PLANO DE CONTINGÊNCIA E CONTINUIDADE DOS SERVIÇOS DA TECNOLOGIA E INOVAÇÃO

2025

Sumário

1. INTRODUÇÃO 4

1.1 Escopo 5

1.2 Aplicação 5

1.3 Vigência 5

2. GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO 6

3. DEFINIÇÕES 7

4. CENÁRIO ATUAL 9

4.1 Serviços Essenciais de TI 9

5. RESPONSABILIDADES 11

5.1. Diretoria de Tecnologia e Inovação 11

5.2. Servidores Públicos 11

6. NÍVEIS DE INCIDENTES 11

7. PRIORIDADES 12

8. PRINCIPAIS RISCOS 13

9. PROCEDIMENTOS PARA BACKUP 15

9.1. Backup 15

9.2. Restauração 15

10. PRINCIPAIS INCIDENTES E AÇÕES DE CONTINGÊNCIA 15

10.1. Problemas com Equipamentos 15

10.2. Monitoramento e Tratamento de Incidentes de Conectividade (Rede Interna e Externa) 16

10.3. Problemas com Acesso aos Sistemas / Serviços Internos da Prefeitura 17

10.4. Problemas com Falta de Energia Elétrica 18

10.4.1 Ordem de Comandos para Desligamento dos Servidores e Dispositivos 18

10.4.2 Ordem de Comandos para Religar os Servidores e Dispositivos 19

10.5. Falha Na Climatização Do Data Center 20

10.6. Ataques de *Malware*, *Ransomware* ou Vírus 20

10.7. Indisponibilidade de Sistemas / Serviços Essenciais 21

10.8. Falha de Software ou Atualização Mal Sucedida 22

10.9. Vazamento de Dados ou Acesso Não Autorizado 23
10.10. Desastres Naturais ou Estruturais 24
10.11. Outros Problemas 25
11. COMUNICAÇÃO 26
11.1. Quem Deve Comunicar 26
11.2. A Quem Comunicar 26
11.3. Como Comunicar 26

1. INTRODUÇÃO

Segundo a *Information Technology Infrastructure Library* (ITIL), a disponibilidade da Tecnologia da Informação (TI) é um elemento essencial para assegurar o funcionamento adequado das atividades de um órgão público municipal. Trata-se de garantir que sistemas, serviços e infraestrutura estejam disponíveis de forma contínua, confiável e alinhada às necessidades da administração e da população.

Considerando que incidentes e situações imprevistas podem ocorrer a qualquer momento, é fundamental que o município esteja preparado para responder de maneira organizada e eficiente.

A interrupção de serviços de TI pode trazer impactos relevantes, como a indisponibilidade de atendimento ao cidadão, atrasos em processos administrativos e riscos relacionados à perda de informações. Por essa razão, a adoção de práticas estruturadas de continuidade contribui para reduzir prejuízos e garantir maior estabilidade na prestação dos serviços públicos.

Conforme orienta o COBIT, o gerenciamento da continuidade busca minimizar os efeitos de eventos que possam comprometer os serviços. Para isso, é necessário manter um plano atualizado, baseado em análise de riscos e integrado às práticas de segurança da informação e gestão da disponibilidade.

O Plano de Contingência e Continuidade de Serviços de TI - PCCSTI reúne diretrizes, estratégias preventivas e procedimentos de resposta, com o objetivo de assegurar a manutenção dos serviços essenciais em situações de crise. Esse documento contempla a identificação de ameaças, a definição de responsabilidades e a previsão dos recursos necessários para a continuidade operacional, incluindo ações de contingência, recuperação de desastres e retomada das atividades da Diretoria de Tecnologia e Inovação.

1.1 Escopo

Este documento define um conjunto de estratégias de proteção (contingência, continuidade e recuperação) necessárias à continuidade dos serviços essenciais disponibilizados pela área de TI.

1.2 Aplicação

Este documento se aplica a todos os serviços de Tecnologia e Informação que são providos pela Administração Direta e Indireta do Município de Criciúma.

1.3 Vigência

O PCCSTI tem vigência de 4 (quatro) anos após a data de sua publicação. O documento será revisto anualmente e poderá ser atualizado de acordo com a necessidade.

2. GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TECNOLOGIA DA INFORMAÇÃO

A gestão de continuidade de serviços de Tecnologia da Informação (TI) refere-se à capacidade da organização de manter a prestação de serviços em níveis previamente definidos e acordados, mesmo após a ocorrência de interrupções. Seu objetivo é assegurar a continuidade das atividades essenciais, reduzindo impactos decorrentes de falhas ou desastres, bem como diminuindo vulnerabilidades por meio de práticas eficazes de análise e gerenciamento de riscos.

A Gestão de Continuidade de Serviços de TI (GCSTI) compreende atividades, tais como:

a) Avaliação do custo-benefício da adoção de práticas de continuidade;

b) Identificação e avaliação de riscos que possam comprometer a prestação dos serviços de TI;

c) Identificação dos serviços mais críticos e essenciais para a continuidade das atividades;

d) Planejamento das ações necessárias para implementação da continuidade;

e) Elaboração de planos de recuperação de serviços;

f) Definição e execução de testes periódicos;

g) Realização de auditorias para verificação da efetividade dos processos;

h) Alinhamento da GCSTI com o gerenciamento de mudanças, assegurando que alterações no ambiente tecnológico sejam avaliadas quanto aos seus impactos na continuidade dos serviços.

Dessa forma, a gestão de continuidade de serviços de TI deve assegurar que a infraestrutura e os serviços não permaneçam indisponíveis por períodos prolongados, garantindo condições adequadas para a retomada das operações.

Para a execução desse processo em situações de incidentes ou desastres, recomenda-se a adoção das seguintes ações:

a) Avaliação imediata dos riscos e impactos decorrentes da interrupção dos serviços;

b) Definição dos tempos de recuperação aceitáveis para cada serviço;

c) Identificação dos serviços prioritários, com adoção de medidas adicionais de proteção;

d) Definição da estratégia a ser utilizada para a restauração dos serviços;

e) Implementação de medidas preventivas e corretivas para redução de impactos;

f) Elaboração, manutenção e testes de um plano de recuperação detalhado, capaz de restabelecer os serviços dentro dos prazos definidos.

3. DEFINIÇÕES

I. Áreas Sensíveis: Áreas que sofrem fortes efeitos negativos quando atingidas pelas consequências do incidente.

II. Área Vulnerável: Área atingida pela extensão dos efeitos provocados por um evento de falha.

III. Contingência: Situação de risco com potencial de ocorrer, inerente as atividades, serviços e equipamentos, e que ocorrendo se transformará em uma situação de emergência. Diz respeito a uma eventualidade; possibilidade de ocorrer.

IV. *Backup*: Cópia de um sistema completo ou de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.

V. *Data Center*: ou Centro de Processamento de Dados, é um ambiente projetado para concentrar servidores, equipamentos de processamento e armazenamento de dados, e ativos de rede, como *switches*, roteadores, *firewalls*, central telefônica virtual, entre outros.

VI. Incidente: É o evento inesperado ou situação que altera a ordem normal das coisas, capaz de causar danos leves ou graves aos sistemas e aos equipamentos de TI. Toda ocorrência anormal, que foge ao controle de um processo, sistema ou atividade, da qual possam resultar danos aos sistemas e/ou equipamentos de TI da Prefeitura Municipal de Criciúma.

VII. Intervenção: É a atividade de atuar durante o incidente, seguindo planos de ações para corrigir ou minimizar os possíveis danos aos equipamentos e sistemas de TI.

VIII. *Firewall*: É uma solução de segurança baseada em hardware ou software que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

IX. *Malware:* Abreviação de "*malicious software*", é qualquer *software* criado para causar dano, roubo de informações ou prejuízo ao sistema.

X. *Ransomware*: Tipo de *malware* que bloqueia ou criptografa os dados da vítima e exige pagamento de resgate para restaurar o acesso.

XI. Vírus: Tipo de *malware* que se replica, infectando outros arquivos ou programas, e pode causar diversos danos ao sistema. Depende da execução do usuário para se espalhar.

XII. *Service Desk*: área responsável pelo atendimento de suporte técnico de TI, atuando como ponto único de contato para registros de incidentes e requisições dos usuários.

XIII. Situação de Emergência: Situação gerada por evento em um sistema ou equipamento que resulte ou possa resultar em danos aos próprios sistemas ou equipamentos ou ao desempenho do trabalho de servidores.

XIV. Máquina Virtual (VM - Virtual Machine): ambiente de computação definido por software que funciona como um computador físico isolado dentro de uma máquina física real (chamada de host ou hospedeiro).

XV. Ativos: equipamentos específicos que permitem estruturar uma rede de computadores, conectando as máquinas da empresa umas às outras e também conectando a organização à internet.

XVI. Monitoramento de link: é uma ferramenta que pode ser utilizada para monitoramento de rede e de acesso à Internet.

4. CENÁRIO ATUAL

Para que o PCCSTI seja efetivo, é necessário realizar a análise contínua do cenário atual da área de Tecnologia da Informação do órgão público municipal. Até o momento, o órgão dispõe dos seguintes ativos em seu inventário tecnológico:

a) 1 sala de Data Center;
b) 2 links de comunicação de dados;
c) 6 servidores de grande porte;
d) 70 sistemas de informação;
e) 649 impressoras;
f) 2.640 computadores;
g) 3.000 usuários;
h) 1 nobreaks de grande porte.

4.1 Serviços Essenciais de TI

Para o desenvolvimento do PCCSTI são considerados como serviços essenciais de TI, aqueles críticos e que se interrompidos podem causar impacto considerável. Neste sendo, a área de DTI considerada como serviços essenciais a serem resguardados por este PCCSTI os seguintes serviços de TI:

1. **Infraestrutura de TI**
    a) Conectividade (internet e rede interna);
    b) Servidores e armazenamento;
    c) Serviços em nuvem;
    d) Backup e recuperação de dados;
2. **Segurança da informação e controle de acesso**
    a) Autenticação de usuários;
    b) Controle de permissões;
    c) Monitoramento e proteção contra incidentes;
3. **Sistemas de atendimento essencial ao cidadão**
    a) Saúde;
    b) Assistência social;
    c) Protocolos e atendimentos;
    d) Ouvidoria;
4. **Arrecadação e tributação**
    a) Emissão de guias (IPTU, ISS);
    b) Nota fiscal eletrônica;
    c) Sistemas de receita;
5. **Sistemas administrativos e financeiros**
    a) Contabilidade, orçamento e execução financeira;
    b) Folha de pagamento;
    c) Compras e contratos;
6. **Comunicação institucional**
    a) E-mail corporativo;
    b) Telefonia;
    c) Ferramentas internas de comunicação;
7. **Transparência e serviços acessórios**
    a) Portal da transparência;

b) Site institucional e serviços informativos;

5. RESPONSABILIDADES

5.1. Diretoria de Tecnologia e Inovação

Compete à Diretoria de Tecnologia e Inovação adotar medidas preventivas e corretivas com o objetivo de mitigar os impactos decorrentes de incidentes, emergências ou situações que possam comprometer os sistemas, equipamentos ou a infraestrutura de Tecnologia da Informação da Administração Direta e Indireta do Município de Criciúma e coordenar as ações de resposta e recuperação dos serviços de TI, garantindo a continuidade operacional e a rápida normalização dos serviços essenciais.

5.2. Servidores Públicos

Compete aos servidores públicos comunicar imediatamente à Diretoria de Tecnologia e Inovação a ocorrência ou suspeita de incidentes, falhas ou situações de risco que possam afetar os sistemas, equipamentos ou a infraestrutura de TI, especialmente em áreas consideradas sensíveis.

6. NÍVEIS DE INCIDENTES

1. Nível I – Situação de baixo impacto, passível de resolução pela equipe de TI, que não compromete a continuidade da prestação de serviços aos cidadãos. Exemplo: falhas em equipamentos periféricos, como teclado, mouse ou impressora.

2. Nível II – Situação de impacto moderado, que impede a utilização de equipamento ou sistema, comprometendo a continuidade da prestação de serviços aos cidadãos.
   Exemplo: computador inoperante (não liga, travamentos) ou indisponibilidade de sistemas específicos.

3. Nível III – Situação de alto impacto, que compromete o funcionamento de sistemas ou da infraestrutura de TI de forma ampla, afetando múltiplos setores ou toda a Administração Pública Municipal.
   Exemplo: indisponibilidade de conexão com a internet, falhas em servidores centrais, interrupção de energia no ambiente de data center ou problemas na rede corporativa.

7. PRIORIDADES

A definição de prioridade no atendimento de incidentes deve observar critérios técnicos e objetivos, alinhados às boas práticas de gestão de serviços de TI. Nesse contexto, adota-se como referência o ITIL, que estabelece a priorização a partir da análise conjunta de dois fatores: impacto e urgência.

a) **Impacto:** refere-se à abrangência do incidente, considerando a quantidade de usuários, sistemas ou unidades afetadas, como setores administrativos, escolas, unidades de saúde, entre outros.
b) **Urgência:** está relacionada ao tempo aceitável para a resolução do incidente, levando em conta a criticidade do serviço afetado. Situações que impactam serviços essenciais e contínuos, como atendimentos de saúde ou atividades educacionais, demandam tratamento prioritário.

A combinação desses dois fatores permite classificar e priorizar os incidentes de forma adequada, assegurando uma resposta proporcional à criticidade e aos efeitos gerados na prestação dos serviços públicos. Conforme quadro 1 abaixo:

Quadro 1 - Matriz de risco

		IMPACTO			
		Crítico	**Alto**	**Médio**	**Baixo**
URGÊNCIA	**Muito Alta**	Crítica	Alta	Alta	Média
	Alta	Alta	Alta	Média	Média
	Média	Alta	Média	Média	Baixa
	Baixa	Média	Média	Baixa	Baixa

8. PRINCIPAIS RISCOS

O quadro 2 define os principais riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

Quadro 2 – Lista de Riscos e Parâmetros

Item	Riscos	Parâmetros
1.	Interrupção de energia elétrica	Causada por fator externo à rede elétrica do prédio ou de sua localidade com duração da interrupção superior a 180 (cento e oitenta) minutos. Causada por fator interno que comprometa a rede elétrica do prédio com curto-circuito, incêndio e infiltrações.
2.	Falha na climatização do *Data Center*	Superaquecimento dos ativos devido a falha no sistema de refrigeração.
3.	Indisponibilidade da rede de comunicação de computadores	Rompimento de cabos decorrente de execuções de obras internas ou externas, desastres ou acidentes.

4.	Falha humana	Acidente ao manusear equipamentos, ações equivocadas de usuários ou técnicos, como desligamento acidental de servidores, exclusão de arquivos/sistemas ou configurações inadequadas em equipamentos.
5.	Ataques internos	Ataque aos ativos do *Data Center* e equipamentos de TI.
6.	Falha de hardware	Falha que necessite de reposição de peça ou reparo, cujo reparo dependa de aquisição por processo licitatório.
7.	Ataque externo	Ataque virtual que comprometa o desempenho, acesso aos os dados ou configuração dos serviços essenciais.
8.	Falha de conectividade com a internet	Queda total ou intermitência nos links de internet (principal e redundante), impactando sistemas online, e-mails e comunicação com serviços em nuvem.
9.	Ataques de *malware*, *ransomware* ou vírus	Detecção de softwares maliciosos que comprometam dados, infraestrutura ou provoquem criptografia indevida de arquivos/sistemas.
10.	Indisponibilidade de sistemas essenciais	Queda de sistemas críticos, protocolo, contabilidade, sistema de saúde/educação, por falhas internas ou externas.
11.	Falha de software ou atualização mal sucedida	Instalações ou atualizações que causam instabilidade, incompatibilidade ou perda de funcionalidade em sistemas operacionais ou aplicações críticas.
12.	Vazamento de dados ou acesso não autorizado	Ocorrência de falhas de segurança que permitam o acesso indevido a informações sensíveis (dados de servidores, cidadãos ou sistemas internos).
13.	Falha no sistema de backup	Inviabilidade de realizar cópias de segurança ou de restaurar dados a partir de backups, comprometendo a continuidade dos serviços em caso de incidente.
14.	Desastres naturais ou estruturais	Enchentes, incêndios, desabamentos, ventanias ou qualquer evento que comprometa fisicamente os equipamentos e as instalações do ambiente de TI.
15.	Interrupção de serviços em nuvem	Queda ou lentidão dos serviços hospedados externamente (ex: e-mails, sistemas SaaS), afetando a operação normal.

9. PROCEDIMENTOS PARA BACKUP

9.1. Backup

Os servidores estão configurados para a realização automática de rotinas de backup diário a partir das 19h, contemplando os servidores virtuais, incluindo servidores de arquivos, hospedados no Data Center.

Os dados são copiados para dois destinos distintos: um servidor de backup interno ao próprio Data Center e um servidor de backup externo, visando maior segurança e redundância das informações, os backups são mantidos por um período de até 7 (sete) dias corridos, além da retenção de cópias mensais e anuais.

9.2. Restauração

A restauração de dados deve ser solicitada a Diretoria de TI e será realizada de acordo com os procedimentos específicos do mesmo. A verificação e o teste de restauração, serão realizados sempre que possível por meio de um software de backup, configurado para verificar automaticamente as condições do backup.

O tempo necessário para a restauração dos dados poderá variar de acordo com a quantidade e o tamanho dos arquivos a serem restaurados.

10. PRINCIPAIS INCIDENTES E AÇÕES DE CONTINGÊNCIA

10.1. Problemas com Equipamentos

Os servidores públicos que enfrentarem problemas técnicos ou necessitarem de suporte deverão acionar a DTI por meio de um dos seguintes canais:

- Atendimento presencial, dirigindo-se diretamente à DTI

- Telefone: (48) 3431-0272 ou ramal 2300;
- E-mail: suporte@criciuma.sc.gov.br
- Protocolo Digital: https://protocolo.criciuma.sc.gov.br

Após o recebimento da solicitação, a equipe técnica realizará o registro do chamado no sistema de Service Desk, o qual será atribuído a um técnico responsável pelo atendimento. Concluído o atendimento, o solicitante será devidamente notificado quanto à solução adotada ou ao encerramento do chamado.

Nos casos em que o problema comprometer a continuidade das atividades, a equipe de suporte realizará atendimento no local, para efetuar uma análise inicial e, sempre que possível, promover a solução imediata. Não sendo possível a resolução no primeiro atendimento, o profissional será direcionado para outra estação de trabalho disponível.

10.2. Monitoramento e Tratamento de Incidentes de Conectividade (Rede Interna e Externa)

A DTI realizará o monitoramento contínuo da infraestrutura de rede, incluindo a rede interna e a conectividade externa (links de internet), por meio de ferramentas específicas e sistemas de firewall, que permitem a identificação de falhas e a localização de sua origem.

Caso o incidente não seja identificado automaticamente, o setor afetado deverá comunicar a ocorrência pelos canais oficiais de atendimento.

Uma vez detectado o incidente, serão adotados os seguintes procedimentos:

- Análise inicial: verificação dos sistemas de monitoramento, firewall, links de internet e componentes da rede interna, com o objetivo de identificar a origem da falha (interna ou externa);
- Diagnóstico técnico: realização de testes e validações em equipamentos de rede, tais como switches, roteadores, cabeamento e configurações de

firewall, podendo incluir reinicialização controlada dos dispositivos, quando necessário;

- Validação com o local afetado: contato com a unidade impactada para coleta de informações adicionais e delimitação da abrangência do incidente;
- Escalonamento: em casos de falhas externas, será realizado contato com o provedor de internet para análise e resolução conjunta;
- Atendimento presencial: não sendo possível a resolução remota, um técnico será deslocado para atendimento in loco, visando a identificação e correção do problema.

Nos casos em que a indisponibilidade afetar múltiplas unidades, o incidente será tratado com prioridade elevada, considerando seu impacto na continuidade dos serviços. Sempre que possível, a equipe de TI deverá comunicar aos setores afetados a previsão para a normalização dos serviços.

10.3. Problemas com Acesso aos Sistemas / Serviços Internos da Prefeitura

A DTI adotará os seguintes procedimentos para tratamento de incidentes relacionados a sistemas e serviços hospedados em ambiente virtualizado:

- Verificação da máquina virtual (VM): confirmação do estado da máquina virtual no ambiente virtualizado, a fim de identificar se o sistema ou serviço encontra-se em execução;
- Reinicialização da VM: caso a máquina virtual não esteja em funcionamento, será realizada sua inicialização ou reinicialização, seguida de testes de acesso ao sistema ou serviço;
- Ação corretiva por meio de backup: na hipótese de falha crítica ou perda de dados, será acionado o processo de restauração de backup, podendo

abranger a recuperação completa da máquina virtual ou de arquivos e sistemas específicos;

- Comunicação com os setores envolvidos: após a análise e o início das ações corretivas, a DTI informará aos setores impactados a previsão de restabelecimento dos serviços, mantendo-os atualizados quanto ao andamento da resolução.

10.4. Problemas com Falta de Energia Elétrica

Em caso de identificação de queda ou ausência total de energia elétrica no Paço Municipal, deverão ser adotadas as seguintes providências:

- Comunicar imediatamente o setor responsável (obras/manutenção) para as devidas verificações e ações corretivas;
- Verificar se a interrupção de energia é de origem interna ou externa;

Na hipótese de interrupção com duração de até 4 (quatro) horas, os sistemas e servidores de rede poderão permanecer em funcionamento, uma vez que estão conectados ao nobreak central dedicado ao Data Center.

Caso a interrupção ultrapasse 4 (quatro) horas, deverá ser realizado o desligamento controlado dos sistemas e equipamentos, com o objetivo de preservar a integridade da infraestrutura. O religamento será efetuado de forma segura após o restabelecimento do fornecimento de energia elétrica.

10.4.1 Ordem de Comandos para Desligamento dos Servidores e Dispositivos

O desligamento dos servidores e dispositivos de infraestrutura deverá ser tratado sempre como última alternativa, sendo realizado apenas em situações estritamente necessárias, como manutenções programadas, riscos elétricos,

incidentes críticos ou indisponibilidades que exijam a interrupção controlada do ambiente. Tais equipamentos não devem ser desligados rotineiramente no dia a dia, considerando que o processo de desligamento e reinicialização pode demandar elevado tempo para restabelecimento completo dos serviços.

Para garantir a integridade dos sistemas e equipamentos, o desligamento deverá seguir a seguinte ordem:

- Acessar o ambiente virtualizado e realizar o desligamento controlado dos servidores virtuais responsáveis pelos serviços;
- Proceder com o desligamento dos servidores físicos;
- Desligar os demais dispositivos de rede, incluindo switches (core do Data Center e de borda nas salas técnicas), roteadores, ONUs, central telefônica virtual e equipamentos de rede sem fio (Wi-Fi).

O processo deve ser conduzido de forma controlada, evitando desligamentos abruptos que possam comprometer dados ou a integridade dos equipamentos.

10.4.2 Ordem de Comandos para Religar os Servidores e Dispositivos

Para o restabelecimento dos serviços de TI, a inicialização dos equipamentos deverá seguir a seguinte ordem:

- Ligar os dispositivos de rede, incluindo switches (core do Data Center e de borda nas salas técnicas), roteadores, ONUs, central telefônica virtual e equipamentos de rede sem fio (Wi-Fi);
- Ligar os servidores físicos;
- Verificar se as máquinas virtuais foram inicializadas automaticamente;
- Caso não tenham sido iniciadas, identificar a causa e proceder com a inicialização manual;

A sequência de inicialização das máquinas virtuais deve priorizar os serviços essenciais, na seguinte ordem: AD01, AD02, servidor de impressão

(Print Server), servidores de arquivos e servidores de banco de dados. Em seguida, devem ser iniciados os demais servidores.

10.5. Falha Na Climatização do Data Center

A DTI realiza o monitoramento contínuo da temperatura do Data Center por meio de sensores específicos. Na ocorrência de falha no sistema de climatização, serão adotadas as seguintes medidas:

- Acionamento da equipe de manutenção predial: para avaliação e correção do sistema de climatização;
- Atendimento técnico especializado: verificação do funcionamento dos equipamentos de ar-condicionado e dos sensores de temperatura;
- Adoção de medidas emergenciais: utilização de ventilação auxiliar, quando necessário, para redução da temperatura ambiente;
- Desligamento controlado de equipamentos não críticos: com o objetivo de evitar superaquecimento e preservar a infraestrutura essencial;
- Registro da ocorrência: documentação detalhada do incidente, incluindo evidências, medições de temperatura e ações executadas;
- Análise posterior: revisão do ocorrido e definição de melhorias, incluindo estratégias de redundância e prevenção.

10.6. Ataques de *Malware*, *Ransomware* ou Vírus

Ataques de *software* malicioso representam riscos graves à integridade, disponibilidade e confidencialidade das informações públicas. Ao identificar um incidente do tipo, são adotadas as seguintes ações:

- Isolamento imediato do dispositivo: O equipamento afetado é desconectado da rede física e lógica (Wi-Fi, cabo, VPN), para impedir a propagação do ataque.

- Análise preliminar do incidente: São verificados sinais de infecção, como lentidão, arquivos criptografados, mensagens de resgate, execução automática de programas, ou atividades suspeitas nos processos.
- Execução de varredura completa: Utiliza-se softwares de detecção e remoção de ameaças (antivírus corporativo, *antimalware* e ferramentas forenses) com bases atualizadas.
- Verificação da extensão da infecção: A análise inclui compartilhamentos de rede, servidores e dispositivos próximos ao afetado.
- Limpeza ou formatação: Se possível, o malware é removido preservando os dados.
- Em caso de *ransomware* ou danos irreversíveis, o equipamento é formatado e restaurado com backup válido.
- Restauração de arquivos comprometidos: Apenas por backups seguros e verificados, garantindo que não contenham arquivos infectados.
- Atualização de todos os sistemas e antivírus da rede: Incluindo verificação da base de assinaturas e aplicação de correções de segurança.
- Registro do incidente e notificação: O caso é documentado e, se envolver tentativa de extorsão ou dados sensíveis, comunicado à Procuradoria Geral do Município.
- Capacitação e alerta preventivo: É enviada comunicação interna alertando os servidores sobre o incidente, reforçando cuidados com e-mails suspeitos, links desconhecidos e downloads.

10.7. Indisponibilidade de Sistemas / Serviços Essenciais

Sistemas ou serviços essenciais são aqueles cuja paralisação pode afetar diretamente o funcionamento da Prefeitura, tais como: folha de pagamento, protocolo, saúde, educação, arrecadação, contabilidade e patrimônio.

Quando ocorre a indisponibilidade de um desses sistemas:

- Detecção e priorização imediata: O sistema afetado é identificado por usuários ou pelo monitoramento, sendo classificado como prioridade crítica;
- Abertura de chamado com status de urgência: A equipe de TI registra o incidente com detalhamento técnico e operacional;
- Ativação do suporte técnico especializado: Se for um sistema contratado, o fornecedor é acionado com prioridade máxima;
- Disponibilização de alternativas provisórias: Planilhas e formulários digitais, uso de sistemas auxiliares ou temporários;
- Geração de relatório final: Incluindo causa-raiz, impacto, tempo de inatividade, setores afetados, medidas adotadas e recomendações preventivas.

10.8. Falha de Software ou Atualização Mal Sucedida

Atualizações de sistemas, drivers, bibliotecas ou sistemas operacionais podem falhar e comprometer o funcionamento normal de serviços. Nestes casos, a resposta técnica segue estas etapas:

- Identificação imediata da falha: Observada por erro na aplicação, comportamento anômalo ou relato de usuários após uma atualização.
- Verificação da compatibilidade: Avalia-se se o pacote de atualização era compatível com a infraestrutura atual (sistema operacional, banco de dados, bibliotecas).
- Execução de restauração:
    - Caso exista ponto de restauração da máquina virtual, realiza-se a reversão para o estado anterior.
    - Em ambientes sem esse recurso, o sistema é reinstalado com a versão funcional anterior.
- Avaliação do impacto da falha:

- Determina-se se a falha afetou apenas um usuário, um setor ou toda a rede.
- Verifica-se se houve perda ou dano de dados.

- Contato com o fornecedor ou desenvolvedor: Para obter correções ou orientações técnicas específicas.
- Realização de testes em ambiente controlado: Antes de aplicar novamente a atualização, ela é testada em máquina de homologação, simulando o ambiente de produção.
- Ajuste no processo de atualização: Incluindo definição de janelas de manutenção, aviso prévio aos usuários e criação de pontos de restauração automáticos.
- Documentação detalhada: Incluindo o pacote afetado, o comportamento observado, a solução aplicada e as boas práticas a seguir nas próximas atualizações.

10.9. Vazamento de Dados ou Acesso Não Autorizado

A ocorrência de vazamento de dados sensíveis ou acesso não autorizado a sistemas da Administração Pública deve ser tratada com rigor, considerando os impactos legais e operacionais envolvidos. Ao identificar ou receber denúncia de incidente desse tipo, as seguintes ações são adotadas:

- Isolamento imediato: O usuário ou sistema envolvido é bloqueado da rede e dos acessos, evitando a continuidade do vazamento.
- Análise de logs e rastreamento de atividades: São coletadas evidências através de registros de acesso, movimentação de dados e logs de sistema, para identificar a origem e a extensão do vazamento.
- Avaliação do impacto: É realizada uma análise do tipo de informação exposta (dados pessoais, sigilosos, financeiros, etc.), da quantidade de dados e dos sistemas comprometidos.

- Notificação obrigatória: Caso se trate de dados pessoais, o incidente será reportado à Autoridade Nacional de Proteção de Dados (ANPD), conforme previsto na Lei Geral de Proteção de Dados (LGPD – Lei nº 13.709/2018).
- Comunicação interna e externa: A equipe de TI comunica formalmente à alta gestão e os setores envolvidos, e, se necessário, orienta os titulares dos dados sobre as medidas de mitigação.
- Revisão de permissões e acessos: Todas as credenciais envolvidas são analisadas, e pode ser realizado um recadastramento de senhas e perfis de acesso nos sistemas.
- Reforço da segurança da informação: Após o incidente, são adotadas medidas preventivas, como a atualização de políticas internas e capacitação dos servidores.
- Elaboração de relatório técnico: Todo o processo é documentado, com descrição do incidente, ações tomadas, tempo de resposta e medidas de prevenção futuras.

10.10. Desastres Naturais ou Estruturais

Em situações extraordinárias como enchentes, incêndios, desmoronamentos, vendavais ou outros eventos naturais/estruturais que comprometam a integridade física dos ativos de TI, a Diretoria de Tecnologia e Inovação adota medidas emergenciais conforme plano de contingência:

- Acionamento do plano de contingência de TI: A equipe segue os procedimentos previamente definidos para continuidade dos serviços críticos em situações de emergência.
- Avaliação da segurança local: Em parceria com a Defesa Civil e a equipe de manutenção predial, é verificada a segurança do ambiente antes de qualquer ação técnica.

- Desligamento controlado dos sistemas: Sempre que possível, os equipamentos de TI são desligados de forma segura para evitar danos por curto-circuito ou superaquecimento.
- Proteção e realocação de equipamentos: Computadores, Notebooks, Servidores e roteadores e equipamentos de rede em geral de menor porte são removidos do local de risco e armazenados em ambiente seguro.
- Redirecionamento dos serviços essenciais: Caso necessário, os principais sistemas e serviços de dados são restaurados a partir de backup em local secundário (site backup ou unidade de contingência).
- Avaliação de danos e recuperação: Após a contenção da situação, é realizada a vistoria técnica para mensurar prejuízos e iniciar os procedimentos de recuperação dos sistemas e da infraestrutura.
- Relatório de incidente e atualização de riscos: Um relatório completo é gerado, incluindo o evento, os danos sofridos, as ações tomadas e as propostas de melhoria na prevenção e resposta futura.

10.11. Outros Problemas

Para qualquer outro tipo de problema que envolva a TI, como impressoras, problemas de acesso que envolvam login e senha e etc.

Os passos a serem seguidos são:

- O usuário deve informar a Diretoria de Tecnologia de Inovação por um dos seguintes meios:
  - Atendimento presencial, dirigindo-se diretamente a DTI;
  - Telefone (48) 3431 0272, ou pelo ramal 2300;
  - E-mail: suporte@criciuma.sc.gov.br
  - Protocolo Digital: https://protocolo.criciuma.sc.gov.br

Após o recebimento da solicitação, a equipe técnica realizará o registro do chamado no sistema de Service Desk, que será atribuído a um técnico responsável pelo atendimento.

Após o atendimento o solicitante é informado da conclusão/resolução do problema.

11. COMUNICAÇÃO

11.1. Quem Deve Comunicar

Qualquer profissional da administração pública direta e indireta de Criciúma, que detecte qualquer tipo de problema ou anomalia, referente aos sistemas, equipamentos e/ou infraestrutura de TI.

11.2. A Quem Comunicar

As ocorrências devem ser comunicadas a Diretoria de Tecnologia e Inovação da Prefeitura Municipal de Criciúma.

11.3. Como Comunicar

A comunicação pode ser realizada por meio de um dos seguintes canais:

- Atendimento presencial, dirigindo-se diretamente a DTI;
- Telefone (48) 3431 0272, ou pelo ramal 2300;
- E-mail: suporte@criciuma.sc.gov.br
- Protocolo Digital: https://protocolo.criciuma.sc.gov.br

Este documento poderá ser revisado, atualizado e corrigido a qualquer tempo, conforme alterações nos processos, necessidades operacionais, adequações técnicas, legais ou normativas da Administração Pública Municipal.