PREVENÇÃO DE INCIDENTES DE VAZAMENTO DOS SEUS DADOS PESSOAIS

Use canais de comunicação oficiais para assuntos de trabalho

O TCE/SC instituiu através da Portaria N. TC-091/2020, o Office e seus aplicativos como ferramenta oficial de veículo de comunicação interna, e-mail e armazenamento em nuvem:

- Não use contas pessoais de e-mails e aplicativos de mensagens para tratar de assuntos corporativos.

E-mail (Portaria N.TC-316/2020)

Utilize o e-mail corporativo somente para assuntos institucionais.
Recebeu algum e-mail suspeito? Clicou no link de um e-mail e depois descobriu que era phishing? O computador está “estranho”? Notou um acesso indevido à sua conta?

Comunique à DTI para que as ações de segurança sejam iniciadas imediatamente. O quanto antes um incidente for detectado e contido, menores serão os transtornos e prejuízos. (art. 11)

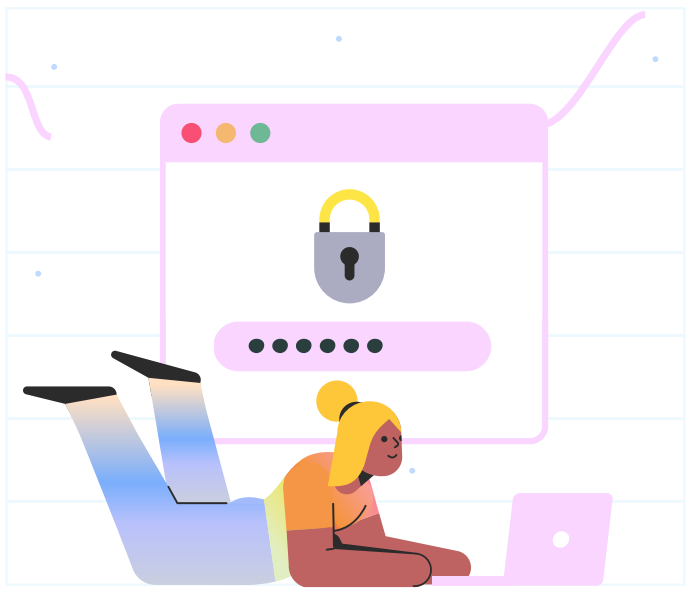
TRIBUNAL DE CONTAS DE SANTA CATARINA
Encarregado de Dados - AGET

Ferramenta de comunicação interna

Utilize o Teams como ferramenta oficial de comunicação interna entre usuários, esse aplicativo criptografa suas mensagens de ponta a ponta.

Senhas (Portaria N.TC-316/2020)

Não disponibilizar senhas e tokens a terceiros é uma prática fundamental de segurança para proteger suas informações pessoais, financeiras e corporativas.
Senhas e tokens são credenciais que garantem acesso a sistemas, dados e serviços, e compartilhar essas informações pode comprometer a integridade e a segurança dos seus dados. (art. 10)



- Não deixe expostas suas senhas;
- Renove as suas senhas a cada 90 (noventa) dias;
- Utilize senha de no mínimo, 8 (oito) dígitos, composta de letras maiúsculas e minúsculas, números e caracteres especiais;
- Certifique-se de que não está sendo observado enquanto utiliza suas senhas;
- Não forneceça sua senha a terceiros;
- Não utilize sua senha em computadores de terceiros;
- Não utilize suas senhas corporativas do TCE/SC em sistemas não corporativos e/ou de uso pessoal.

Reduza a coleta de dados por sites

Reduzir a coleta de dados por sites previne incidentes de dados pessoais ao limitar a quantidade de informações que os sites podem coletar:

- Preencha somente os dados necessários;
- Configure o navegador para bloquear cookies de terceiros e apenas aceitar aqueles essenciais para o funcionamento de sites confiáveis.

Utilize equipamentos fornecidos pela Instituição

O uso de equipamentos institucionais no TCE/SC é crucial para garantir a segurança da informação, permitindo controle sobre dados sensíveis, monitoramento de atividades, conformidade com normas de segurança, proteção contra ameaças cibernéticas e uso responsável dos recursos públicos:

- O TCE/SC lida com dados sensíveis de contas públicas, auditorias e fiscalizações. O uso de equipamentos da instituição garante que esses dispositivos tenham as configurações adequadas de proteção, como criptografia, antivírus e políticas de acesso, reduzindo o risco de vazamentos de informações.
- Permite que a equipe de TI do TCE/SC tenha maior controle sobre o monitoramento de atividades e possíveis incidentes de segurança, possibilitando uma resposta rápida a ameaças, invasões ou comportamentos suspeitos.
- Assegura que os servidores públicos utilizem os recursos de forma responsável e dentro dos limites de suas atribuições, evitando o uso indevido de informações sensíveis em dispositivos pessoais, o que poderia expor o TCE/SC a vulnerabilidades legais e de segurança.

Autenticação de múltiplos fatores

A autenticação de múltiplos fatores (MFA) é essencial para a proteção de dados, pois adiciona uma camada extra de proteção além da senha, tornando muito mais difícil para atacantes acessarem informações confidenciais, mesmo que a senha seja comprometida.

Ao exigir um segundo fator, como um código gerado por um aplicativo ou enviado por SMS, o sistema garante que apenas o usuário autorizado, com acesso a esse fator adicional, possa efetuar o login, reduzindo significativamente o risco de violações de segurança e proteção contra ataques cibernéticos, como phishing e roubo de credenciais.

Adote a política da mesa limpa (Portaria N. TC-0140/2023)

Papéis e mídias de armazenamento eletrônicas, contendo informações de responsabilidade do TCE/SC, não devem permanecer sobre a mesa desnecessariamente. (art. 85)

Adotar bloqueio de tela como prática ao afastar-se de sua máquina

Os computadores (desktop, notebooks e terminais), quando não estiverem sendo utilizados, deverão ser desligados ou protegidos com mecanismo de tela e teclados controlados por senha, token ou mecanismo de autenticação similar, quando sem monitoração, e protegidos por tecla de bloqueio, senha ou outros controles. (art. 86)

Compartilhamento de dados pessoais e sensíveis

Viola a Lei Geral de Proteção de Dados aquele servidor/colaborador que exporta, copia, documentos que possuam dados pessoais e/ou dados pessoais sensíveis, de colegas, e os repassa ou encaminha a terceirios sem autorização, previsão legal, ou necessidade justificável.

Divulgação de documentos em elaboração

Divulgar, compartilhar um documento em elaboração, antes de sua publicação, como um relatório de auditoria preliminar, um voto de um conselheiro, ou um edital de licitação em fase de minuta; havendo quebra de protoloco de sigilo, pode o servidor/colaborador ser resposabilizado por seus atos de forma administrativa, civil e/ou penal.