**PLANO DE CONTIGÊNCIA PARA O DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO DO CONSELHO REGIONAL DE ENGENHARIA E AGRONOMIA DO ACRE**

Um plano de contingência para T.I. (Tecnologia da Informação) é um conjunto de medidas e procedimentos pré-definidos que uma organização adota para lidar com eventos imprevistos ou desastres que possam afetar seus sistemas de tecnologia. O objetivo principal do plano de contingência é garantir a continuidade dos serviços de T.I. e minimizar os impactos negativos decorrentes de interrupções.

Um plano de contingência típico para T.I. geralmente inclui as seguintes etapas:

1. Análise de riscos: Identificação dos principais riscos que podem afetar os sistemas de T.I. da organização, como falhas de hardware, ataque de hackers, desastres naturais, entre outros.
2. Avaliação de impacto: Avaliação dos possíveis impactos desses riscos, incluindo perda de dados, interrupção dos serviços, danos financeiros, perda de reputação, entre outros.
3. Estratégias de mitigação: Desenvolvimento de estratégias e medidas para mitigar os riscos identificados. Isso pode incluir a implementação de medidas de segurança, redundância de sistemas, backup regular de dados, treinamento de funcionários, entre outros.
4. Plano de resposta a incidentes: Definição de um plano detalhado para responder a incidentes e lidar com interrupções. Isso envolve a designação de responsabilidades, a criação de uma cadeia de comunicação eficaz, a definição de procedimentos de resposta a incidentes e a realização de simulações e testes periódicos para garantir que o plano esteja atualizado e funcionando corretamente.
5. Recuperação de desastres: Definição de medidas para recuperar os sistemas de T.I. após um incidente grave. Isso pode incluir a restauração de backups, a recuperação de dados perdidos, a reparação de hardware danificado, entre outros.
6. Treinamento e conscientização: Realização de treinamentos regulares para os funcionários sobre os procedimentos do plano de contingência, além de promover a conscientização sobre a importância da segurança da informação e da adoção de boas práticas de T.I.

É importante ressaltar que um plano de contingência para T.I. deve ser revisado e atualizado regularmente para se adaptar às mudanças na infraestrutura de tecnologia e nos riscos enfrentados pela organização. Além disso, é essencial que o plano seja testado por meio de exercícios de simulação e que haja um processo contínuo de melhoria e aprimoramento.

Plano de Contingência para T.I. do Conselho Regional de Engenharia e Agronomia do Acre

1. Análise de riscos:
	* Identificar os principais riscos que podem afetar os sistemas de T.I., como falhas de hardware, falhas de software, ataques de hackers, desastres naturais, interrupções de energia, entre outros.
2. Avaliação de impacto:
	* Avaliar os possíveis impactos desses riscos, incluindo interrupção dos serviços, perda de dados, danos financeiros, perda de reputação, entre outros.
3. Estratégias de mitigação:
	* Implementar medidas de segurança, como firewalls, antivírus, sistemas de detecção de intrusões, para proteger os sistemas de T.I. contra ataques externos.
	* Realizar backups regulares dos dados críticos e armazená-los em locais seguros e fora das instalações principais.
	* Estabelecer redundância nos sistemas, incluindo servidores espelhados e fontes de energia alternativas, para garantir a disponibilidade contínua dos serviços.
	* Implementar políticas de acesso e controle de dados para garantir que apenas usuários autorizados tenham acesso aos recursos de T.I.
	* Manter os sistemas e software atualizados com as versões mais recentes e corrigir vulnerabilidades conhecidas.
	* Realizar auditorias de segurança periódicas para identificar possíveis vulnerabilidades e corrigi-las.
4. Plano de resposta a incidentes:
	* Definir um plano detalhado de resposta a incidentes, incluindo uma equipe de resposta composta por membros de diferentes áreas da organização.
	* Estabelecer uma cadeia de comunicação clara para notificar rapidamente as partes relevantes em caso de incidente.
	* Documentar os procedimentos a serem seguidos em diferentes tipos de incidentes, como violação de dados, falha de sistema ou interrupção de serviços.
	* Realizar treinamentos regulares para a equipe de resposta a incidentes, simulando cenários de crise e praticando os procedimentos de resposta.
5. Recuperação de desastres:
	* Estabelecer procedimentos de recuperação de desastres para restaurar os sistemas e serviços de T.I. após um incidente grave.
	* Manter backups atualizados e testados regularmente para garantir a integridade dos dados.
	* Estabelecer um local de recuperação alternativo onde os serviços possam ser restaurados em caso de danos às instalações principais.
	* Documentar os procedimentos de recuperação e designar responsabilidades claras para cada etapa do processo.
6. Treinamento e conscientização:
	* Realizar treinamentos regulares para os funcionários sobre as políticas de segurança da informação, boas práticas de T.I. e os procedimentos do plano de contingência.
	* Promover a conscientização sobre a importância da segurança da informação e incentivar os funcionários a relatarem quaisquer incidentes ou vulnerabilidades detectadas.
7. Revisão e melhoria contínua:
	* Realizar revisões periódicas do plano de contingência para garantir que esteja atualizado com as mudanças na infraestrutura de T.I. e nos riscos enfrentados.
	* Realizar exercícios de simulação regulares para testar a eficácia do plano de contingência e identificar áreas de melhoria.
	* Manter um processo contínuo de melhoria, atualizando o plano conforme necessário e implementando as lições aprendidas com incidentes anteriores.

É importante adaptar este plano de contingência às necessidades e características específicas do Conselho Regional de Engenharia e Agronomia do Acre, levando em consideração seus sistemas de T.I. existentes, recursos disponíveis e requisitos de segurança. Recomenda-se envolver profissionais de T.I. qualificados para auxiliar na criação e implementação do plano de contingência.