2024

CARTILHA DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE

TRIBUNAL REGIONAL ELEITORAL DO PARÁ

2024
BELÉM/PA

CARTILHA DE

SEGURANÇA DA INFORMAÇÃO

Tribunal Regional Eleitoral do Pará

Dados Internacionais de Catalogação-na-Publicação (CIP)

B823c Brasil. Tribunal Regional Eleitoral do Pará

Cartilha de segurança da informação e privacidade. / Tribunal Regional Eleitoral do Pará. – Belém, PA: TRE-PA, 2024.

35 p. : il.

1. Justiça Eleitoral - Brasil. 2. Segurança da informação – privacidade. 3. Medidas de segurança – processamento de dados. 4. Sistemas de recuperação da informação – Medidas de segurança.

CDD (23.ed.) : 005.8

Luan Alex Silva
Bibliotecário
CRB-2/1730

TRIBUNAL REGIONAL ELEITORAL DO PARÁ

PRESIDENTE
Des. LEONAM GONDIM DA CRUZ JÚNIOR

VICE-PRESIDENTE E CORREGEDOR
Des. JOSÉ MARIA TEIXEIRA DO ROSÁRIO

DIRETORA GERAL
NATHALIE CHRISTINA DE OLIVEIRA CASTRO

SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO
FELIPE HOUAT DE BRITO

SECRETÁRIO DE GESTÃO DE PESSOAS
WALBER JOAQUIM DOS REMÉDIOS

SECRETÁRIA JUDICIÁRIO
FERNANDA MOREIRA SOUSA

SECRETÁRIA DE PLANEJAMENTO
HÉRIKA CARLA DA COSTA SODRÉ DE SOUZA

SECRETÁRIO DE ORÇAMENTO, FINANÇAS E CONTABILIDADE
RICARDO SERRUYA DE MEDEIROS

SECRETÁRIO DE ADMINISTRAÇÃO
JUDIRON RODRIGUES DE CARVALHO

SECRETÁRIA DE AUDITORIA
CLÁUDIA MYLENE PINHEIRO RIBEIRO

PRESIDENTE DA COMISSÃO DE SEGURANÇA DA INFORMAÇÃO
ANTONIO EDIVALDO DE OLIVEIRA GASPAR

SUMÁRIO

*Pescar informações ou clicks do usuário através de mensagens

SUMÁRIO

CARTA DO PRESIDENTE

DES. LEONAM GONDIM
DA CRUZ JÚNIOR

"É com satisfação que apresento esta Cartilha de Segurança da Informação e Privacidade, cumprindo um importante papel de cuidar da segurança da informação no Tribunal Regional Eleitoral do Pará.

As informações de uma instituição são dados valiosos e sensíveis, e, portanto, objeto de apurada atenção deste Regional para a preservação de sua confiabilidade e de sua integridade.

Em uma sociedade digital, integrada, ligada e dependente de diversas tecnologias de comunicação, cuidar da segurança da informação é proteger, não somente a instituição e o conteúdo de suas informações, mas também tudo o que a envolve, perpassando, necessariamente, pela transparência, por seus usuários e destinatários; pela proteção contra invasões ou ações maliciosas e pelo resguardo do sigilo e de dados sensíveis.

Assim, este documento visa instruir os usuários magistradas(os), servidoras(es), estagiárias(os) e colaboradoras(res) quanto aos conceitos básicos de segurança da informação e proteção de dados, objetivando a promoção de boas práticas de segurança cibernética no ambiente de trabalho do Tribunal."

CARTA DA DIRETORIA GERAL

NATHALIE CHRISTINA
DE OLIVEIRA CASTRO

"Tendo em vista a automatização cada vez maior dos processos administrativos deste Regional, é essencial que os dados sejam mantidos íntegros e disponíveis. Nesse escopo, a cartilha objetiva elevar o nível de conscientização em segurança da informação da(o) usuária(o), especialmente quanto ao modo de utilização dos diversos recursos dos sistemas que permeiam a Justiça Eleitoral.

É indubitável que a segurança da informação sustenta a confiança no processo eleitoral, dessa forma, é de suma importância a disseminação de boas práticas na área, buscando orientar os usuários desta Justiça Especializada para uma utilização segura dos recursos de tecnologia da informação disponibilizados pela instituição.

Desejo que esta cartilha seja um instrumento de conscientização da importância da Segurança da Informação, bem como auxilie magistradas(os), servidoras(es), estagiárias(os) e colaboradoras(res), na compreensão das ameaças do ambiente virtual, e também na utilização dos sistemas de forma consciente, além de manter a segurança de seus dados, computadores e dispositivos móveis."

APRESENTAÇÃO

SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO

FELIPE HOUAT DE BRITO

Senhoras Magistradas e Senhores Magistrados, Servidoras e Servidores, Colaboradoras e Colaboradores, Estagiárias e Estagiários,

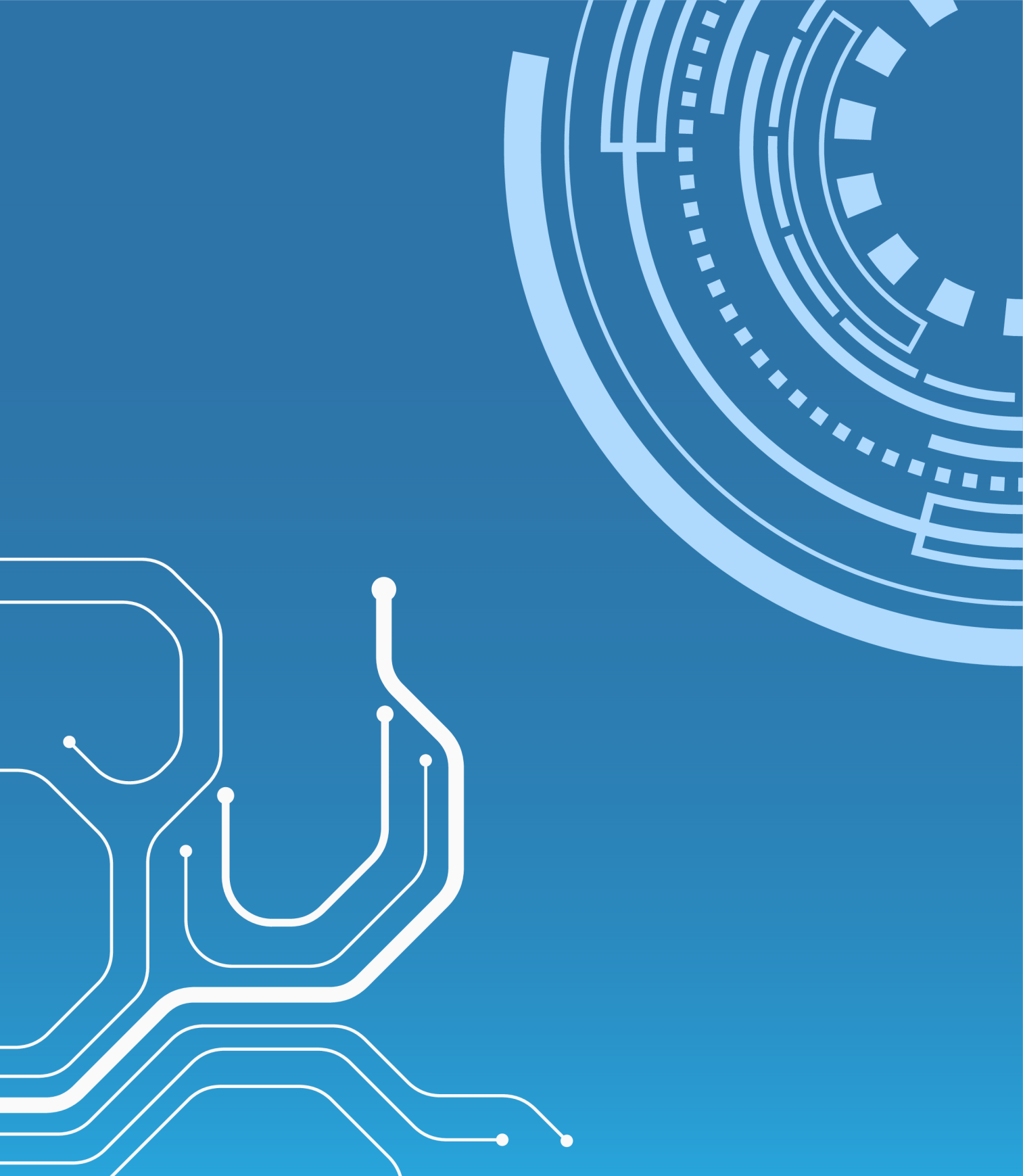
É com grande satisfação que fazemos o lançamento desta Cartilha de Segurança da Informação do Tribunal Regional Eleitoral do Pará. A Segurança da Informação e a privacidade são pilares fundamentais para a integridade e a confiabilidade dos processos eleitorais. Neste cenário dinâmico e desafiador, é imperativo que adotemos práticas robustas de proteção de dados para salvaguardar as informações confiadas a nós pelo público.

A Cartilha da Segurança da Informação e Privacidade do TRE do Pará é um passo decisivo nessa direção. Ela não apenas orienta, mas também reflete nosso compromisso contínuo com a excelência operacional e a transparência. Encorajo cada um de vocês a se familiarizar com seu conteúdo e a incorporar suas diretrizes em nosso trabalho diário.

Juntos, fortaleceremos ainda mais a segurança de nossos sistemas e a confiança do eleitorado na integridade do processo eleitoral.”

HISTÓRICO DE REVISÕES/ALTERAÇÕES

Número	Data	Versão	Responsável	Motivo
001	31/08/2023	1.0	CSI	Elaboração inicial do documento
002	20/03/2024	2.0	CGSI	Revisão, inserção de outros tópicos no conteúdo da Cartilha



I. TÓPICOS INTRODUTÓRIOS

O que é Segurança da Informação?

A Norma ABNT ISO/IEC 27001 define a Segurança da Informação como um conjunto de ações e medidas adotadas para proteger a integridade, confidencialidade e disponibilidade das informações, seja em formato digital ou físico, além de detectar, combater e prevenir possíveis ameaças a esses dados. A Segurança da Informação é responsabilidade de todos e envolve a implementação de controles e procedimentos institucionais objetivando assegurar que os dados sejam protegidos contra acessos não autorizados, modificações indevidas, divulgação não autorizada e indisponibilidade.

Sobre a Comissão de Segurança da Informação - CSI

O Art. 10 da Res. TSE 23.644/2021, trata da constituição, no âmbito dos Tribunais Eleitorais, da Comissão de Segurança da Informação (CSI). Subordinada à Presidência do Tribunal. A Comissão de Segurança da Informação (CSI) do TRE do Pará, inicialmente designada por meio da Portaria DG nº 10.621 de 01 de setembro de 2009, passou por sucessivas alterações, resultando na composição dada pela Portaria TRE-PA nº 22072/2023 para o biênio 2023/2024, por meio da qual foi estruturada através do Comitê multidisciplinar composto por 27(vinte e sete) membros representantes da Presidência, Corregedoria, Diretoria-Geral, de cada Secretaria, Assessoria de Comunicação Social, Gabinete da Polícia Judicial (GPJ) e Cartórios Eleitorais.

Dentre as atribuições descritas para a CSI no Art. 11 da Resolução 23.644/2021 do TSE, destaca-se a competência de “Promover a divulgação da PSI-JE e normativos, bem como ações para disseminar a cultura em segurança da informação, no âmbito do Regional”.

Princípios ou Pilares da Segurança da Informação

Além da integridade, confidencialidade e disponibilidade, algumas referências sobre o tema incluem outros princípios, ou pilares, da segurança da informação que formam um conjunto de diretrizes que fundamentam as práticas e políticas que orientam a proteção dos ativos de informação. Aqui estão os principais pilares, com suas respectivas definições:

a) Confidencialidade: garante que as informações só sejam acessadas por pessoas autorizadas. Visa evitar o acesso não autorizado ou divulgação de dados sensíveis.

- Exemplo: Criptografia de dados, controle de acesso.

b) Integridade: garante que as informações não sejam alteradas de maneira não autorizada. Visa proteger contra modificações não autorizadas nos dados.

- Exemplo: Assinaturas digitais, controle de versão.

c) Disponibilidade: garante que as informações e os recursos estejam disponíveis quando necessários. Visa evitar interrupções e garantir o acesso oportuno aos dados.

- Exemplo: Backup regular, redundância de links de comunicação e servidores.

d) Autenticidade: certifica a identidade das partes envolvidas em uma transação. Visa garantir que as informações sejam provenientes de fontes confiáveis.

- Exemplo: Sistemas de autenticação, biometria.

e) Não Repúdio (ou irretratabilidade): garante que uma parte não possa negar sua participação em uma transação. Visa estabelecer a responsabilidade pelas ações realizadas.

- Exemplo: Assinaturas digitais, registros de auditoria.

f) Segurança Física: protege os ativos de informação contra ameaças físicas, como roubo, incêndio ou desastres naturais.

- Exemplo: Controle de acesso físico, armazenamento seguro.

g) Resiliência: capacidade de se recuperar de incidentes de segurança e manter a operação normal.

- Exemplo: Planos de contingência, backups regulares.

O que é um ataque cibernético?

Um ataque cibernético refere-se a uma tentativa de explorar vulnerabilidades em sistemas de computadores, redes, dispositivos ou serviços online com o objetivo de comprometer, roubar, destruir ou manipular informações, além de interromper operações normais. Os ataques cibernéticos podem assumir diversas formas, incluindo malware, phishing, ataques de negação de serviço (DDoS), invasões de sistemas, entre outros. Os atacantes, muitas vezes referidos como cibercriminosos ou hackers, buscam explorar fraquezas de segurança para ganho financeiro, roubo de informações pessoais, espionagem industrial, sabotagem, ou mesmo para simplesmente causar danos.

A constante evolução das tecnologias digitais também implica uma adaptação contínua das estratégias de segurança para mitigar os riscos associados a esses ataques. Além disso, destaca-se a importância de conscientizar tanto indivíduos quanto organizações sobre práticas seguras online, o reconhecimento de ameaças e a necessidade de colaboração para a proteção contra ataques cibernéticos.

Tratamento de Dados Pessoais

É toda operação realizada com Dados Pessoais e compreende a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; nos termos da LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD) inciso X do Artigo 5º.

LGPD e o Servidor

O art. 47 da LGPD define que o agente de tratamento de dados ou qualquer pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação em relação aos Dados Pessoais.

Classificação das informações

As informações que são produzidas e custodiadas pelo TRE do Pará são de grande importância não somente para os magistrados, servidores e colaboradores, mas também para toda a sociedade. Por este motivo, é fundamental que a informação receba o devido tratamento. Deste modo, a classificação da informação é como um guia valioso, categorizando dados com base em sua sensibilidade. Imagine um espectro que vai de informações públicas, compartilháveis abertamente, até dados altamente confidenciais e estratégicos, exigindo controle rigoroso. Essa prática não só ajuda a adaptar medidas de segurança proporcionais ao valor dos dados, mas também orienta como eles são compartilhados, armazenados e protegidos, seja localmente ou em nuvem. O correto entendimento e aplicação da classificação da informação, é essencial para aumentar a proteção de nossos dados, garantindo que cada pedaço de informação seja tratado com a proteção que merece.

O que é a Política de Segurança da Informação da Justiça Eleitoral (PSI-JE)

A política de segurança da informação é um conjunto de regras, diretrizes e procedimentos que visam proteger os ativos de informação de um órgão público ou empresa. Essa política deve incluir ações preventivas e corretivas para garantir a confidencialidade, integridade e disponibilidade dos dados.

O Tribunal Superior Eleitoral (TSE) instituiu, por meio da Resolução nº 23.644/2021, as diretrizes para a implementação da Política de Segurança da Informação (PSI) da Justiça Eleitoral. Esta norma tem o objetivo adequar o uso dos recursos de Tecnologia da Informação e Comunicação, assegurando a continuidade da prestação jurisdicional e dos serviços eleitorais à sociedade, com foco na proteção da segurança da informação e na mitigação de riscos cibernéticos.

Os principais objetivos da PSI são, entre outros: instituir diretrizes estratégicas, responsabilidades e competências, buscando a estruturação da segurança da informação; promover ações que evitem incidentes, de modo a preservar os dados e a imagem da instituição; e nortear os trabalhos de conscientização e de capacitação de pessoal em segurança da informação e em proteção de dados pessoais.

As diretrizes desta Resolução devem ser aplicadas a magistrados, membros do Ministério Público, servidores efetivos e requisitados, ocupantes de cargos em comissão sem vínculo efetivo, estagiários, prestadores de serviço, colaboradores e usuários externos que utilizem ou tenham acesso a ativos de informação e processamento no âmbito da Justiça Eleitoral.

Todos somos co-responsáveis pela Segurança da Informação do Tribunal

No TRE do Pará, reconhecemos que o sucesso e eficácia das medidas de segurança da informação e a salvaguarda dos Dados Pessoais dependerão da conscientização e comprometimento de todos que estejam a serviço da Justiça Eleitoral. Portanto, a Segurança da Informação é uma responsabilidade compartilhada por todos, uma vez que cada um desempenha um papel vital na preservação da confidencialidade, integridade e disponibilidade das informações. Seja no uso de sistemas informatizados, manuseio de documentos e dados ou na comunicação cotidiana, todos contribuímos para a evolução da maturidade em segurança da informação.

A co-responsabilidade implica em adotar práticas seguras, reportar potenciais ameaças e estar atento às diretrizes estabelecidas para proteção de dados. Ao fomentar e fortalecer essa cultura de segurança, garantimos não apenas a conformidade com recomendações dos órgãos de controle, normas e regulamentos, mas também a confiança da Sociedade em relação à garantia da legitimidade do processo eleitoral.

II. QUAIS OS PRINCIPAIS RISCOS EXTERNOS ?

Phishing*

Phishing de email é uma técnica de fraude em que criminosos enviam mensagens falsas, disfarçadas de legítimas, para enganar usuários e obter informações sensíveis, como senhas e dados financeiros.

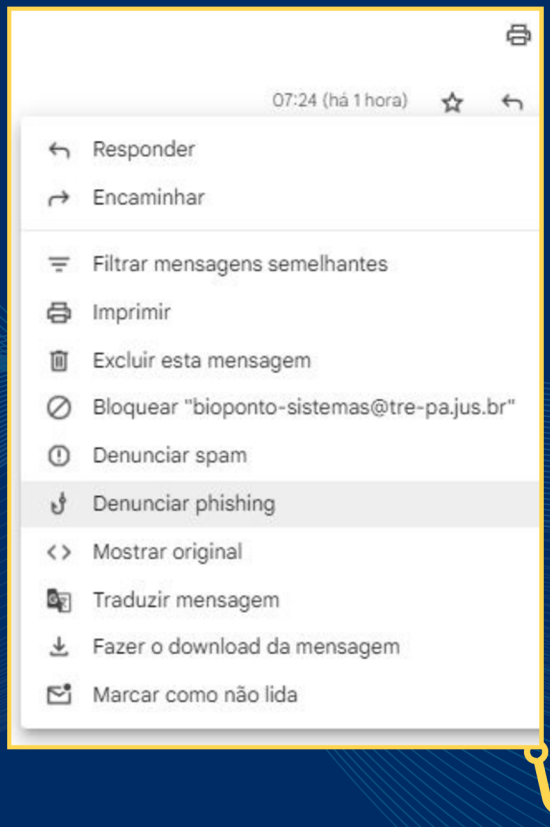
A ameaça de phishing é real e está sempre à espreita. Por isso, precisamos ser diligentes e adotar uma postura defensiva para proteger nossos dados. Mantenha-se alerta ao receber e-mails estranhos e inesperados, desconfie sempre de mensagens que tentam induzir o destinatário a agir rapidamente, criando um senso de urgência. Verifique cuidadosamente os remetentes. Nunca clique em links suspeitos, mesmo que pareçam ser de amigos ou empresas conhecidas. Sua vigilância é a melhor defesa contra tentativas de phishing. Juntos, podemos construir uma barreira robusta contra ameaças online.

*PESCAR INFORMAÇÕES OU CLICKS DO USUÁRIO ATRAVÉS DE MENSAGENS

IMPORTANTE:

Para denunciar e-mails de phishing no Gmail, siga os passos abaixo.

Abra o e-mail suspeito: **Não clique em nenhum link ou anexo no e-mail.** Clique nos três pontos verticais: Esses pontos estão no canto superior direito da mensagem, próximo ao ícone de resposta.



Selecione "Denunciar phishing": No menu suspenso, clique em "Denunciar phishing". Isso abrirá uma janela de confirmação.

Confirme a denúncia: Clique em "Denunciar mensagem" para enviar o e-mail ao Google para análise. Isso ajuda a proteger outras pessoas de possíveis ataques.

Denunciar e-mails de phishing ajuda a manter a segurança da sua conta e contribui para a segurança da comunidade de usuários do Gmail.

Smishing

Smishing é um ataque de phishing feito por SMS (mensagem de texto). Similar ao Phishing, a tática se resume a pedir, com urgência, que a vítima realize alguma ação para evitar uma suposta consequência negativa. Passando-se por instituições bancárias ou até mesmo por conhecidos, os fraudadores se aproveitam da distração das pessoas ao celular e as induzem a clicar em links maliciosos ou fornecer credenciais. Por isso, desconfie de pedidos urgentes de números desconhecidos. Nunca responda a essas mensagens nem clique em links suspeitos enviados por SMS.

Engenharia social

Engenharia social é a habilidade de conseguir acesso a informações confidenciais pessoais ou acesso físico a áreas importantes de uma instituição, mediante técnicas de persuasão. A engenharia social também é usada para obter acesso a sistemas ou realizar atividades fraudulentas. Em vez de utilizar equipamentos sofisticados ou métodos tecnológicos avançados para realizar essa atividade, o atacante explora a interação humana, manipulando a confiança e ingenuidade das vítimas. Os ataques podem incluir (ou mesclar) táticas como phishing, falsificação de identidade e criação de pretextos elaborados para induzir as pessoas a compartilhar informações sensíveis. A busca de informações pode ocorrer nos locais mais diversos, como redes sociais, mesas de trabalho e lixeiras, e pela atenção às conversas alheias em locais sociais. A conscientização, a atenção e a educação sobre ameaças digitais são essenciais para se proteger contra ataques desse tipo.

Malware

O malware é a designação atribuída a qualquer "software malicioso", que representa uma ameaça persistente no cenário cibernético, assumindo diversas formas, desde vírus de computador a ransomware. Essas ameaças podem resultar em perda de dados sensíveis, danificar sistemas e redes, permitir acesso não autorizado e até mesmo extorsão financeira. Para se defender contra a ameaça dos malwares, o TRE do Pará adotará medidas e práticas essenciais à segurança, incluindo a instalação e manutenção de sistemas antivírus atualizados, a implementação de firewalls, o monitoramento de rede e a análise comportamental para identificar atividades suspeitas. Caso você suspeite que o antivírus de seu computador não foi instalado, ou não está funcionando corretamente, informe imediatamente a Secretaria de Tecnologia da Informação.

Ransomware

Atualmente, o ransomware é um dos principais objetivos dos ataques cibernéticos. Neste tipo de ataque, o criminoso utiliza métodos avançados para obter acesso a sistemas de instituições, incluindo servidores de aplicação e de arquivos, criptografando todos os dados armazenados. Isso resulta na indisponibilidade das máquinas e dos dados da organização, que só pode ser restaurada mediante o pagamento de um resgate exigido pelo atacante. No entanto, o prejuízo causado por esse tipo de ataque é quase incalculável e pode paralisar a instituição por dias, semanas ou até meses. Além disso, o pagamento do resgate não garante a recuperação dos dados nem impede futuros ataques.

Se você perder o controle de sua máquina de trabalho, informe imediatamente à STI.

III. A IMPORTÂNCIA DA SEGURANÇA DE SENHAS

Crie senhas robustas e não compartilhe com terceiros

Você sabia que quanto mais complexas suas senhas mais difícil será a tarefa de um Hacker de quebrá-las? Por isso, não facilite a vida dos atacantes, fortaleça suas senhas, pois essa é uma barreira inicial essencial para a sua proteção. Use senhas longas (no mínimo 10 caracteres) e complexas, com uma combinação de letras maiúsculas e minúsculas, números e caracteres especiais. Evite informações pessoais fáceis de adivinhar, como datas de nascimento.

Também é importante usar senhas diferentes em diferentes sites. Lembre-se, reutilizar senhas é uma prática que precisamos evitar, pois aumenta o risco caso um dos sites que você possui cadastro seja comprometido. Use senhas únicas, exclusivas para cada conta.

Nunca compartilhe suas credenciais de acesso ao computador ou aos sistemas com terceiros, mesmo que seja um colega de trabalho, pois cada login é como uma chave única de acesso à rede de uso pessoal e intransferível.

Que a força da senha esteja com você

Em nosso ambiente digital, a segurança das senhas é uma linha de defesa considerada fundamental. Elaborar senhas fortes é uma habilidade essencial que precisamos desenvolver para proteger nossos dados contra ameaças online. Não subestime o poder de uma senha robusta na preservação da integridade e confidencialidade das suas informações.

Além disso, lembre-se de redefinir suas senhas regularmente. Para manter as informações do Tribunal seguras, a Secretaria de Tecnologia da Informação poderá aplicar políticas para trocas de senhas em períodos pré-definidos, ou imediatamente em casos de ataques cibernéticos.

Alguns sites além de testar a força de sua senha demonstram em quanto tempo elas podem ser quebradas.

Experimente testar sua habilidade de compor senhas nos sites a seguir:

https://testedesenha.com.br/
https://bitwarden.com/password-strength/

#SenhasFortes

Fortaleça sua defesa online!

No mundo digital, além de uma senha forte, você precisará de um código temporário ou um dispositivo adicional para acessar sua conta, essa é a função da autenticação de dois fatores (2FA). A autenticação de dois fatores é uma camada adicional de segurança que protege as contas institucionais do Tribunal.

Ative o 2FA hoje e faça da autenticação de dois fatores a sua barreira extra contra ameaças cibernéticas. A proteção e a privacidade de dados importantes estão nas suas mãos.

#DuplaDefesaDigital

Diga Não às Práticas Inseguras com Senhas!

Comportamentos inseguros podem abrir portas para invasões. Logo, evitar práticas inseguras com senhas é fundamental. Sempre encerre a sessão usando sair/desconectar/logout. Salvar senhas no navegador é uma prática não recomendada, pois esse será o primeiro alvo de um atacante, caso tenha acesso ao seu computador.
Use gerenciadores de senha e nunca (nunca mesmo!) deixe-as visíveis em Post-it. Sua privacidade agradece!

Juntos, podemos construir uma barreira sólida contra ameaças cibernéticas.

Gerenciadores de senhas - Mantenha suas contas seguras

Os gerenciadores de senha desempenham um papel fundamental na promoção da segurança online. Com a quantidade crescente de contas e senhas que precisamos lembrar, é fácil cair na armadilha de usar senhas simples ou reutilizá-las. Os gerenciadores de senha oferecem uma solução eficaz, permitindo que os usuários criem senhas complexas e únicas para cada conta, armazenadas com segurança em um cofre digital. Além disso, eles simplificam o processo de login, automatizando o preenchimento de campos de senha.
Ao optar por um gerenciador de senha confiável, os usuários fortalecem sua postura de segurança, reduzindo significativamente o risco de violações de dados e facilitando a adoção de práticas sólidas de autenticação.
Consulte a STI, caso tenha dúvidas sobre quais gerenciadores de senhas você pode usar para proteger suas senhas.

Segurança da informação no trabalho e na vida pessoal

No que diz respeito à segurança da informação, é fundamental o cumprimento das políticas e diretrizes estabelecidas pelo Tribunal. Ademais, recomenda-se a adoção de boas práticas de segurança em âmbito pessoal, como a criação de senhas fortes e a implementação de medidas de proteção contra fraudes e acessos não autorizados a contas e dispositivos.

IV. GARANTINDO A SEGURANÇA EM REDES SOCIAIS

Reforce suas defesas

Em um mundo cada vez mais conectado, a segurança das nossas redes sociais é a chave para um ambiente virtual confiável. Por isso, apesar de todos os benefícios que as redes sociais oferecem, elas também apresentam uma ampla gama de problemas de segurança e preocupações. Vamos juntos fortalecer nossas defesas digitais: Use senhas fortes e exclusivas para suas contas em redes sociais, e habilite a proteção de 2FA. Revise com frequência as atividades de login e notificações de segurança para garantir que não haja atividades suspeitas em sua conta. Revise e remova aplicativos de terceiros conectados à sua conta que você não usa mais ou não reconhece.

Cuidado com Perfis falsos

Os criminosos podem criar perfis falsos se fazendo passar por alguém que você conhece na esperança de que você se conectará a eles. Se forem bem-sucedidos, eles terão acesso a tudo o que você publicar e enviarão solicitações de amizade aos seus contatos com a intenção de roubar informações pessoais ou pedir dinheiro.

Compartilhe com os outros apenas o que for realmente necessário

As redes sociais são frequentemente usadas por golpistas para procurar seus alvos e reunir informações de perfis públicos. Regularmente revise e ajuste as configurações de privacidade para controlar quem pode ver suas informações, postagens e amigos. Evite compartilhar informações sensíveis, não exponha nas Redes Sociais dados como endereço, telefone, CPF, detalhes financeiros, etc.

Seja cuidadoso ao fornecer a sua localização e cuidado ao divulgar fotos e vídeos que permitam deduzir a sua localização. Não divulgue planos de viagens e nem por quanto tempo ficará fora da sua residência. Essas práticas impedem que informações sensíveis sejam facilmente acessadas por terceiros não autorizados.

Quanto mais informações conseguirem encontrar, mais convincentes eles parecerão para uma possível vítima.

Segurança no aplicativo de mensagem instantânea

Embora amplamente utilizados para troca de mensagens, os aplicativos de mensageria como WhatsApp ou Telegram podem apresentar riscos significativos de segurança da informação. As principais ameaças incluem ataques de phishing e golpes que visam obter informações pessoais ou financeiras.

A falsificação de identidade, a clonagem do aplicativo e a propagação de software maliciosos (malware), também constituem riscos à privacidade, contribuindo para um cenário desafiador. Por esse motivo, a conscientização sobre práticas seguras, como verificação cuidadosa de mensagens suspeitas, é fundamental para mitigar esses riscos. Regularmente, verifique e atualize suas configurações de privacidade, limitando quem pode ver suas informações pessoais (como foto do perfil) e status. Importante também é a ativação de bloqueio por impressão digital. Evite interações com mensagens suspeitas ou de desconhecidos, reduzindo o risco de phishing e golpes. Mantenha o aplicativo e o sistema operacional atualizados para corrigir vulnerabilidades conhecidas.

Fique atento às seguintes dicas ao utilizar serviços de mensagem instantânea:

- Caso haja necessidade de aceitar algum tipo de arquivo, tenha um antivírus atualizado em sua máquina e tenha certeza da identidade da pessoa que está enviando. Nunca aceite arquivos de pessoas desconhecidas, principalmente se tiverem a extensão “exe”, "xlsx" e “doc” (ou extensões desconhecidas), pois podem conter malware;

- Desconfie de contatos de desconhecidos que alegam ser representantes de instituição financeira, suporte de computadores etc. e que solicitam dados pessoais e/ou sigilosos.

Para comunicação institucional com servidores e colaboradores do Tribunal, dê preferência ao aplicativo Google Chat, disponível no aplicativo de E-mail ou através da URL https://mail.google.com/chat/.

Como ocorre a clonagem do WhatsApp?

A clonagem do WhatsApp envolve o acesso ao aplicativo da vítima em outro dispositivo. Os golpistas requerem um código de seis dígitos enviado por SMS para o telefone da vítima. Este código é gerado pelo WhatsApp em situações como a troca de número ou de aparelho, quando se deseja transferir todas as conversas para um novo dispositivo ou número.

Para obter este código, os golpistas utilizam técnicas de engenharia social. Eles ligam para a vítima, se fazendo passar por representantes de empresas ou serviços conhecidos, e solicitam o código, geralmente alegando alguma necessidade urgente. Devido à persuasão habilidosa dos golpistas, a vítima é levada a acreditar estar lidando com uma entidade legítima e acaba fornecendo o código solicitado. Para evitar a clonagem do aplicativo, além de nunca enviar para outra pessoa o código de verificação (mensagens SMS) do Whatsapp, que possibilita a transferência do aplicativo para outro smartphone, é de suma importância habilitar a “confirmação em duas etapas” do WhatsApp.

“Importante lembrar: o WhatsApp nunca pede códigos por ligação. Se alguém solicitar um código recebido por SMS, desconfie e leia o SMS com atenção.

Proteja suas senhas e evite compartilhá-las.”

Proteja seu WhatsApp: Dicas Essenciais

- Ative a Confirmação em Duas Etapas: Reforce a segurança da sua conta ativando a confirmação em duas etapas. Com essa camada extra de proteção, mesmo que alguém obtenha seu código de verificação, ainda precisará de uma senha adicional para acessar sua conta.

- Cadastre sua Digital ou Rosto: Aproveite as tecnologias biométricas do seu dispositivo para proteger ainda mais seu aplicativo. Cadastre sua impressão digital ou reconhecimento facial para garantir que apenas você tenha acesso ao seu WhatsApp.

- Use Verificação Biométrica no WhatsApp Web: Mantenha seus dados seguros mesmo quando estiver usando o WhatsApp Web. Ative a verificação biométrica para garantir que somente você possa acessar suas conversas e informações, mesmo em dispositivos conectados.

- Confira Dispositivos Conectados: Crie o hábito de verificar regularmente os dispositivos conectados à sua conta. Revise a lista de aparelhos autorizados e remova qualquer um que não reconheça para evitar acessos não autorizados.

- Mantenha Tudo Atualizado: Mantenha seu aplicativo e seu sistema operacional sempre atualizados. As atualizações frequentes geralmente incluem correções de segurança importantes que ajudam a proteger sua privacidade e dados contra ameaças.

> “Com essas medidas simples, você pode fortalecer significativamente a segurança do seu WhatsApp e desfrutar de uma experiência mais tranquila e protegida.”

V. INSTRUÇÕES FINAIS

Navegando na Internet com Segurança

Muitos sites da internet representam riscos e visam infectar sistemas operacionais de computadores pessoais e smartphones. Portanto, é importante evitar páginas com conteúdo inadequado (adulto, racista, intolerante, violento ou relacionado a manifestações contrárias aos direitos humanos) e softwares sem licença, pois tais práticas são proibidas pelas políticas de segurança da Justiça Eleitoral. As orientações a seguir podem ajudar a manter uma navegação segura na Internet:

- Verifique se o endereço que está aparecendo em seu navegador é realmente o que você deseja acessar;
- Não confie em tudo o que vê ou lê;
- O navegador não garante sozinho a segurança de informações pessoais, senhas e dados bancários;
- Nunca autorize a instalação de softwares de desconhecidos ou popups que redirecionam para sites estranhos;
- Antes de clicar em um link, veja na barra de status do navegador se o endereço de destino do link está de acordo com a descrição do mesmo;
- Sempre desconfie de ofertas e sorteios dos quais não tenha conhecimento prévio.

Proteja o acesso à Internet de seus filhos.

Precisamos construir juntos um ambiente digital seguro para nossos filhos, moldando uma experiência online positiva para o futuro deles. A educação digital é a chave para capacitá-los a navegar nas redes sociais com sabedoria. Ensine-os sobre a importância da privacidade, o impacto das postagens online e como adotar comportamentos online seguros.

Oriente para nunca fornecerem informações sensíveis, como imagens ou vídeos pessoais. Informe sobre os riscos de uso da Webcam e que ela não deve ser usada para se comunicar com desconhecidos. Não esquecer de conversar com seus filhos sobre o que eles fazem na Internet e nas redes sociais, bem como estabelecer limites de tempo e conteúdo.

Existem aplicativos gratuitos como o Family Link, que ajuda os responsáveis a gerenciar as contas do Google dos seus filhos. Com ele é possível criar uma conta do Google para o seu filho, aprovar ou bloquear aplicativos e jogos, ajustar o tempo de tela, proteger a privacidade da criança, dentre outras funcionalidades.

O Family Link está disponível para dispositivos Android e iOS.

Para saber mais sobre o Family Link, acesse:
https://families.google/intl/pt-BR/familylink/

Atualizações Constantes do Sistema Operacional

Proteger-se contra ameaças cibernéticas exige uma postura proativa. Por isso, seja no trabalho ou em casa, não subestime a importância das atualizações de segurança que abrangem tanto os Sistemas Operacionais quanto os aplicativos. Automatizar esse processo é uma estratégia eficaz, assegurando que nenhuma atualização crítica passe despercebida.

Deste modo, a equipe técnica da STI poderá, sempre que for necessário, disparar atualizações automáticas dos sistemas operacionais e aplicativos, objetivando mitigar vulnerabilidades dos Sistemas Operacionais, fortalecendo a segurança digital para manter o parque computacional constantemente atualizado e resiliente contra ameaças cibernéticas.

Dica: sempre que aparecer o ícone de atualizações na área de verificação do Windows (próximo de data e hora), o computador precisará ser reiniciado para instalar as versões mais recentes de software.

Utilização de Dispositivos de Armazenamento Removíveis

Se precisar utilizar um pendrive para transferir arquivos, certifique-se de protegê-lo, garantindo que seu computador possua um antivírus instalado e atualizado. Isso é essencial porque alguns vírus podem ser ativados automaticamente, comprometendo seu computador pessoal através da conexão USB. O antivírus do Tribunal está configurado para realizar verificações automáticas nos dispositivos, mantendo os computadores protegidos contra possíveis ameaças originadas de pendrives.

Mesa limpa e ambiente protegido

Mantenha o ambiente de trabalho seguro começando pela sua mesa.
Ao se ausentar de sua mesa, garanta que:

- Documentos com informação restrita, ou que considere importantes estão protegidos, preferencialmente em armários com chaves;
- Que seu computador esteja bloqueado;
- Que dispositivos móveis como notebooks, pendrives, tablets e smartphones estejam seguros e protegidos e não fiquem expostos na mesa;
- Se imprimir algo, use a funcionalidade de senha para que a impressão seja liberada somente quando digitar a senha na impressora. Caso perceba que existem documentos com informações restritas ou sensíveis que não pertencem a você na impressora, entre em contato com a equipe de TI.

Como relatar incidentes de segurança

Em uma cartilha de segurança da informação e privacidade não poderíamos deixar de mencionar sobre a necessidade de comunicar os incidentes de segurança. Mesmo com a adoção de medidas preventivas, é importante reconhecer a possibilidade de ocorrência de tais incidentes. Logo, ao identificar uma violação, o primeiro passo é relatar imediatamente à equipe de segurança cibernética da Secretaria de Tecnologia da Informação. Você pode fazer isso via Service Desk – TRE-PA/STI, fornecendo, no mínimo, as seguintes informações:

Relatório de Incidente:

- Data e hora
- Nome da pessoa que está relatando
- Unidade
- Qual é o problema ? (descrição do incidente)
- Qual é o efeito do incidente ?
- Como foi descoberto ?
- Os dados que foram afetados
- Tipo de ativo (desktop, impressora, sistema, etc)
- Nome do Sistema / endereço URL do Sistema
- Quem mais foi informado

Para reportar incidentes de segurança da informação, utilize os canais do Service Desk (servicedesk@tre-pa.jus.br) ou outros meios divulgados na página da Intranet do Tribunal.

Nestes casos, a equipe de segurança irá avaliar o incidente, e tomar as medidas necessárias para limitar danos e investigar a causa raiz, implementando ações de resposta adequadas a cada incidente. Lembre-se, não se trata apenas da responsabilidade da equipe de TI; como destacamos, todos desempenham um papel fundamental na proteção dos dados, reportando comportamentos suspeitos e adotando práticas seguras em relação à credenciais/senhas, computadores e sistemas do Tribunal. Em síntese, a consciência, a rápida resposta e a colaboração de todos são essenciais para minimizar danos e proteger as informações da Justiça Eleitoral.

Projeto gráfico e Editoração

1ª Edição 2024

Capa em triplex e laminação brilho 300g/m^2

Miolo couché brilho 120g/m^2


TRIBUNAL
REGIONAL
ELEITORAL
DO PARÁ