POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

DA COSTA & LEMOS SOCIEDADE DE ADVOGADOS

Introdução

A presente Política de Segurança da Informação ("PSI") tem como objetivo estabelecer regras, controles e responsabilidades no que se refere ao tratamento de informações realizado pela COSTA & LEMOS SOCIEDADE DE ADVOGADOS ("Escritório"), atendendo aos requisitos da legislação brasileira de proteção de dados, incluindo, sem limitação, a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados ("LGPD").

Essa PSI deverá ser observada rigorosamente por todos os sócios, empregados, estagiários, prestadores de serviços, consultores e correspondentes do Escritório.

CAPÍTULO I - REQUISITOS DE SEGURANÇA

1. Todo acesso aos dados, estejam armazenados em meios físicos ou informáticos, deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas. As autorizações devem ser revistas, confirmadas e registradas continuamente pelos sócios.

2. Os dados e os sistemas de informação do Escritório devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a integridade, sigilo e disponibilidade dos mesmos.

CAPÍTULO II - REGRAS ESPECÍFICAS SOBRE USO DE PROGRAMAS E E-MAIL

3. Não é permitido executar programas que tenham como finalidade a decodificação de senhas, o monitoramento de redes, a leitura de dados de terceiros, a propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços.

4. Não é permitido executar programas, instalar equipamentos, armazenar arquivos ou promover ações que possam facilitar o acesso de usuários não autorizados aos dados armazenados pelo Escritório.

5. Apenas softwares licenciados podem ser usados pelos sócios, empregados, estagiários e consultores do Escritório. O Escritório respeita os direitos autorais dos softwares que usa e reconhece que deve pagar o justo valor por eles, coibindo e monitorando o eventual uso indevido de programas não licenciados.

6. Não é permitido enviar informações confidenciais para e-mails externos desconhecidos sem proteção. Nesses casos, deve-se aplicar senha ao arquivo contendo os dados.

7. O uso do correio eletrônico para envio e recebimento de e-mails profissionais deverá ocorrer apenas por meio do correio eletrônico do Escritório.

8. É proibido o uso do correio eletrônico para envio de mensagens que possam comprometer a imagem do Escritório perante seus clientes e a comunidade em geral, ou que possam causar prejuízo moral e financeiro ao Escritório.

9. Em havendo o recebimento de links ou arquivos anexados oriundos de remetentes desconhecidos ou com características suspeitas, sua abertura ou acesso somente poderá ocorrer após prévia análise por um especialista na área de Segurança da Informação.

10. É vedada a utilização de e-mail para envio de spams (mensagem de conteúdo publicitário), assim como para o envio de e-mails do tipo corrente (alusivos a crianças desaparecidas etc.).

CAPÍTULO III - MÁQUINAS E ESTAÇÕES DE TRABALHO

11. As estações de trabalho, incluindo equipamentos portáteis e documentos físicos, devem ser protegidas contra danos ou perdas, bem como de acesso, uso ou exposição indevidos.

12. O acesso à estação de trabalho deverá ser encerrado no final do expediente, desligando-se o equipamento.

13. Quando se ausentarem de suas respectivas mesas, todos os sócios, empregados, estagiários, prestadores de serviços, consultores e correspondentes que estejam nas instalações físicas do Escritório deverão bloquear suas estações de trabalho (desktops ou notebooks) com senha.

14. Informações sigilosas, corporativas ou cuja divulgação possa causar prejuízo ao Escritório e/ou seus clientes ou terceiros prestadores de serviços, fornecedores ou parceiros em geral só devem ser utilizadas em equipamentos com controles adequados.

CAPÍTULO IV - DISPOSITIVOS MÓVEIS (NOTEBOOKS, CELULARES E TABLETS)

15. Quando em deslocamentos de automóvel, recomenda-se a colocação de notebooks em porta-malas ou em local não visível.

16. O notebook deve ser colocado em mochilas ou malas discretas, em detrimento de malas convencionais para notebook. Não é recomendada a colocação do notebook em carrinhos de aeroportos, tampouco que seja ele despachado junto à bagagem.

17. Em locais públicos (tais como, recepção de hotéis, restaurantes e aeroportos), recomenda-se a manutenção do notebook próximo e sempre à vista, evitando-se distância do equipamento.

18. Em hotéis, sempre que possível, é recomendável a guarda do notebook no cofre do apartamento. É imprescindível avaliar se, em pequenas viagens, faz-se realmente necessário levar o notebook.

19. Para notebooks, tablets e celulares, recomenda-se sempre o uso do bloqueio de tela com senha.

20. É vedado o uso de redes de conexão públicas ou desconhecidas para conectar os dispositivos móveis onde estejam armazenados dados tratados pelo Escritório.

CAPÍTULO V - BOAS PRÁTICAS DE SEGURANÇA

21. Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

22. Ao utilizar uma impressora coletiva, o documento impresso deve ser imediatamente recolhido.

23. O documento confidencial jamais deve ser utilizado como rascunho, devendo ser imediatamente destruído, no caso de descarte.

24. Não devem ser discutidos ou comentados assuntos confidenciais, citados nomes ou tratativas, dentro ou fora do ambiente de trabalho, em locais públicos, ou próximos de visitantes, seja ao telefone ou com algum colega, parente ou fornecedor.

25. É exigido a todos os profissionais quando do seu ingresso no Escritório assinar o acordo de confidencialidade e não divulgação, assumindo o compromisso com as informações tratadas pelo Escritório.

26. Com o encerramento do vínculo de sócio, empregado, estagiário ou consultor, o e-mail corporativo é desativado, devendo ser mantidos os compromissos assumidos, tanto por meio do acordo de confidencialidade, quando pela presente PSI, mesmo após o desligamento.

27. Em caso de extinção do vínculo ou rescisão do contrato, por qualquer motivo, deverá o envolvido devolver todas as informações confidenciais geradas e manuseadas em decorrência da atividade ou emitir declaração de que as destruiu.

28. Todo produto resultante do trabalho dos sócios, empregados, estagiários, prestadores de serviços, consultores ou correspondentes realizado no contexto da relação mantida com o Escritório é de propriedade deste.

29. Uma cópia de segurança de todos os dados armazenados pelo Escritório deve ser mantida atualizada, em periodicidade trimestral.

30. É recomendável a utilização de ferramentas de armazenamento na nuvem (Dropbox, One Drive, Google Cloud, etc.) dos documentos produzidos pelo Escritório. Nesse caso, deverá ser mantida cópia integral e fidedigna de todo o conteúdo armazenado na nuvem em um HD externo, mantido na sede do Escritório.

31. Os sócios, empregados, estagiários e consultores do Escritório devem administrar seus arquivos gravados, excluindo os arquivos desnecessários.

32. É vedado o acesso a sites com conteúdo impróprio.

33. Não é permitido uso de modem 3G considerando a suscetibilidade de acessos ilegais ocorrerem por meio desse tipo de conexão.

34. Na hipótese de ser necessário transportar arquivos por meio de mídias removíveis (HD Externo ou *PenDrive*) e for concedida a autorização necessária para tanto, é recomendado que os arquivos sejam apagados imediatamente após a utilização, a fim de evitar vazamento de informação sensível.

35. Somente os sócios estão devidamente autorizados a falar em nome do Escritório para os meios de comunicação: Blogs, Twitter, Facebook, LinkedIn ou Grupos de Discussão (fóruns, newsgroups e similares).

CAPÍTULO VI – REGRAS ESPECÍFICAS PARA HOME OFFICE

36. As seguintes diretrizes devem ser observadas quando o trabalho para o Escritório estiver sendo executado em Home Office:

- Instalar programas antivírus no caso de uso do desktop ou notebook pessoal para a execução do trabalho em Home Office. Caso o antivírus esteja sendo instalado pela primeira vez, fazer um prévio escaneamento completo no desktop ou notebook;

- Instalar apenas softwares necessários para o trabalho;

- Não permitir que outras pessoas utilizem o computador que é utilizado para executar as tarefas do Escritório;

- Usar apenas a rede Wi-Fi ou cabeada residencial, mas utilizando-se de senha com um padrão forte, com mais de 8 caracteres, contendo letras maiúsculas, minúsculas, números e símbolos;

- Trabalhar a partir de um cômodo isolado da casa e, se possível, de porta fechada;

- Conscientizar os familiares da importância e relevância do seu trabalho para que o Home Office seja produtivo;

- Manter as práticas de arrumação enquanto estiver de Home Office, guardando documentos e anotações em gavetas e bloqueando o computador/notebook;

- Somente utilizar softwares confiáveis e aprovados pelo Escritório para a realização de videoconferências.

CAPÍTULO VII – DISPOSIÇÕES FINAIS

37. As violações de segurança devem ser imediatamente comunicadas aos sócios do Escritório, que analisarão e investigarão a ocorrência, determinando as medidas necessárias, visando à correção da falha ou reestruturação de processos, com o fim de solucionar a questão e minimizar seus efeitos.

38. Esta Política entra em vigor a partir de 01 de agosto de 2019 e tem prazo de validade indeterminado, podendo ser revista e alterada a qualquer tempo.