENTIFICAÇÃO DAS VULNERABILIDADES

Ameaça	Vulnerabilidade	É vulnerável		
		Sim	Não	Parcial
Erro no roteamento – Empresa (1A)	Poucos servidores da terceirizada aptos a mexer com a tabela de roteamento			X
Erro de configuração de IP – Empresa (1B)	Poucos servidores da terceirizadas aptos a configurar os IP's das unidades da PRF			X
Erro no roteamento - NUTIC/SC (1C)	Poucos servidores da PRF aptos a mexer no roteamento interno	X		
Problemas no roteador Firewall - NUTIC/SC (1D)	Servidor firewall não redundante	X		
Rede WIFI com acesso a rede interna (2A)	Usuário externo acessar a rede interna via WIFI	X		
Rompimento de fibra ou problema no rádio enlace (3A)	Obras que danificam o link	X		
Rompimento de fibra (4A)	Obras que danificam o link	X		
Limitação de conhecimento técnico a apenas 1 funcionário (5A)	Atende apenas em horário de expediente	X		
Queima de equipamentos (6A)	Sem equipamentos para reposição	X		
Falta de energia (6B)	Fornecimento de energia instável	X		
Configurações impróprias para o bom funcionamento da rede de rádio (7A)	Senha padrão de configuração, acesso de muitas pessoas com esta senha	X		
Estações espalhadas pelo Estado inteiro (8A)	Danificar equipamento que esteja longe dos técnicos	X		
Locais vulneráveis a furto (9A)	Locais afastados e com pouca segurança	X		
Erro configuração do servidor (10A)	Funcionários não habilitados mexendo nas configurações			X

Loop na rede (10B)	Troca de cabos de rede do aparelho ao alcance do usuário	X		
Dano no servidor (11A)	Problema físico ocasionando a parada do servidor	X		
Conhecimento técnico em apenas 2 servidores para o Brasil inteiro (12A)	Técnicos de férias ou com excesso de demandas	X		
Manipulação errada dos usuários dos arquivos e pastas (13A)	Exclusão acidental ou proposital de arquivos comuns aos núcleos	X		
Produção e Backup nos mesmos lugares (14A)	Risco de dano ao data center			X
Pouco espaço de armazenamento livre (15A)	Usuários adicionando arquivos pessoais no servidor de arquivos	X		
Erro de configuração (17A)	Configuração complexa e de conhecimento restrito a poucos servidores			X
Dano no servidor (18A)	Problema físico ocasionando a parada do servidor	X		
Erro de configuração (19A)	Muitas pessoas configurando e com pouco conhecimento	X		
Muitos Administradores de domínio (20A)	Possibilidade de configuração errada	X		
Existe apenas o AD principal (20B)	Problema no AD principal	X		
Sem atualizações de sistemas (20C)	Contaminação de vírus	X		
Dano no servidor (21A)	Problema físico ocasionando a parada do servidor	X		

ANEXO 5 – IDENTIFICAÇÃO DAS CONSEQUÊNCIAS

Cenário do Incidente	Ativo Afetado	Consequências
Rompimento de fibra da empresa fornecedora MPLS	Link Internet/MPLS	Unidades ficam sem acesso
	Fibra da concessionária	Unidades ficam sem acesso
	Telefone Voip	Unidades foram da sede ficam sem telefonia
	Servidor Arquivos	Unidades fora da sede ficam sem acesso
	Proxy	Unidades fora da sede ficam sem acesso
	AD	Unidades fora da sede ficam sem acesso
Rompimento de fibra da concessionária	Fibra da concessionária	Unidades que usam a fibra da concessionária ficam sem internet e acesso aos servidores
	Telefone Voip	Unidades que usam a fibra da concessionária ficam sem telefonia voip
	Servidor Arquivos	Unidades que usam a fibra da concessionária ficam sem acessar o servidor de arquivos
	Proxy	Unidades que usam a fibra da concessionária ficam sem acessar o proxy
	AD	Unidades que usam a fibra da concessionária ficam sem acesso ao AD
Prédio da sede sem energia	Link Internet/MPLS	Sem acesso à internet
	Fibra da concessionária	Unidades sem comunicação
	Radiocomunicação	Sem comunicação na região da Grande Florianópolis
	Telefone Voip	Sem comunicação
	Servidor Arquivos	Sem comunicação
	Proxy	Sem comunicação
	AD	Sem comunicação
Dano no Virtualizador	Telefone Voip	Unidades sem comunicação 191 sem comunicação
	Servidor Arquivos	Sem acesso aos arquivos
	Proxy	Sem acesso
	AD	Sem novos logins no domínio Problema no DHCP e DNS

Invasão da rede	Servidor de Arquivos	Acesso aos arquivos confidenciais Exclusão dos arquivos

ANEXO 6 – AVALIAÇÃO DO RISCO

Ameaça	Afeta Ativo Importante		Existe Controle			Há Vulnerável			Há Consequências		Tratar?	
	S	N	S	N	P	S	N	P	S	N	S	N
Erro no roteamento – Empresa (1A)	X		X					X	X			X
Erro de configuração de IP – Empresa (1B)	X		X					X	X			X
Erro no roteamento - NUTIC/SC (1C)	X			X		X			X		X	
Problemas no roteador Firewall - NUTIC/SC (1D)	X			X		X			X		X	
Rede WIFI com acesso a rede interna (2A)	X			X		X			X		X	
Rompimento de fibra ou problema no rádio enlace (3A)	X			X		X			X		X	
Rompimento de fibra (4A)	X				X	X			X		X	
Limitação de conhecimento técnico a apenas 1 funcionário (5A)	X			X		X			X		X	
Queima de equipamentos (6A)	X				X	X			X		X	
Falta de energia (6B)	X			X		X			X		X	
Configurações impróprias para o bom funcionamento da rede de rádio (7A)	X				X	X			X		X	
Estações espalhadas pelo Estado inteiro (8A)	X			X		X			X		X	

Locais vulneráveis a furto (9A)	X					X			X		X	
Erro configuração do servidor (10A)	X				X			X	X		X	
Loop na rede (10B)	X			X		X			X		X	
Dano no servidor (11A)	X				X	X			X		X	
Conhecimento técnico em apenas 2 servidores para o Brasil inteiro (12A)	X				X	X			X		X	
Manipulação errada dos usuários dos arquivos e pastas (13A)	X				X	X			X		X	
Produção e Backup nos mesmos lugares (14A)	X			X				X	X		X	
Pouco espaço de armazenamento livre (15A)	X			X		X			X		X	
Usuários acessando pastas de setores em que ele não está mais (16A)	X				X	X			X		X	
Erro de configuração (17A)	X			X				X	X		X	
Dano no servidor (18A)	X			X		X			X		X	
Erro de configuração (19A)	X			X		X			X		X	
Muitos Administradores de domínio (20A)	X				X				X		X	
Existe apenas o AD principal (20B)	X			X	X				X		X	
Sem atualizações de sistemas (20C)	X			X	X				X		X	
Dano no servidor (21A)	X			X	X				X		X	

ANEXO 7 – CONTROLES E JUSTIFICATIVAS

Ameaça	Controle	Justificativa
Erro no roteamento - NUTIC/SC (1C)	Centralizar as rotas em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de ausência do responsável.	Evitar informações duplicadas e configurações fora do padrão.
Problemas no roteador Firewall - NUTIC/SC (1D)	Centralizar configurações em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de ausência do responsável.	Evitar informações duplicadas e configurações fora do padrão.
Rede WIFI com acesso a rede interna (2A)	Acesso à rede WIFI individual e utilizando login LDAP.	Responsabilização de cada acesso.
	Não permitir acesso à rede interna pelo WIFI.	Evitar acesso externo à rede intranet e servidores.
Rompimento de fibra ou problema no rádio enlace (3A)	Aditivo no contrato permitindo rotas alternativas	Evitar que o concentrador da rede MPLS seja apenas um, assim como a saída da internet.
Rompimento de fibra (4A)	Funcionários do NUTIC/SC serem aptos a realizar a rota alternativa pela concessionária	Não ficar dependente de um único funcionário da concessionária
Limitação de conhecimento técnico a apenas 1 funcionário (5A)	Funcionários do NUTIC/SC serem aptos a realizar a rota alternativa pela concessionária	Não ficar dependente de um único funcionário da concessionária
Queima de equipamentos (6A)	Aquisição de equipamentos que eventualmente costumam ficar inoperantes	Equipamentos em que a troca seja fácil, a equipe do NUTIC/SC pode realizar a troca e subir o serviço.
Falta de energia (6B)	Aquisição de geradores em sites importantes	Existem repetidoras que atendem locais urbanos ou estratégicos para a PRF que não podem ficar sem energia
Configurações impróprias para o bom funcionamento da rede de rádio (7A)	Durante a garantia, apenas a empresa fornecedora dos equipamentos deve realizar configurações	Evitar configurações que afetem a rede e possa não receber suporte da empresa fornecedora
Estações espalhadas pelo Estado inteiro (8A)	Contratar serviço de manutenção com SLA's de acordo com a importância de	Como a PRF/SC não possui mão de obra especializada suficiente para

	cada site	realizar todas as manutenções, deve-se terceirizar
Locais vulneráveis a furto (9A)	Contratar soluções completas de segurança (vídeo, alarme, iluminação, etc)	Trabalhar tanto de forma ostensiva quanto preventiva para evitar a perda de equipamentos
Erro configuração do servidor (10A)	Definir responsabilidade atrelando servidor ao funcionário e deixar a senha root/administrador com acesso de apenas um funcionário	Evitar configurações realizadas sem autoria, evitando alterações por impulso, precisando o funcionário testar para depois colocar em produção.
Loop na rede (10B)	Configurar Spanning Tree Protocol em todos os Switches	Evitar diversos loops que podem ocorrer na rede
Dano no servidor (11A)	Servidor redundante em outra cidade. Configuração de duas contas nos aparelhos. Saída SIP para telefone externa na sede e placa GSM em outra Cidade	Redundância do servidor Asterisk e de saída para a telefonia externa
Conhecimento técnico em apenas 2 servidores para o Brasil inteiro (12A)	Solicitar capacitação nacional para que configurações rotineiras possam ser realizadas por servidores do NUTIC/SC	Evitar sobrecarregar o suporte nacional e ter resolução mais rápida de problemas locais no VOIP
Manipulação errada dos usuários dos arquivos e pastas (13A)	Implementar servidor de log para receber os eventos de exclusão do servidor de arquivos. Ativar o “snapshot” do storage para 21 dias do servidor de arquivos	Ter auditoria para casos de exclusão voluntária de arquivos ou pastas. Garantir que seja possível recuperar es exclusões acidentais e voluntárias por 21 dias
Produção e Backup nos mesmos lugares (14A)	Levar o servidor de backup para outra Cidade.	Garantir a integridade dos arquivos
Pouco espaço de armazenamento livre (15A)	Realizar auditoria no storage para eliminar arquivos duplicados ou que n estejam mais em uso	Existem diversos discos criados que estão em desuso, mas ocupando espaço no storage
Usuários acessando pastas de setores em que ele não está mais (16A)	Melhorar a política de segurança da informação, sendo responsabilidade dos chefes dos setores informar de imediato a saída de funcionário do núcleo	Evitar que funcionários que sejam realocados ou demitidos permaneçam acessando arquivos em que não tem mais permissão
Erro de configuração (17A)	Centralizar configurações em apenas um funcionário, mas com mais funcionários	Evitar informações duplicadas e configurações fora do padrão.

	aptos a realizar em caso de ausência do responsável.	
Dano no servidor (18A)	Configurar outro servidor proxy para que possa assumir em casa de falha do principal e em Cidade diversa	Evitar que a navegação das unidades seja interrompida por problema físico no proxy
Erro de configuração (19A)	Centralizar configurações em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de ausência do responsável.	Evitar informações duplicadas e configurações fora do padrão.
Muitos Administradores de domínio (20A)	Diminuir o número de administradores de domínio e criar auditoria de todas as atividades realizadas pelos administradores	Evitar que muitas pessoas alterem a configuração do AD e não seja documentado o que foi feito e nem quem fez
Existe apenas o AD principal (20B)	Configurar o servidor secundário para que possa assumir imediatamente após o principal ficar inoperante, sendo que aquele deverá replicar de forma instantânea as configurações do principal	Evitar que com a queda do AD não se consiga mais novos logins na rede e nem acesse o servidor de arquivos
Sem atualizações de sistemas (20C)	Ativar as atualizações automáticas e programar para serem realizadas durante a madrugada	Evitar que novos formas de ataques cibernéticos possam danificar o AD
Dano no servidor (21A)	AD secundário deve ser localizado em outra Cidade	Manter ativo as funções realizadas pelo AD

ANEXO 8 – PLANO DE TRATAMENTO DE RISCOS

Controle	Recursos Necessários	Responsável	Início/fim
Centralizar as rotas em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de ausência do responsável.	Capacitação	Técnico de redes e Servidor PRF	01/09/2018 a 31/12/2018
Centralizar configurações em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de ausência do responsável.	Capacitação	Técnico de redes e Servidor PRF	01/09/2018 a 31/12/2018
Acesso à rede WIFI individual e utilizando login LDAP.	Implementar controladora	Técnico de redes e Servidor PRF	01/09/2018 a 15/10/2018
Não permitir acesso à rede interna pelo WIFI.	Implementar controladora	Técnico de redes e Servidor PRF	01/09/2018 a 15/10/2018
Aditivo no contrato permitindo rotas alternativas	Recurso financeiro	Chefe do NUTIC/SC	01/09/2018 a 30/06/2019
Funcionários do NUTIC/SC serem aptos a realizar a rota alternativa pela concessionária	Contato com o responsável da concessionária	Chefe do NUTIC/SC	01/09/2018 a 15/10/2018

Aquisição de equipamentos que eventualmente costumam ficar inoperantes	Recurso financeiro	Gerente do Rádio Digital	01/09/2018 a 30/06/2019
Aquisição de geradores em sites importantes	Recurso financeiro	Gerente do Rádio Digital	01/09/2018 a 31/12/2019
Durante a garantia, apenas a empresa fornecedora dos equipamentos deve realizar configurações	Contato com a empresa fornecedora	Gerente do Rádio Digital	01/09/2018 a 15/10/2018
Contratar serviço de manutenção com SLA's de acordo com a importância de cada site	Recurso financeiro	Gerente do Rádio Digital	01/09/2018 a 31/12/2019
Contratar soluções completas de segurança (vídeo, alarme, iluminação, etc)	Recurso financeiro	Gerente do Rádio Digital	01/09/2018 a 31/12/2019
Definir responsabilidade atrelando servidor ao funcionário e deixar a senha root/administrador com acesso de apenas um funcionário	Definir política de segurança	Gerente de Segurança	01/09/2018 a 31/12/2018
Configurar Spanning Tree Protocol em todos os Switches	Capacitação	Técnico de redes e Servidor PRF	01/09/2018 a 15/10/2018
Servidor redundante em outra cidade. Configuração de duas contas nos aparelhos. Saída SIP para telefone	Recurso financeiro	Servidor PRF	01/09/2018 a 31/12/2018

externa na sede e placa GSM em outra Cidade			
Solicitar capacitação nacional para que configurações rotineiras possam ser realizadas por servidores do NUTIC/SC	Capacitação	Servidores PRF	01/09/2018 a 30/06/2019
Implementar servidor de log para receber os eventos de exclusão do servidor de arquivos. Ativar o “snapshot” do storage para 21 dias do servidor de arquivos	Técnicos do NUTIC/SC	Servidor PRF	01/09/2018 a 30/06/2019
Levar o servidor de backup para outra Cidade.	Local disponível e infraestrutura	Chefe NUTIC/SC e Servidor PRF	01/09/2018 a 31/12/2018
Realizar auditoria no storage para eliminar arquivos duplicados ou que n estejam mais em uso	Técnicos do NUTIC/SC	Servidor PRF	01/09/2018 a 30/06/2019
Melhorar a política de segurança da informação, sendo responsabilidade dos chefes dos setores informar de imediato a saída de funcionário do núcleo	Definir política de segurança	Gerente de Segurança	01/09/2018 a 31/12/2018
Centralizar configurações em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de	Capacitação	Técnicos e Servidor PRF	01/09/2018 a 31/12/2018

ausência do responsável.			
Configurar outro servidor proxy para que possa assumir em casa de falha do principal e em Cidade diversa	Local disponível e infraestrutura	Chefe NUTIC/SC e Servidor PRF	01/09/2018 a 31/12/2018
Centralizar configurações em apenas um funcionário, mas com mais funcionários aptos a realizar em caso de ausência do responsável.	Capacitação	Técnicos e Servidor PRF	01/09/2018 a 31/12/2018
Diminuir o número de administradores de domínio e criar auditoria de todas as atividades realizadas pelos administradores	Capacitação	Técnicos e Servidor PRF	01/09/2018 a 31/12/2018
Configurar o servidor secundário para que possa assumir imediatamente após o principal ficar inoperante, sendo que aquele deverá replicar de forma instantânea as configurações do principal	Suporte especializado	Técnicos e Servidor PRF	01/09/2018 a 31/12/2018
Ativar as atualizações automáticas e programar para serem realizadas durante a madrugada	Técnicos do NUTIC/SC	Servidor PRF	01/09/2018 a 31/12/2018
AD secundário deve ser localizado em outra Cidade	Local disponível e infraestrutura	Chefe NUTIC/SC e Servidor PRF	01/09/2018 a 31/12/2018

ANEXO 9 – ANÁLISE DE IMPACTOS E TEMPO DE INDISPONIBILIDADE ACEITÁVEIS

Recurso	Impacto	Tempo admissível
Acesso à internet	Policiais sem atualizar sistemas informatizados. Usuários da rodovia sem conseguir imprimir documentos nas unidades. Fiscalização de veículos e pessoas prejudicada.	1 hora
WIFI	Policiais sem conseguir realizar consultas pelo aplicativo da PRF. Preenchimento de autos de infração e outros sendo feito de forma manual, reduzindo muito a agilidade do serviço.	1 hora para locais sem dados móveis. 4 horas para locais com dados móveis.
Radiocomunicação	Policiais sem comunicação rápida em situações de emergência, afetando inclusive, salvamento de pessoas.	4 horas em locais estratégicos 6 horas nos demais locais
Servidor de Arquivos	Serviço administrativo ficará inoperante, boa parte da documentação de todo o administrativo fica no servidor	3 horas
Proxy	Computadores sem acesso à internet, acessando apenas sites do governo.	1 hora
Firewall	Toda a rede é afetado com a interrupção do Firewall	1 hora
Active Directory	Novos logins, novas computadores não entrarão no domínio	8 horas