CARTILHA DE SEGURANÇA DA INFORMAÇÃO

Encontre aqui orientações para manter os seus dados e dos nossos cooperados sempre protegidos.

SICOOB

INTRODUÇÃO

Nas próximas páginas, você vai encontrar informações importantes sobre:

- Lei Geral de Proteção de Dados Pessoais (LGPD);
- Melhores práticas no tratamento de dados pessoais;
- Orientações de segurança para home office;
- Como proteger seus dados;
- Informações pessoais em redes sociais;
- Utilização de dispositivos móveis;
- Evitando ataques de engenharia social; e
- Dicas para evitar Phishing.

Consulte este documento sempre que precisar.

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A Lei Geral de Proteção de Dados Pessoais (LGPD) - Lei nº 13.709/2018, regula e impõe uma profunda transformação na forma pela qual as empresas no Brasil utilizam ou tratam dados pessoais. Ela visa garantir que as pessoas tenham mais privacidade e controle sobre seus dados, e que seja evitado o mal-uso deles por terceiros. Entenda um pouco mais sobre a LGPD:

- A Lei Geral de Proteção de Dados Pessoais (LGPD) foi criada para regulamentar o tratamento dos dados pessoais e fazer com que a privacidade das pessoas seja respeitada. Com a LGPD, os dados pessoais só poderão ser tratados se respeitarem princípios citados na Lei, como finalidade, necessidade, transparência, segurança, não discriminação etc.;
- Todos os processos que tratam dados pessoais devem estar em conformidade com a LGPD. Portanto, além de tomar cuidado com os seus dados, você também deve tomar cuidado com os dados de outras pessoas que de alguma forma são tratados por você, principalmente, evitando seu vazamento;
- Tratamento é qualquer ação que seja executada com os dados pessoais, como um simples registro ou acesso de dados de colaborador (como RG, CPF, endereço, biometria etc.), armazenamento, transferência, classificação, eliminação, ou qualquer outra manipulação de dados pessoais. Sendo assim, é importante estar atento, pois a LGPD impactará várias áreas, como RH, Marketing, administrativo, TI, dentre outras. E além dos meios digitais, isso também vale para meios físicos, como formulários em papel, documentos, registros manuais de portarias para acesso em condomínio etc.;
- A LGPD demanda uma mudança de atitude para a forma de como tratamos os dados pessoais e isso terá impacto nos processos do negócio. Quem não cumprir a Lei, pode ter a atividade de coleta de dados suspensa, a ampla divulgação da infração para a imprensa e até mesmo a possibilidade de receber multa. E não se trata apenas de estar em conformidade com a Lei, mas também de manter a conformidade ao longo do tempo. Portanto, todos nós devemos conhecer os princípios da LGPD, pois, de alguma forma, utilizamos dados de cooperados e/ou dos colaboradores em nossas atividades.

Para complementar, temos um curso pra você!

Acesse o módulo de educação do sistema de gestão de pessoas e dê o play no curso sobre a LGPD.

MELHORES PRÁTICAS NO TRATAMENTO DE DADOS PESSOAIS

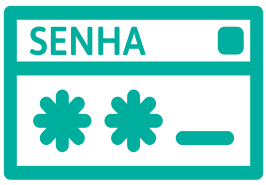
É necessário cuidado ao manipular dados pessoais de outras pessoas e ser conservador com os seus próprios dados pessoais. Seguem dicas de melhores práticas para o tratamento de dados pessoais:

- Ao compartilhar seus dados em aplicativos e serviços online, procure saber todas as finalidades da utilização e evite o uso por pessoas não autorizadas;
- Ao utilizarmos redes sociais, estamos disponibilizando nossos dados pessoais. Por isso, tenha cuidado com quais dados você compartilha;
- Limite o acesso às suas informações pessoais às pessoas que, de fato, precisam delas para a execução de suas atividades;
- Se precisar divulgar dados pessoais, verifique antes a identidade da pessoa que solicita e a real necessidade de passar essa informação;
- Sempre questione se, para a aquisição de determinado produto ou serviço, você precisa realmente informar todos os dados solicitados;
- Cuidado com mensagens aparentemente legítimas e verdadeiras que são utilizadas para capturar dados de usuários;
- Seja cuidadoso(a) com o que você compartilha. Quanto mais informações pessoais você revela online, mais vulnerável você fica a roubo de identidade e golpes;
- Proteja sua privacidade. Leia a política de privacidade de sites onde você está compartilhando conteúdo e saiba como sua informação poderá ser usada;
- Pense a longo prazo. Uma vez que uma informação é compartilhada na Internet, talvez nunca mais possa ser deletada;
- Bloqueie sua estação de trabalho sempre que for se ausentar;
- Não armazene dados pessoais sensíveis localmente em sua estação de trabalho, como por exemplo, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político;
- Não utilize o verso de fotocópias com dados pessoais ou informações sensíveis como folhas de rascunho;
- Se for necessário armazenar dados pessoais fisicamente, guarde-os em armários com portas fechadas à chave, ou em local seguro e de acesso restrito; e
- Tenha cautela ao descartar documentos com informações pessoais ou dados sensíveis. É importante fazer esse descarte após utilização de um triturador ou fragmentadora de papel.

ORIENTAÇÕES DE SEGURANÇA PARA HOME OFFICE

Trabalhar de casa tem sido uma alternativa mais segura neste momento, por conta da Covid-19. No entanto, essa ação exige cuidados redobrados com a segurança. Se você está em home office, siga essas dicas e saiba como manter suas informações seguras mesmo longe da organização:

- Utilize somente sua rede residencial ou móvel para o trabalho remoto. Não realize o acesso remoto por meio de rede wi-fi pública ou de vizinhos;
- Se possível, configure uma senha forte para seu wi-fi; E, principalmente, assegure que seu roteador não está configurado com a senha padrão do fabricante;
- Sempre que possível, utilize dispositivos corporativos que já possuam as configurações e atualizações de segurança da organização para a realização do acesso remoto, ao invés de dispositivos pessoais;
- Não é permitido o acesso aos equipamentos e sistemas de informações da empresa por pessoas não autorizadas (familiares, visitantes, desconhecidos, etc);
- Não realize o acesso remoto por meio de máquinas instaladas em locais públicos (Coworking, Lan House, Cyber café e outros locais do gênero);
- Bloqueie seu computador sempre que se ausentar da estação de trabalho;
- Mantenha as estações de trabalho, dispositivos móveis e os computadores portáteis atualizados com todos os patches de correção e de segurança fornecidos pelo fabricante, devidamente aplicados;
- Evite usar opções de preenchimento automático de dados como “Lembre-se de mim”;
- Se suspeitar de comprometimento da sua senha de acesso, troque-a imediatamente;
- Não discuta informações confidenciais em locais públicos ou de circulação de pessoas não ligadas à empresa;
- Utilize o acesso via VPN somente para execução de atividades que requeiram esse tipo de acesso;
- Esteja atento caso receba ligação de alguma pessoa se identificando como colaborador , solicitando informações sensíveis, pedindo que seja informada alguma senha padrão, a execução de algum procedimento como alteração de perfil ou concessão de acesso, pois pode ser uma pessoa mal-intencionada se passando por um colaborador; e
- Nunca forneça informações sensíveis, pessoais ou da empresa, por telefone ou outros meios, quando a iniciativa do contato não for sua.



COMO PROTEGER SEUS DADOS

Você sabe criar senhas fortes, seguras e difíceis de adivinhar? Com essas dicas simples, você aprende a fazer isso e deixa seus dados mais protegidos. Dá uma olhada:

- Crie senhas fortes e difíceis de decifrar por pessoas mal-intencionadas;
- Sua senha é pessoal, inequívoca e intransferível. Jamais revele-a a terceiros, nem mesmo para um colaborador do Sicoob ou alguém de sua confiança;
- Evite gravar senhas para preenchimento automático em sistemas e browsers;
- Não guarde sua senha em agenda, gaveta ou próxima ao monitor;
- Mude suas senhas regularmente ou ao suspeitar de quebra de sigilo;
- Não utilize as mesmas senhas para acesso aos sistemas do Sicoob e sistemas pessoais;
- Ao criar uma senha, evite usar palavras curtas, data de nascimento, telefone ou sequências (exemplo:"123456", "qwerty", "asdfghjkl", etc). Para montar uma senha forte, use letras maiúsculas e minúsculas, números e símbolos;
- Ninguém está autorizado a solicitar sua senha em nome do Sicoob;
- Desconfie e não clique em links desconhecidos recebidos por WhatsApp, Telegram, SMS e outros;
- Verifique as configurações de privacidade das suas redes sociais e seja sempre cauteloso com o que você posta publicamente; e
- Evite compartilhar suas informações pessoais, como número de telefone ou data de aniversário. Estas informações são peças-chave para verificação de identidade e conta, e podem ser utilizadas por pessoas mal-intencionadas.

INFORMAÇÕES PESSOAIS EM REDES SOCIAIS

O número de pessoas que utilizam redes sociais é altíssimo e, com isso, há constante aumento de vazamentos de informações pessoais de usuários. Por exemplo, mais de 540 milhões de usuários do Facebook já tiveram seus dados expostos em servidores na nuvem, sem qualquer tipo de senha de acesso. É importante citar, ainda, que os dados pessoais são importantes ativos de marketing, pois as empresas podem saber detalhes dos gostos e preferências. O principal valor desses dados é, certamente, conseguir prestar serviços cada vez mais personalizados, conforme os anseios, desejos individuais. Por isso, é preciso cuidado ao compartilhar dados pessoais em redes sociais.

Seguem algumas dicas para utilizar as redes sociais e manter cautela com seus dados pessoais:

- Seja cuidadoso com o que você posta e compartilha nas redes sociais. É ótimo quando somos lembrados, mas também pode ser muito perigoso;
- Leia e conheça a política de privacidade de sites de mídias sociais, pois é assim que você fica sabendo como seus dados serão utilizados;
- Evite compartilhar sua vida e rotina, pois pessoas mal-intencionadas podem utilizar suas informações pessoais para prática de crimes diversos;
- Altere e limite o compartilhamento de dados nas suas redes sociais por meio das configurações de privacidade;
- Bloqueie propagandas baseadas nas suas informações pessoais, alterando as configurações de uso de dados por anunciantes na plataforma;
- Evite fazer check-in nas redes sociais, indicando o local que você está no momento. Quando você faz isso, a sua localização é compartilhada também com pessoas mal-intencionadas;
- Desative a sincronização dos aplicativos de redes sociais com os contatos do seu celular. Essa permissão é opcional e deve ser negada;
- Apague seu histórico periodicamente. Redes sociais armazenam suas ações como acessos, curtidas, pesquisas, comentários, páginas acessadas etc. Em caso de vazamento de contas, pessoas desconhecidas podem ter acesso a todo seu histórico. Além disso, também é indicado apagar o cache e cookies regularmente, limitando o acesso às suas ações em navegadores da Internet, utilizadas por empresas para venda de anúncios direcionados;
- Não permita o reconhecimento facial. Apesar de interessante, é arriscado. Afinal, seu rosto fica armazenado no banco de dados e pode ser encontrado em imagens diversas da Internet, sendo veiculado fora da rede social.

UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS

Assim como seu computador, o seu dispositivo móvel também pode ser usado para a prática de atividades maliciosas, como furto de dados, envio de spam e propagação de códigos maliciosos.

Confira dicas de segurança para utilização de dispositivos móveis:

- Instale um software antimalware antes de instalar qualquer aplicativo, principalmente aqueles desenvolvidos por terceiros;
- Mantenha o sistema operacional e os aplicativos sempre atualizados;
- Fique atento às notícias do fabricante, principalmente sobre segurança;
- Seja cuidadoso ao instalar aplicações desenvolvidas por terceiros, como complementos, extensões e plug-ins. Procure por fontes confiáveis e bem avaliadas pelos usuários, e verifique se as permissões necessárias para a execução são coerentes com a destinação da aplicação;
- Tenha cautela ao usar aplicativos baseados em geolocalização, pois isto pode comprometer a sua privacidade;
- Evite utilizar redes Wi-Fi públicas;
- Mantenha interfaces de comunicação como bluetooth e Wi-Fi desabilitadas, e somente as habilite quando for necessário;
- Configure a conexão bluetooth para que seu dispositivo não seja encontrado por outros dispositivos;
- Sempre que possível, mantenha as informações de dados pessoais sensíveis em formato criptografado;
- Fique de olho no seu dispositivo móvel, principalmente em locais de risco. Procure não o deixar sobre a mesa e tenha cuidado em ambientes públicos;
- Use conexão segura sempre que a comunicação envolver dados confidenciais;
- Cadastre uma senha de acesso que seja forte e bem elaborada, combinando números, símbolos e letras maiúsculas e minúsculas;
- Configure-o, se possível, para que os dados sejam apagados após algumas tentativas de desbloqueio sem sucesso. Use esta opção com cautela, principalmente se você tem filhos e eles “brincam” com o seu dispositivo;
- Ao se desfazer do seu dispositivo móvel, apague todas as informações nele contidas e restaure a opção de fábrica.

EVITANDO ATAQUES DE ENGENHARIA SOCIAL

Engenharia social é a habilidade de um cibercriminoso conseguir acesso a informações confidenciais de uma empresa por meio da persuasão. Execute suas atividades com muita atenção, para que pessoas mal-intencionadas não induzem você a passar informações sensíveis ou executar alguma tarefa da qual possa ser tirado proveito.

Para evitar golpes de Engenharia Social, siga essas importantes recomendações de segurança:

- Caso receba uma ligação de alguém se identificando como colaborador do Sicoob, solicitando informações sensíveis ou pedindo alguma senha padrão, por exemplo, fique atento! Pode ser uma pessoa mal-intencionada se passando por um colaborador;
- Evite fazer cadastros na Internet, especialmente fornecendo seus dados pessoais;
- Nunca forneça informações sensíveis, pessoais ou da empresa, por telefone ou outros meios, quando a iniciativa do contato não for sua;
- Use as ferramentas oficiais do Sicoob, como a Central de Suporte e Serviços do Sicoob (Top Desk), Microsoft Teams e Outlook para conversar com outros funcionários. Por meio delas podemos identificar e validar o solicitante;
- Seja cuidadoso com o que você posta na Internet, principalmente nas redes sociais. Essas informações podem ser usadas por malfeitores para confirmar os seus dados cadastrais e responder perguntas de segurança; e
- Evite expor assuntos relacionados ao seu trabalho em público ou em redes sociais. Use o bom senso, sempre!

DICAS PARA EVITAR PHISHING

Phishing é um processo fraudulento utilizado para adquirir informações de usuários, ou até mesmo infectá-los. É a forma mais comum de ataque cibernético e tem uma taxa de sucesso relativamente alta. Seguem dicas para não cair em Phishing:

- Pense bem antes de clicar em links, sejam eles de sites ou e-mails, e nunca clique naqueles que pareçam suspeitos;
- Antes de clicar em algum link, posicione o ponteiro do mouse em cima desse link para que seja exibido o verdadeiro endereço web, depois verifique se este direciona a um site confiável e com boa reputação;
- Nunca abra arquivos anexos suspeitos recebidos por e-mail;
- Se você desconfiar de um e-mail recebido, mesmo que seja de alguém conhecido, cuidado: pode ser um e-mail falso;
- Tenha um cuidado especial com mensagens que solicitam “ação imediata” ou que ameacem você a perder algo caso não responda à mensagem, como, por exemplo, atualizar o aplicativo bancário para não ter a conta bloqueada;
- Evite fornecer informações pessoais por telefone, principalmente em ligações não solicitadas;
- Se algum e-mail parece ser Phishing, provavelmente é. Não teste sua sorte!

E aí, gostou das dicas?

Agora que você chegou até aqui, quer dizer que já aprendeu um pouco mais sobre Segurança da Informação e está mais bem preparado para manter seus dados pessoais e dos nossos cooperados sempre protegidos.

Se ficou alguma dúvida entre em contato com a área de Segurança da Informação pelo e-mail segurancadaInformacao@sicoob.com.br

SICOOB

Cartilha desenvolvida pela área de Comunicação e Marketing