Câmara Municipal de
Vargem Grande do Sul

CARTILHA DE BOAS PRÁTICAS E RECOMENDAÇÕES

PROTEÇÃO DE DADOS E SEGURANÇA CIBERNÉTICA

1 – Identificação do Propósito do Tratamento e Minimização dos Dados na Coleta

A identificação da finalidade do tratamento de dados pessoais serve, fundamentalmente, para que as operações do ciclo devida do dado sejam realizadas em conformidade com as regras estabelecidas pela Lei Geral de Proteção de Dados Pessoais (LGPD).

Dessa maneira, o colaborador deve identificar o propósito de cada tratamento que pretenda realizar antes mesmo do Início desse tratamento, verificando qual a base legal adequada para o desenvolvimento dessa finalidade e se os dados a serem coletados são os estritamente necessários para o cumprimento desse propósito.

Na proteção de dados e da privacidade, menos é mais, pois, conforme o princípio da necessidade, a coleta de dados deve sedar de maneira restritiva, sempre limitada, portanto, ao propósito previamente estabelecido.

2 - Transparência e Lealdade no Tratamento de Dados Pessoais

O tratamento de dados pessoais deve ser realizado pelo colaborador sempre de forma lícita, transparente e garantindo a lealdade desse processamento para com os clientes cujos dados pessoais estão sendo tratados. Dessa forma, na medida em que se assegura a privacidade dos dados pessoais, se exige mais transparência quanto às atividades do tratamento, que deve ser sempre realizado em consonância com o ordenamento jurídico e em conformidade com a finalidade inicialmente comunicada aos clientes.

O colaborador não pode utilizar os dados pessoais para outras finalidades que não sejam compatíveis com o propósito original apresentado antes da coleta dos dados, devendo, igualmente, garantir aos clientes que seus dados pessoais sejam conservados apenas durante o tempo necessário às finalidades para as quais foram recolhidos.

Por fim, os dados pessoais não podem ser coletados senão para finalidades específicas, sendo vedada a coleta para fins indefinidos.

3- Promoções dos Direitos e Garantias dos Titulares de Dados.

O colaborador deve sempre realizar as atividades de tratamento de dados pessoais respeitando e priorizando os direitos e garantias dos clientes. Dessa maneira, deve imprimir os mais variados esforços para garantir que os titulares de dados sejam corretamente atendidos quando realizarem requisições.

Como as de retificação e de atualização de seus dados, bem como deve ser garantida aos clientes a possibilidade de revogação de seu consentimento nos tratamentos em que esse for solicitado.

Além disso, o colaborador deve garantir aos clientes informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, assegurando, também, a impossibilidade de realização do tratamento para fins discriminatórios, ilícitos ou abusivos.

Portanto, são direitos dos clientes, enquanto titulares de dados, informação sobre o tratamento, eventuais compartilhamentos, as condições do consentimento, quando for o caso, e a possibilidade de sua revogação.

4- Anonimização e Pseudonimização dos Dados Pessoais

O colaborador deve utilizar os meios técnicos razoáveis e disponíveis no momento do tratamento, para garantir, sempre que necessário, a manutenção da privacidade do cliente, a anonimização ou pseudonimização dos dados pessoais, situações empregadas para que o dado perca, permanentemente ou temporariamente, a possibilidade de associação, direta ou indireta, a um indivíduo.

A pseudonimização é o tratamento de dados pessoais que garante que tais dados não possam mais ser atribuídos ao titular de dados sem o uso de informações adicionais. Na pseudonimização, os dados permanecem como dados pessoais.

Por sua vez, a anonimização é o tratamento de dados pessoais que garantem que os dados não possam mais ser atribuídos ao titular de dados de forma alguma. Os dados pessoais que passam pelo processo de anonimização se tornam dados estatísticos.

5- Consentimento

O consentimento é a manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados Pessoais para uma finalidade determinada. Nesse sentido, caso o consentimento seja coletado para o tratamento dos dados pessoais, deve-se garantir que todos seus requisitos sejam cumpridos.

Além disso, o colaborador deve garantir instrumentos controles para gerenciar a concessão ou revogação do consentimento pelo cliente.

O consentimento explícito é necessário para o tratamento de dados pessoais sensíveis: origem racional ou étnica, dados genéticos ou biométricos, filiação política, religiosa ou filosófica, dado referente à saúde ou a vida sexual, opinião política, filiação sindical e convicção religiosa.

6- Avaliações do Risco

O colaborador deve realizar o diagnóstico dos processos de tratamento dos dados pessoais, identificando os riscos envolvidos na atividade.

Compreendendo a importância da mitigação desses riscos para evitar incidentes de segurança, o colaborador deve elaborar um plano de conformidade do processamento de dados, contendo: a descrição do risco (área de ocorrência, atividade afetada e evento de risco), a avaliação do risco eminente (probabilidade, impacto, nível de risco inerente), a avaliação do risco residual (controles existentes, avaliação do controle, nível de risco residual) e o plano de resposta ao risco (tipo de tratamento, medidas de tratamento, responsável pela implementação das medidas).

7- Compartilhamentos dos Dados Pessoais

O compartilhamento de dados pessoais somente deve ocorrer.

Quando consentâneo com a finalidade do tratamento desses dados. Em algumas situações, é necessário, inclusive, o consentimento do titular de dados para que esse compartilhamento seja permitido, obedecidos os requisitos legais.

Dessa mesma forma, é obrigação do colaborador não compartilhar documentos com os dados pessoais dos clientes por e-mail, nuvens não homologadas pela Câmara e, especialmente, por aplicativos de comunicação instalados nos celulares funcionais ou pessoais.

8 - Treinamento e Comunicação

O estabelecimento de uma cultura de proteção de dados e privacidade é indispensável para o desenvolvimento do tratamento de dados baseado nos princípios da Lei Geral de Proteção de Dados.

O colaborador deve sempre buscar o aprimoramento de sua capacidade decisória quanto as atividades envolvidas no tratamento de dados pessoais por meio de capacitações relacionadas com o tema. Além disso, deve se colocar como agente promotor das boas práticas de proteção de dados e privacidade no ambiente da sua unidade, incentivando os demais colaboradores a realizarem suas atividades também em conformidade com essas boas práticas.

9 - Resposta a Incidentes de Segurança.

As boas práticas de proteção de dados e privacidade também exigem do colaborador / funcionário prontidão no atendimento a incidentes de seguranças. Vazamentos de dados pessoais, co-rompimento do banco dedados, utilização de ferramenta não autorizada, ou até mesmo documentos contendo dados pessoais esquecidos na impressora devem ser considerados incidentes de seguranças e ser tratados pelos colaborador de forma séria e diligente.

Todos os esforços para responder ao incidente devem ser adotadas, especialmente a transparência na comunicação ao superior hierárquico, a chefia de gabinete (nos termos do art. 7º do Decreto (Nº 59.767) e ao titular de dados pessoais.

10- Monitoramento

O colaborador deve monitorar se todas as regras, políticas, processos e procedimentos estão sendo observados nas atividades de tratamento de dados pessoais, garantindo, assim o cumprimento das garantias e direitos dos titulares desses dados.

Além disso, deve sempre buscar, no monitoramento, uma forma de promoção de melhorias nas suas atividades de tratamento dedados pessoais, corrigindo erros e inconsistências que venha a detectar por meio desse monitoramento.

11- INTERPRETAÇÃO

A privacidade é o uso adequado dos dados. Quando as administrações públicas coletam informações fornecidas pelos cidadãos, vereadores, demais interessados elas devem usar esses dados apenas para a finalidade a que se designam.

12- CONDUTAS RECOMENDADAS / BOAS PRÁTICAS

- Conhecer os direitos dos titulares e saber direcioná-lo ao encarregado que poderá atende-lo sobre o aspecto do tratamento de dados pessoais;
- POLÍTICA DA TELA BLOQUEADA + POLÍTICA DA MESA LIMPA.
- Utilizar antivírus em suas máquinas;
- Utilizar Senhas Fortes / Trocar de Senha Periodicamente;
- Sugerir medidas que possam contribuir para a proteção de dados pessoais da sua empresa, do seu Setor.
- Ler as Políticas de Privacidade e Termos de uso dos Sites.

Afinal o que são termos de Uso e Política de Privacidade?

Os **Termos e Condições** indicam as regras que devem ser respeitadas ao se fazer uso do site e podem prevenir eventuais reclamações dos usuários.

O **Aviso de Privacidade de Dados** é utilizada para informar aos usuários do site como suas informações pessoais serão coletadas, armazenadas e compartilhadas com outros parceiros ou vendidas para outras empresas.

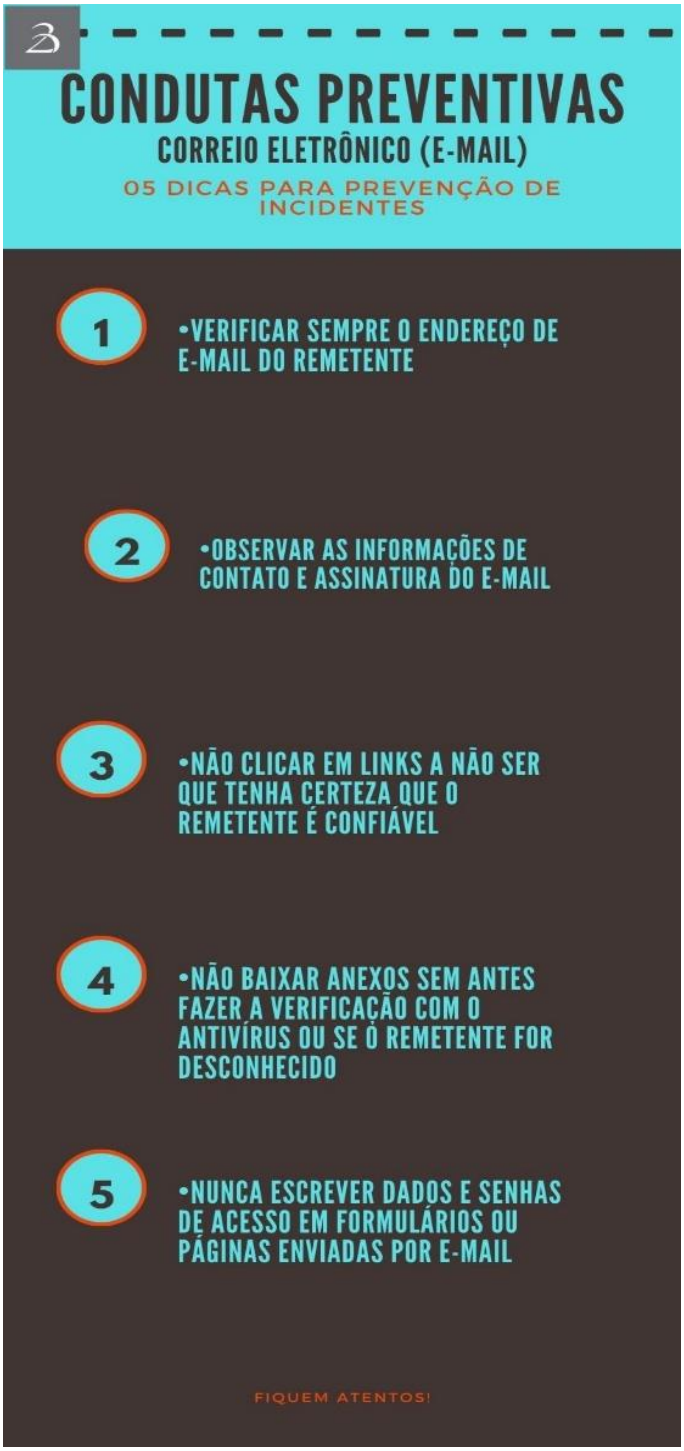
"Termo de Uso" e o "Aviso de Privacidade" são **contratos eletrônicos** que visam limitar a responsabilidade, direcionar a forma de utilização do seu produto/serviço por parte dos clientes, assim como esclarecer possíveis dúvidas que seu cliente tenha sobre o funcionamento do seu serviço/produto.

Tais documentos são **contratos de adesão** (significa que há imposição dos termos e condições aos clientes), portanto, devemos entender que para que esses documentos tenham validade jurídica precisamos estabelecer as cláusulas de modo coerente e sem abusividade.

Obs.: As vítimas comuns incluem sistemas desatualizados ou sem detecção de vírus e spam.

13- PECULIARIDADES SOBRE AUTILIZAÇÃO DO E-MAIL

Com o intuito de prevenir incidentes relacionados à utilização do correio eletrônico, sugerimos as seguintes condutas a serem adotas:



13.1 Do Direito à privacidade na utilização de e-mail

O Poder Judiciário através do julgamento de casos, entende que o direito à privacidade não se aplica sobre a caixa de e-mail referente a conta corporativa.

Portanto, havendo algum incidente que careça de acesso ao e-mail pelo órgão ou empresa, estes poderão acessá-los sem qualquer objeção.

13.2 Como identificar e-mail suspeito

Os golpistas tentam copiar e-mails e mensagens de texto de empresas legítimas para enganar você e obter senhas e informações pessoais. Estes sinais podem ajudar a identificar fraudes:

- O endereço de e-mail ou telefone do remetente não correspondem ao nome da empresa a qual ele alega pertencer.
- O endereço de e-mail ou telefone usados para entrar em contato com você não são os mesmos que você informou à empresa.
- Um link em um e-mail parece correto, mas o URL não corresponde ao site da empresa.
- O e-mail é bem diferente dos outros que você já recebeu da empresa.
- O e-mail solicita informações pessoais, como o número do cartão de crédito ou a senha de uma conta.
- O e-mail não foi solicitado e contém anexo.

13.3 Reconhecer e evitar e-mails de phishing

Phishing refere-se a tentativas fraudulentas de obter suas informações pessoais. Os golpistas usam todos os meios possíveis — e-mails e mensagens de texto falsos, anúncios pop-up enganosos, downloads falsos, spam no calendário e até mesmo chamadas falsas — para induzir você a compartilhar informações, como a senha do ID Apple ou os números dos cartões de crédito.

14-SENHAS

14.1 – O que é?

Uma **senha** ou **palavra-passe**ou ainda **palavra-chave** ou ***password***, é uma palavra ou código secreto previamente convencionado entre as partes como **forma de reconhecimento.**

14.2- Finalidades das senhas

Em sistemas de computação, senhas são amplamente utilizadas para autenticar usuários e conceder-lhes privilégios — para agir como administradores de um sistema, por exemplo ou permitir-lhes o acesso a informações personalizadas armazenadas no sistema.

MAS NÃO SÓ, como tais chaves são capazes de identificar um usuário, elas também são capazes de trazer a responsabilização cível, criminal, administrativa em caso de prática / conduta ilícita, discriminatória no mundo da web.

Enganam-se quem acredita que a internet é terra sem lei, as mesmas infrações previstas em nossas legislações também valem para o mundo digital.

14.3-A importância da Alteração

Um usuário deve alterar a senha a cada 30 dias e um histórico das 12 senhas anteriores garante que o usuário crie senhas exclusivas durante um ano.

14.4 Criação de Senhas Fortes

Para se proteger dos mais novos métodos de invasão, você precisa de senhas robustas. E se você está se perguntando: "qual é a força da minha senha?", veja algumas dicas de como criar senhas fortes:

1. **Ela é longa?** Tente usar pelo menos 10 ou 12 caracteres, ou o máximo possível.
2. **Ela é difícil de adivinhar?** Evite sequências, como "12345" ou "qwerty", pois elas podem ser hackeadas por força bruta em segundos. Pelo mesmo motivo, evite também palavras comuns ("senha1").
3. **Ele tem tipos variados de caracteres?** Letras minúsculas e maiúsculas, símbolos e números devem fazer parte da senha. A variedade pode tornar a sua senha mais imprevisível.
4. **Substituições óbvias de caracteres** são evitadas**?** Por exemplo, usar o número zero "0" no lugar da letra "O". Essas substituições já estão codificadas nos softwares de hackeamento atuais. Então, evite isso.
5. **A senha usa combinações de palavras incomuns?** As senhas podem ser mais seguras se usarem palavras inesperadas. Mesmo que você use palavras comuns, é possível organizá-las em uma ordem estranha e certificar-se de que não estejam relacionadas. Ambos os métodos podem neutralizar os hackeamentos baseados em dicionários.

6. **Você consegue memorizá-la?** Use algo que faça sentido para você, mas que será difícil para os computadores adivinharem. Mesmo senhas aleatórias podem ser lembradas pela memória muscular, sendo semilegíveis. Mas senhas que impeçam o seu acesso não ajudam muito.
7. **Você já usou a senha antes?** Reutilizar senhas compromete várias contas. Use sempre algo original.
8. **A senha apresenta uma regra difícil de ser adivinhada por computadores?** Um exemplo pode ser uma senha de três palavras com quatro letras cada, onde as duas primeiras letras de cada palavra são substituídas por números e símbolos. Por exemplo: "?4sa#2to?6da" em vez de "casagatovida".

Exemplos de senhas seguras

Geralmente, existem duas abordagens principais para criar senhas confiáveis:

Senhas com palavras, que são baseadas em uma combinação de várias palavras reais. Palavras incomuns com caracteres trocados ou aleatórios foram usadas no passado, como "Tr1que" para "truque" ou "F4t7b4LL" para "futebol". Os hackeamentos de algoritmos já conhecem esse método e, por isso, as melhores senhas com palavras geralmente usam uma mistura de palavras comuns não relacionadas em ordem aleatória. Às vezes, é possível usar uma frase cortada e invertida com um padrão que só o usuário conhece.
Por exemplo, "gaT!Esc#l?Cas!" (usando as palavras *gato, escola* e *casa*.)

As senhas com palavras funcionam porque são:

- Fáceis de lembrar.
- Enganam as invasões baseadas em dicionários e de força bruta.

Sequências de caracteres aleatórios, que são puramente ao acaso e usam uma combinação de todos os tipos de caracteres. Essas senhas incluem letras maiúsculas e minúsculas, símbolos e números em ordem espontânea. E como não há um método lógico de organização dos caracteres, é incrivelmente difícil de adivinhá-las. Mesmo um software de hackeamento pode levar trilhões de anos para descobrir essas senhas.
Um exemplo de sequência de caracteres aleatórios pode ser "f2m_+Vm3cV*j" (que pode ser lembrado usando o mnemônico, *fruta 2 maçã _ + VISA música 3 café VISA * joao)*.

As sequências de caracteres aleatórios funcionam porque são:

- Quase impossíveis de adivinhar.
- Muito difíceis de hackear.
- Podem ser lembradas pela memória e por mnemônicos.

Exemplos de senhas fortes

Ao criar sua senha, exemplos podem ajudar durante o processo.

Veja algumas dicas de como criar uma senha forte:

Exemplo 1: EUqUsO!bOsEfE?

Exemplo 2: !HMnrsQ4VaGnJ-tT

Exemplo 3: rosapatosimpleslua

14.5 Procedimento para alteração de Senhas

14.6. Gerenciador de Senhas Fortes

Os usuários precisam usar senhas diferentes para cada sistema, pois se um criminoso decifrar a senha do usuário uma vez, ele terá acesso a todas as contas do usuário. Um gerenciador de senha pode ajudar o usuário a criar e lembrar de senhas fortes. Clique no link abaixo para visualizar um gerador de senhas fortes.

https://privacycanada.net/strong-password-generator/

16- A IMPORTÂNCIA DO BACKUP

Backups precisos ajudam a manter a integridade de dados, se os dados forem corrompidos. Uma empresa precisa verificar o seu processo de backup para garantir a integridade do backup, antes que ocorra perda de dados.

Aconselha-se a realização de backup periodicamente.

Entenda junto ao Departamento de TI (Tecnologia e Informação) como se dá o backup da sua empresa.

17- DICAS PRÁTICAS

1. Como identificar um boleto falso
2. Como identificar um site de compra falso
3. Como identificar o golpe do falso financiamento:

Acesse o link e assista o vídeo abaixo:

https://g1.globo.com/fantastico/noticia/2021/01/31/mais-de-60-milhoes-de-brasileiros-ja-sofreram-com-fraude-financeira-na-internet-diz-pesquisa.ghtml

2 – Como autenticar o whatsapp em duas etapas

Acesso o link: https://www.youtube.com/watch?v=SpCONE_gYKE

3.Se o navegador exibir pop-ups incômodos

Se, ao navegar na Internet, você vir um pop-up ou alerta que oferece um prêmio gratuito ou que informa um problema no dispositivo, não acredite. Esses tipos de pop-up geralmente são anúncios fraudulentos, criados para induzir você a fornecer informações pessoais ou dinheiro ao golpista.

Não ligue para o número nem clique nos links para solicitar o prêmio ou corrigir o problema. Ignore a mensagem e continue navegando na página ou feche a janela ou aba.

4.Se uma solicitação para fazer download de software for exibida

Tenha muito cuidado ao fazer download de conteúdo da Internet. Alguns downloads disponíveis na Internet podem não conter o software que alegam ter ou podem conter software imprevisto ou indesejado. Isso inclui apps que solicitam a instalação de perfis de configuração que podem controlar seu dispositivo. Se instalados, software desconhecido ou indesejado pode se tornar invasivo e irritante e pode até danificar o Mac e roubar os dados.

5. Se você receber uma ligação ou voicemail suspeitos

Os golpistas podem falsificar números de telefone reais de empresas e fazer elogios e ameaças como forma de pressionar você a fornecer informações, dinheiro e até cartões de crédito. Se você receber uma ligação suspeita ou não solicitada de alguém que afirma ser da Apple, encerre a ligação.

6.SÉRIE DE VÍDEOS SOBRE SEGURANÇA CIBERNÉTICA

A Cybersecurity and Infrastructure Security Agency e o Cybersecurity Educationand Training Assistance Program, CYBER.ORG , formaram uma parceria para produzir a Série Cyber Safety. Assista aos vídeos a seguir para obter dicas sobre como se manter seguro online:

- **Série de segurança cibernética: Phishing** - neste vídeo, abordamos o phishing, que é o processo em que golpistas enganam você para que forneça suas informações pessoais.

  https://www.youtube.com/watch?v=08oJtFFH6a0

- **Série de segurança cibernética: Segurança** de videochamada - Neste novo mundo de videochamadas, é mais importante do que nunca usar boas práticas de segurança cibernética em todas as reuniões das quais participamos.

  https://www.youtube.com/watch?reload=9&v=m-Sy92NjFmY

- **Série Cyber Safety: Segurança em jogos online** - Neste vídeo, falamos sobre segurança em jogos online. Aqui estão algumas dicas rápidas para ter certeza de que

você está seguro no vasto mundo dos jogos e mantendo suas informações pessoais privadas!

https://www.youtube.com/watch?v=V1b4odH-20g

- **Série Cyber Safety: Fazendo senhas fortes** - Assim, o vídeo apresenta métodos para fazer uma senha memorável com as letras, números e caracteres especiais necessários que serão seguros e manterão suas informações privadas.

  https://www.youtube.com/watch?v=OiQKZWNeAjc&feature=emb_title

  Obs.: Os vídeos são em idioma inglês, mas é possível acionar a tradução automática para o português.

7-RESUMO DA PROBLEMÁTICA ENVOLVENDO A PROTEÇÃO DOS DADOS PESSOAIS

Acesse o link:

https://g1.globo.com/fantastico/noticia/2021/05/30/cartao-clonado-motoboy-anuncio-falso-golpes-explodem-durante-a-pandemia-veja-casos.ghtml

18- MUDANÇA CULTURAL / MINDSET

MAIS IMPORTANTE: Entenda a importância dessas mudanças e coloque em prática no seu dia a dia. Será preciso mudar nossos hábitos, e isso depende da mudança em nossa mente.

COLOQUE EM PRÁTICA ESSA MUDANÇA CULTURAL!

19- CANALDE COMUNICAÇÃO

protecaodedados@vargemgrandedosul.sp.leg.br

Encarregado de Dados: Dra Caroline Salvi Brandão, procuradora jurídica.