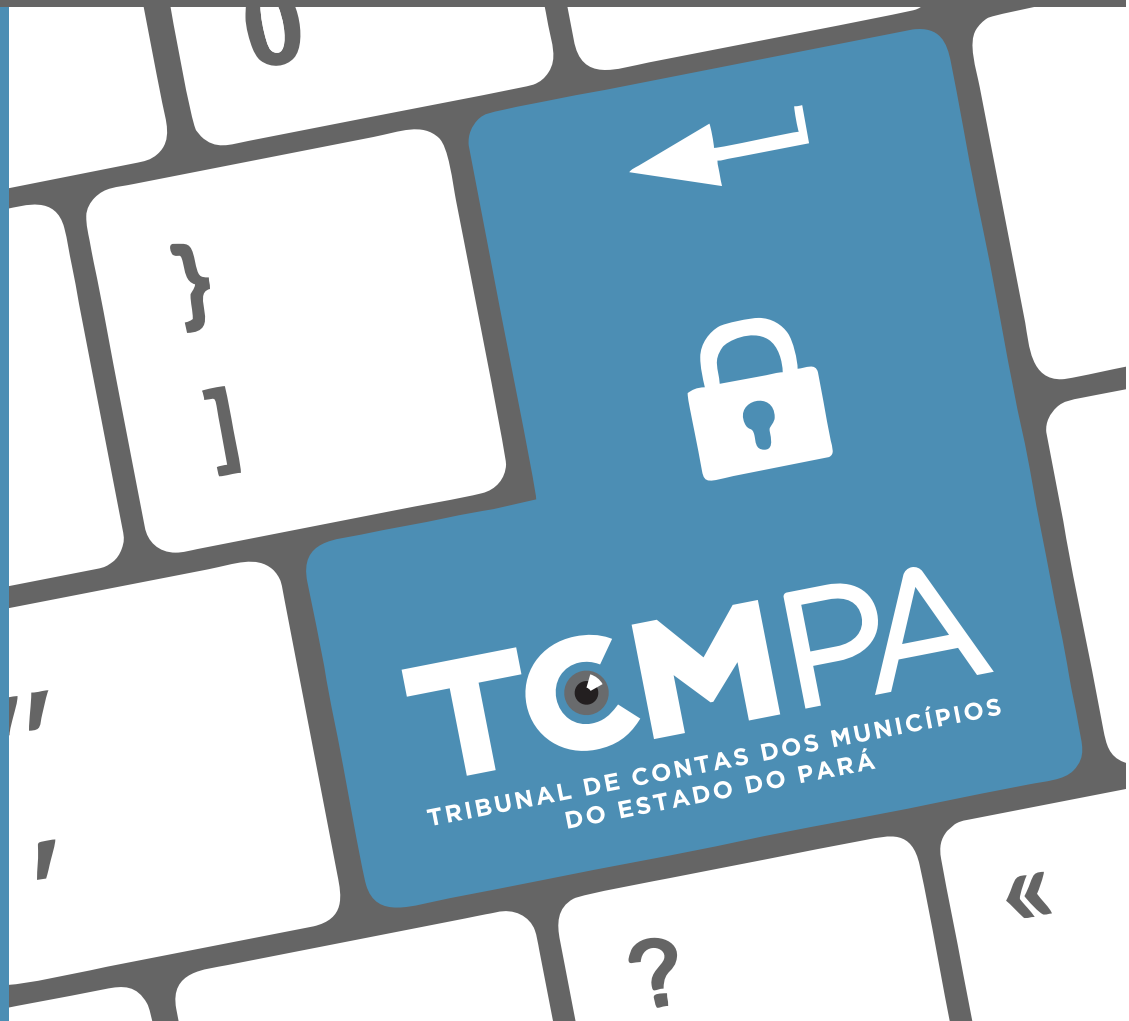
SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ORIENTAÇÃO PARA O SERVIDOR



2018

TRIBUNAL DE CONTAS DOS MUNICÍPIOS DO ESTADO DO PARÁ

▪ COMPOSIÇÃO ▪

Luiz Daniel Lavareda Reis Junior - **Conselheiro Presidente**

Mara Lúcia Barbalho da Cruz - **Conselheira Vice-Presidente**

José Carlos Araújo - **Conselheiro Corregedor**

Aloisio Augusto Lopes Chaves - **Conselheiro Ouvidor**

Conselheiros:

Antônio José Costa de Freitas Guimarães

Francisco Sérgio Belich de Souza Leão

Sebastião Cezar Leão Colares

Idealização, adaptação e revisão:
Núcleo de Informações Estratégicas

**Projeto gráfico,
diagramação e ilustração:**
Assessoria de Comunicação

Referência de sites utilizados nas pesquisas:
Adaptado da Cartilha de Segurança da Informação do Ministério do Planejamento, Orçamento e Gestão.
http://www.planejamento.gov.br/servicos/central0de-conteúdo/publicacoes/cartilha_sic.pdf

Site Certbr: http://cartilha.cert.br/

Leitores podem entrar em contato pelos e-mail:
nie@tcm.pa.gov.br

▪ SUMÁRIO ▪

▪ APRESENTAÇÃO ▪

A Segurança da Informação e Comunicações não está restrita apenas a sistemas computacionais, informações eletrônicas ou qualquer outra forma mecânica de armazenamento. Ela está relacionada com a proteção existente ou necessária sobre dados, informações ou documentos que possuem valor para alguém ou uma organização.

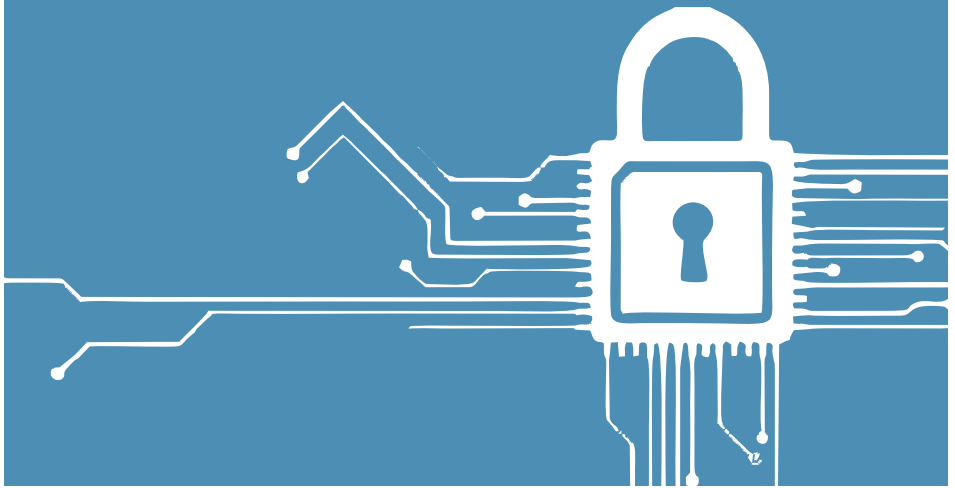
A segurança é obtida através de padrões e medidas de proteção capazes de neutralizar ameaças contra alguém ou alguma coisa. Possui como propriedades básicas: disponibilidade, integridade, confidencialidade e autenticidade da informação. Por isso, torna-se da maior importância a educação para o uso ético, seguro e legal das tecnologias e das informações, pois o seu uso inadequado pode criar vulnerabilidades que comprometam as instalações, serviços e bens, comprometendo assim as propriedades básicas da informação.

Ciente da importância estratégica em controlar e garantir a proteção da informação e manter e zelar pela integridade e sigilo

Ciente da importância estratégica de controlar e garantir a proteção da informação e sigilo dos dados corporativos, o Tribunal de

Contas dos Municípios do Estado do Pará desenvolveu a cartilha "*Segurança da Informação e Comunicação*". Este é um manual do órgão, referente as políticas de segurança da informação e comunicação, que busca esclarecer o compromisso com a proteção dos dados da propriedade e/ou guarda, devendo ser cumprida por todos os servidores e colaboradores.

Nesta cartilha, abordaremos os principais aspectos que possam levar a cada um dos servidores e demais colaboradores do Tribunal de Contas dos Municípios do Estado do Pará (TCM/PA) a uma reflexão para mudança de atitudes pessoais e profissionais que assegurem a proteção dos recursos de informação e comunicações do TCM-PA.



1 A SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO -SIC

O que é informação?

É todo e qualquer conteúdo,dotado de valor, para uma pessoa ou organização.

Qual o valor da informação?

Na sociedade atual, muitas vezes referenciada como Sociedade da Informação ou Sociedade do Conhecimento, a informação é um ativo estratégico, apontada como o principal patrimônio de uma organização. E, como tal, permanece sob constante risco.

Qual o papel da Segurança da Informação e Comunicações – SIC?

A SIC compreende um conjunto de iniciativas cujo objetivo é assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações. Deve contemplar todo o ciclo de vida da informação, desde a elaboração, transmissão, recepção e tratamento até seu descarte, independente dos meios empregados nestes processos.

Tendo em vista o valor estratégico da informação, sua segurança tornou-se crucial.

2 PORPRIEDADES BÁSICAS A SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO -SIC

Para referenciar as propriedades da segurança da informação é comum utilizar o acrônimo **DICA** (Disponibilidade, Integridade, Confidencialidade e Autenticidade).

DICA

Disponibilidade: propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade. Proteger essa propriedade significa assegurar ao usuário o acesso à informação, sempre que ela precisar.

Integridade: propriedade de que a informação não seja modificada ou destruída de maneira não autorizada ou acidental. Protegê-la significa assegurar que nada foi acrescentado,retirado ou modificado sem a explícita permissão do seu proprietário.

Confidencialidade: propriedade de que a informação nãoseja revelada ou disponibilizada a indivíduo, entidade,orgão ou sistema, não autorizado ou não credenciado.Dados privados ou com algum grau de sigilo devem ser apresentados somente ao(s) seu(s) dono(s) ou ao(s) grupo(s) com a devida permissão para tal.

Autenticidade: propriedade de que a informação seja produzida, expedida, modificada ou destruída por indivíduo, entidade, órgão ou sistema, devidamente identificado ou certificado.

3 O QUE TENHO A VER COM A SIC?

A segurança de uma determinada informação pode ser afetada por fatores comportamentais, pelo ambiente ou infraestrutura que a cerca ou ainda por pessoas mal-intencionadas, que tem o objetivo de furtar, destruir ou modificar os dados para fins ilícitos.

Para que toda informação possa servir adequadamente ao seu propósito, sem prejudicar quaisquer pessoas ou instituições, é necessária a gestão segura dos recursos que lidam com essas informações.

A SIC vai muito além da tecnologia da informação. Mais do que isso, ela está intimamente relacionada ao nosso comportamento e nossas atitudes. Assim, exige-se, em tempos de inclusão digital, uma mudança de comportamento, tendo em vista o potencial lesivo da velocidade com que correm as informações nos meios digitais, como a Internet, por exemplo.

Torna-se necessário que os conceitos relacionados à segurança da informação sejam compreendidos e seguidos por todos os servidores, autoridades e colaboradores do TCM-PA, na vida pessoal e profissional. Todos devem ter um compromisso com a disponibilidade, integridade, confidencialidade e autenticidade (DICA) das informações da nossa instituição.

SIC na vida pessoal

Celulares e tablets sem senha ou sistema de bloqueio. O que pode acontecer se eu deixar assim?

Os celulares e *tablets* têm sido cada vez mais utilizados para armazenamento de dados. Agenda de contatos, mensagens com conversas pessoais, e-mails e arquivos, dentre outros, podem estar facilmente disponíveis para alguém mal-intencionado utilizar, caso você não faça uso de senhas ou sistemas de bloqueio da tela. Para que você consiga utilizar estes recursos, disponíveis na maioria dos dispositivos atuais, leia o manual do equipamento ou entre em contato com o suporte técnico e solicite orientações sobre como implementar esta simples, mas importante medida preventiva.

Proteja sua informação pessoal! Coloque senha e bloqueio de tela em seus dispositivos pessoais.

Engenharia Social: O que é e como me afeta?

São ações feitas por pessoas mal intencionadas, para obter acesso a informações importantes ou sigilosas de pessoas ou organizações, por meio da enganação ou exploração da confiança dos indivíduos.

Para isso, o golpista pode se passar por outra pessoa, assumir outra personalidade e até fingir que é um profissional de determinada área. Ele explora as emoções e fragilidades das pessoas que, quando não treinadas ou preparadas para se defender desses ataques, podem ser facilmente manipuladas. Na dúvida, não passe suas informações! Elas podem ser indevidamente divulgadas e trazer sérios riscos à você e sua família.

Cuide das informações sob sua responsabilidade. Só lembrando da real importância quando perdemos ou quando precisamos dela.

AS SUAS INFORMAÇÕES ESTÃO SEGURAS?

Não dê informações pessoais por telefone, e-mail ou mensagem, a não ser que você tenha absoluta certeza de quem está pedindo.

ORIENTE SEUS FAMILIARES E SEUS FUNCIONÁRIOS!

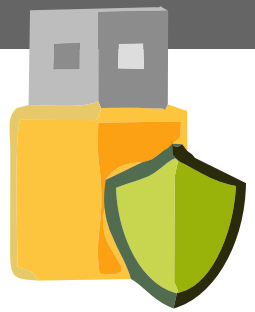
Você consegue, ao entrar em um site, identificar se é falso? Saiba como se proteger em https://cartilha.cert.br/golpes

Phishing

Do inglês *"fishing"*, vem de uma analogia criada pelos fraudadores, onde "iscas" (mensagens eletrônicas) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

Comprar ou transacionar via internet pode ser muito prático e fácil! Mas e se o site for falso?

As opções de compras e de transações bancárias via internet estão cada vez mais numerosas, acessíveis e amigáveis. Contudo, existem *sites* maliciosos que simulam os *sites* reais para roubar informações e dinheiro dos usuários (conhecido como *phishing – veja ao lado*). Se desconfiar de qualquer coisa, feche imediatamente o navegador e contate a empresa através do telefone fixo para confirmar o endereço e os dados apresentados.



Pen drive e HDs externos com informações pessoais. E se eu perder?

Com o aumento de capacidade das mídias removíveis, é cada vez maior a quantidade de informações que estão gravadas em HDs externos e nos pequenos Pen-drives.

Todas estas mídias podem se tornar um ponto fraco na segurança dos seus dados. Imagine um Pen-drive recheado de informações particulares (ou mesmo sensíveis para sua empresa) "dando sopa" por aí. Nada agradável, certo?

Exatamente pensando nisto alguns fornecedores criaram aplicativos que permitem que você defina uma senha de acesso para estas informações gravadas. Assim, mesmo no caso de perda ou roubo do dispositivo, suas informações estarão a salvo.

Tenha os dispositivos móveis (pen drives e Hds externos) sempre com você ou guarde-os em local seguro, sem se esquecer da utilização de **ferramentas que protegem os dados** neles armazenados.

Defina senhas para acesso a sua rede sem fio (Wi-fi) doméstica! Saiba como se proteger em: http://cartilha.cert.br/redes/

Rede sem fio (Wi-Fi) em casa. Como devo me proteger?

Redes Wi-Fi se tornaram populares pela mobilidade que oferecem, pela conveniência e facilidade de uso em diferentes tipos de ambientes. Por terem instalação bastante simples, muitas pessoas as instalam em casa sem qualquer cuidado com configurações mínimas de segurança.

Pessoas mal intencionadas podem fazer uso de sua rede de forma não autorizada e, inclusive, ter acesso a dados e arquivos dos computadores e dispositivos de sua rede doméstica.

Contas e formulários financeiros disponíveis com seus dados. Será que alguém pode se aproveitar?

O fim do mês chega e, junto com ele, contas e mais contas para pagar. Mas o que fazemos com os recibos, boletos e afins? Guardamos em ambientes seguros? Nestes documentos existem informações valiosas, como, por exemplo, seu endereço residencial, o seu CPF e identidade e, em alguns casos, seus telefones pessoais. Esses dados podem ser utilizados por pessoas mal intencionadas das mais variadas formas (falsificação de documentos, fraudes, assaltos, sequestros, entre outros). Lembra-se da Engenharia Social?

E-mails suspeitos ou fraudulentos, spams e com vírus. Como posso me proteger?

Quem nunca recebeu um e-mail com um suposto alerta do SERASA ou da Receita Federal, de atualização de cadastro de banco ou de uma promoção absurdamente imperdível, com um *link* "clique aqui"? Em sua grande maioria, são e-mails maliciosos, conhecidos como

Seus dados e informações pessoais deixados por aí podem ser usados para os mais diversos fins maliciosos, inclusive contra você!

Atenção aos e-mails recebidos! Analise a origem, a mensagem e, na dúvida, não clique em nenhum link. Mantenha seus programas antivírus sempre atualizados e faça uso dos filtros de spam da sua caixa de e-mail.

Phishing Scam

Forma de fraude eletrônica, caracterizada por tentativas de adquirir fotos, músicas e outros dados pessoais ao se fazer passar por uma pessoa confiável ou uma empresa enviando uma comunicação eletrônica oficial. Isso ocorre de várias maneiras, principalmente por email, mensagem instantânea e SMS.

phishing scams (veja ao lado), cujo objetivo é adquirir seus dados pessoais e financeiros. Usam as mais diversas técnicas como simular um *site* legítimo ou instalar um programa malicioso (vírus e cavalos-de-tróia, por exemplo) em seu computador.

Uso de Redes Sociais e Blogs. Devo me preocupar?

As redes sociais e *blogs* fazem parte de nosso cotidiano. Eles permitem que você se informe sobre os assuntos do momento, saiba o que seus amigos e ídolos estão fazendo, pensando e os lugares que estão frequentando. Entretanto, a grande popularidade das redes sociais também chama a atenção de pessoas mal-intencionadas.

Tenha cuidado com as informações publicadas. Dados e fotos sobre você, seus hábitos, de sua família, seus amigos, seus bens, informações do seu tra- balho e lugares frequentados podem ser usadas indevidamente, tanto para cau- sar danos à sua imagem e reputação, como para o uso criminoso em tentativas de sequestro e furto.

Se você tem filho(s) ou crianças próximas, tenha cuidado redobrado e os oriente para que se protejam dos riscos das redes sociais. Saiba que tipo de conteúdo acessam em sua navegação e, sobretudo, oriente para não se relacionarem com estranhos e nem forneçam informações pessoais na rede.

A SIC no ambiente de trabalho

Com a simples mudança de hábitos pessoais e funcionais, podemos contribuir para a implantação de uma nova cultura de SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES no TCM-PA.

Todos os dias pessoas, empresas e organizações governamentais são vítimas de tentativas de ataques, cujo objetivo é a captura ou destruição de dados ou informações importantes. Por isso, é preciso tomar cuidado e ficar atento para que as informações corporativas não sejam colocadas em risco.

Pense bem antes de divulgar algo nas suas redes sociais, pois tudo o que você publicar pode ser lido ou acessado por qualquer pessoa, e assim você não terá mais controle do que pode ser feito com aquela informação. Não é possível voltar atrás!

ORIENTE SEUS FILHOS

Existem inúmeras situações de insegurança que podem afetar as informações e os sistemas que as gerenciam, tais como: incêndios, alagamentos, problemas elétricos, fraudes, uso inadequado, engenharia social, guerras e seqüestros. Apesar de não serem totalmente gerenciáveis, podem ter seu impacto bastante reduzido com a tomada de ações preventivas.

Equipamentos de Informática

a) Mantenha atualizado o antivírus de sua estação de trabalho. A equipe técnica da Diretoria de Tecnologia da Informação do TCMPA irá se encarregar disso, mas, em caso de problema, entre em contato com o ***suporte@tcm.pa.gov.br*** para que a situação seja corrigida;

b) Evite trazer CD´S, DVD´S, *pen drives* ou quaisquer outros dispositivos móveis de fora do TCM para utiliozação no computador do trabalho. Você pode estar trazendo vírus de outros equipamentos para a sua estação e, consequentemente poderá infectar não só o seu equipamento, mas toda a rede interna do órgão; e

c) Suspeite de softwares e *link*s recebidos por e-mail em que você clica e não acontece nada.

Uso de Senhas

É importante termos certos cuidados na criação, no uso e na guarda de senhas pessoais. Você é o responsável legal por qualquer ação cometida com a sua senha.

Você protege suas senhas assim:

a) evite senhas simples, tipo: 12345, ABCDE, 8765, que podem ser rapidamente descobertas. Busque mesclar letras minúsculas, maiúsculas, números e caracteres especiais (*,&,¨%,$,#);

b) não utilize informações pessoais que podem ser facilmente descobertas, tais como: nome, sobrenome, número de CPF, telefone, placa de carro, identidade, data de nascimento e similares;

c) não utilize a mesma senha para diversas finalidades, por exemplo, para sistemas corporativos, conta bancária, correio eletrônico, etc.

d) altere suas senhas periodicamente; e

e) jamais repasse sua senha a terceiros, nem mesmo ao seu chefe ou à equipe da área de informática.

Utilização

O e-mail institucional foi criado e disponibilizado a você com o objetivo de ser usado para o propósito do seu trabalho. Assim, não utilize o e-mail institucional do TCM-PA para assuntos pessoais e não utilize e-mail pessoal para fins de trabalho.

Pessoas mal intencionadas utilizam-se de códigos maliciosos para obter informações sobre senhas, dados bancários, número do cartão de crédito e do CPF, além de poder colocar em risco informações sensíveis do seu trabalho.

Você é responsável pelas informações enviadas pela Internet! O e-mail institucional é um recurso importante e está sujeito a monitoramento e investigação.

Ao utilizar seu e-mail institucional:

a) não clique em *link*s e não abra anexos recebidos de remetentes desconhecidos;

b) não cadastre o e-mail institucional em listas de discussões não ligadas ao trabalho;

c) não envie e nem repasse mensagens com conteúdo impróprio, ofensivo e do tipo corrente;

d) não envie dados sigilosos do TCM-PA para seu e-mail particular.

Uso da Identidade Funcional (crachá)

A utilização da identidade funcional integra o conjunto de medidas de segurança adotado por este Ministério. Sua utilização é obrigatória não apenas para o ingresso em todas as unidades do TCM-PA, mas, também, para utilização enquanto exercemos nossas atividades durante a jornada de trabalho.

Isso facilita nossa identificação junto aos demais servidores, áreas de acesso e, inclusive, perante os cidadãos que demandam nossos serviços.

Informações restritas e sigilosas

Todos os servidores e colaboradores são responsáveis pelo sigilo das informações que recebem ou tratam no âmbito do TCM-PA e devem conhecer e obedecer às restrições de acesso e divulgação associadas.

E não se esqueça:

a) ao deixar sua estação de trabalho, guarde todo documento que possa conter informação que não deva ser de conhecimento alheio;

b) não deixe sua sala aberta, facilitando o acesso de pessoas alheias à unidade;e

c) ao se ausentar, lembre-se de desligar ou bloquear o computador. Já imaginou as implicações de alguém não autorizado utilizando a sua conta, acessando e divulgando indevidamente informações sob sua responsabilidade?

O uso do crachá é obrigatório nas dependências do TCM-PA. Trata-se de uso pessoal e em nenhuma hipótese deve ser emprestado ou usado por outro que não seja Você!

Lembre-se: não esqueça documentos em impressoras ou fotocopiadoras. Informações em papéis ou mídias devem ser manuseadas e descartadas de forma adequada.

4 ZELAR PELA SIC DO TCMPA

Conheça e pratique a Politica de Segurança da Informação e Comunicações do TCM-PA. Ajude a promover uma cultura de segurança da informação. Dissemine essa ideia!

Você sabia que também é seu dever zelar pela SIC do Tribunal de Contas dos Municípios -TCMPA?

É dever de todos nós zelar pela Segurança das informações e comunicações do TCM-PA. Toda e qualquer ação ou omissão, intencional ou acidental, que resulta no comprometimento da SIC pode resultar em responsabilização do servidor nas esferas penal, civil e administrativa.

O que posso fazer para melhorar a SIC?

Sua participação é fundamental e indispensável para o sucesso da segurança da informação e comunicações, tanto na vida pessoal quanto na profissional. Cultive um comportamento seguro, oriente as pessoas e colegas de seu convívio, reveja sempre as dicas dessa cartilha e busque conhecer os riscos aos quais você se expõe.

Em caso de suspeitas ou denúncias de quebra de segurança, ou ainda sugestões de melhoria, entre em contato pelo e-mail: ouvidoria@tcm.pa.gov.br

5 A QUEM POSSO RECORRER EM CASO DE DÚVIDAS, SUSPEITAS, DENÚNCIAS OU PROBLEMAS À SIC NO TCMPA

Um incidente isolado, que aparentemente apresenta pouco risco, pode representar parte de uma operação de maior abrangência e maior potencial de risco.

- **É importante informar todo e qualquer incidente identificado ao : suporte@tcm.pa.gov.br**
- **Em casos específicos de suspeita de e-mails maliciosos, encaminhe-os para: ouvidoria@tcm.pa.gov.br**

Você é parte crucial para o sucesso das ações de SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO no TCMPA!