Título: **MANUAL DA SEGURANÇA DA INFORMAÇÃO - Pública**

1. OBJETIVO

Orientar todos os colaboradores da organização em relação às práticas para o atendimento à política de segurança da informação.

2. ESCOPO

Todos os colaboradores e parceiros de negócio.

3. REFERÊNCIAS

- Norma ISO/IEC 27001:2022;
- PSI 010 - Política de segurança da informação.

4. DEFINIÇÕES

- Conteúdo impróprio: Toda informação que não agrega valor à empresa;
- Mídias: Dispositivos que podem conter e armazenar informações da empresa: CD, DVD, pen0drives, unidades de backup, demais dispositivos em geral;
- Contexto de segurança: área física ou lógica da organização, onde se encontra uma informação e que pode ser utilizada com proteção de controles de segurança. Fora do contexto de segurança ela representa risco para a organização;
- Dado Pessoal (DP): toda informação relacionada a pessoa física que possa identificá-la ou torná-la identificável, como Nome, endereço, CPF, documentos pessoais, telefone, e-mail, etc;
- ANPD: Autoridade Nacional de Proteção de Dados Pessoais, órgão do governo responsável por fiscalizar e cumprir a legislação de dados pessoais no Brasil.

5. A INFORMAÇÃO

A informação é o bem mais precioso da empresa e ela deve ser tratada de forma a garantir a:

- **Confidencialidade –** é uma propriedade de que a informação esteja disponível somente às pessoas autorizadas;
- **Integridade –** propriedade da informação que garante sua precisão, confiabilidade, sua completude ao longo do processo ou do seu ciclo de vida;
- **Disponibilidade –** ela deve estar disponível para aqueles que, por direito, têm acesso a qualquer momento no seu ciclo de processamento.

6. COMPORTAMENTO SEGURO

Espera-se que os colaboradores mantenham o comportamento adequado mediante as tecnologias, normas e procedimentos que utilizam, bem como em conformidade com os valores da sociedade a qual pertencem. Sugerimos, assim, um padrão adequado para nossa empresa nos seguintes aspectos:

- É proibida a instalação de softwares no seu computador sem a homologação do departamento de TI. Toda necessidade de instalação deve ser registrada no "service desk";
- Não faça downloads de origem duvidosa;
- Não visite sites não confiáveis ou de conteúdo impróprio;
- Não divulgue informações internas e/ou confidenciais sobre a empresa em rodas de amigos, redes sociais, e-mail ou qualquer tipo de mídia sem a expressa autorização da empresa;
- Não são permitidos dispositivos particulares para conexão na rede corporativa da empresa, toda exceção deve ser tratada e formalizada no "service desk" com a devida autorização;
- A utilização de dados pessoais (DP) nos processos organizacionais deve obedecer às diretrizes de segurança da informação e princípios legais relacionados à proteção de dados pessoais. Tome cuidado com as informações de DP que você tem acesso e esteja ciente que os controles de segurança estão atuantes;
- Perceba que pode haver pessoas de má índole que podem querer informações internas da nossa empresa e podem abordar você para questioná-las sobre situações corporativas do seu cotidiano. A resposta deve ser que você não tem autorização para falar sobre esses temas. Esse assunto é conhecido como engenharia social que busca levantar informações sigilosas;
- A mesa de trabalho deve estar sempre limpa de documentos confidenciais quando estiver ausente da sua área de trabalho, post-it com informações devem ser removidos;
- A tela do computador em caso de saída do local de trabalho deve sempre ficar bloqueada para que sempre solicite um usuário e senha;
- No teletrabalho deve-se utilizar de forma discreta o equipamento de processamento remoto quando for feita a conexão em ambiente público. O Ambiente deve ter segurança mínima de acesso para proteger os recursos.

Todo o comportamento impróprio que vá contra essas orientações estará sujeito a sanções disciplinares.

7. ACESSO A SISTEMAS CORPORATIVOS

Os acessos a sistemas corporativos são segregados a níveis de perfis, por função e/ou por usuário. Cada usuário deve ter sua liberação devidamente registrada e aprovada por superior responsável pelo sistema.

Todos os acessos devem ser registrados no sistema de gestão de pessoas para auditoria a qualquer tempo e necessidade.

7.1 SENHAS DE ACESSO

Todos os colaboradores/fornecedores e terceiros da BySeven serão identificados por um nome único de usuário e uma senha particular e intransferível para obter acesso aos sistemas e recursos de TI da empresa. A utilização de usuários genéricos ou compartilhados somente é permitida onde não houver uma forma de contornar o problema e sob autorização e conhecimento da diretoria.

8. ACESSO FÍSICO

Os acessos a empresa devem ser limitados as atividades diárias dos colaboradores em conformidade nossas políticas de acesso. Áreas sensíveis devem ter controle físico limitado, essas áreas devem ser controladas eletronicamente gerando registros de acesso para futura análise em caso de crise.

Os terceiros devem ser acompanhados pelos colaboradores para o atendimento de seus objetivos previamente acordados em propostas de trabalho e/ou contrato de trabalho.

Áreas de risco devem ser sinalizadas para a devida orientação ao usuário.

9. ACESSO À INTERNET

O acesso à internet deve ser utilizado para fins profissionais, agregando valor as funções internas e voltadas para o negócio da empresa. Toda ação contrária poderá ser monitorada e/ou bloqueada, podendo desta forma implicar em sanções disciplinares.

Todo acesso à internet que não estejam diretamente relacionados ao desempenho das atividades dos serviços estabelecidos para a função do colaborador está proibido.

10. ACESSO A E-MAIL

O acesso ao e-mail corporativo deve ser utilizado para fins profissionais, agregando valor as funções internas e voltadas para o negócio da empresa. Toda ação contrária poderá ser monitorada e/ou bloqueada, podendo desta forma implicar em sanções disciplinares.

11. TELETRABALHO (TRABALHO REMOTO)

Todo cliente externo deve ser controlado por sistemas que permitam registro de acesso e suporte à conexão segura, capaz de proteger as conexões de internet**.**

12. USO DE DISPOSITIVOS

A utilização dos dispositivos de processamento deve ser feita exclusivamente para uso corporativo no tratamento da informação alinhado com os processos e objetivos do negócio. As atividades realizadas devem estar alinhadas com a função do recurso que as utilizam. O uso do dispositivo de armazenamento com conteúdo pessoal é proibido, mitigando assim os riscos de conteúdo malicioso na rede.

13. CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as informações geradas em documentos eletrônicos pela empresa devem ser classificadas pelo dono do processo para orientação dos usuários.

13.1 Tratamento de informação confidencial

A informação identificada como confidencial deve ser cercada de cuidados.

O usuário deve observar o contexto de segurança no uso da informação confidencial, que delimita o uso apenas no processo corporativo o qual o uso é permitido. Quando detectado o uso fora do contexto, deve ser acionado uma não conformidade.

O não atendimento a essas recomendações implicará em sanções disciplinares.

13.1.1 Dispositivos móveis com informação confidencial

Os dispositivos móveis devem suportar o uso de criptografia a nível de sistema operacional para garantir que em caso de roubo, haja uma camada resistente de ataques ao sistema de arquivos.

13.1.2 Transferência de informação confidencial

A transferência de informação confidencial deve ser realizada por meio de canal seguro, utilizando-se, de preferência, os canais oficiais corporativos da organização para comunicações externas que necessitem de envio de informações confidenciais da organização.

13.2 Tratamento de informação com Dados pessoais

Todo e qualquer tratamento de dados pessoais da organização deve ser considerado informação **confidencial**. Deve estar de acordo com os requisitos das normas e leis vigentes sobre proteção e privacidade de dados pessoais.

O tratamento de dados deve observar as seguintes diretrizes:

a) **Finalidade:** os processos e sistemas da informação que utilizarem dados pessoais devem ter finalidades, isto é, propósitos legítimos e específicos.

b) **Necessidade:** a coleta e tratamento de dados pessoais deve ser limitada tão somente aos dados estritamente necessários para o cumprimento das finalidades estabelecidas para sua utilização. Dados desnecessários devem ter seu tratamento interrompido e obedecer às orientações de descarte estabelecidas neste manual.

c) **Livre acesso e transparência:** o Titular de dados pessoais tem direito de acessar as informações sobre o tratamento de dados pessoais de forma clara, gratuita e facilitada. Tais informações são disponibilizadas na Política de privacidade publicada no website da organização https://www.byseven.com.br/politica-de-privacidade.

d) **Base legal:** o tratamento de dados pessoais deve ser pautado em ao **menos uma base legal** de tratamento em conformidade com a lei vigente de proteção de dados pessoais. Segue alguns exemplos das bases legais utilizadas na organização:

- Por meio de consentimento formal e por escrito do titular de dados;

- Por cumprimento de obrigação legal ou regulatória pela organização, como leis e normas de natureza trabalhista, fiscal, tributária, previdenciária e etc;
- Por cumprimento de obrigações contratuais, como contratos firmados com clientes, colaboradores, fornecedores e parceiros de negócios;
- Por cumprimento de determinações judiciais e/ou administrativas ou ainda para defesa ou andamento de processos judiciais e/ou administrativos dos quais a empresa é parte ativa ou interessada;
- Por legítimo interesse da organização na oferta de produtos ou serviços aos seus clientes, bem como a serviços que interessem aos seus clientes como solicitação de orçamentos ou de outras informações requeridas pelo cliente.

13.2.1 Comunicações

Eventuais demandas ou suspeitas de violações de dados pessoais e/ou confidencialidade como fragilidades ou falhas relacionadas a segurança dos dados pessoais, que possam trazer danos ou riscos relevantes relacionados a algum titular de dados/clientes, devem ser reportadas pelo usuário, o mais rápido possível, para que sejam tomadas as devidas providências.

Demais demandas, como dúvidas, orientações, sugestões relacionadas ao tratamento de dados pessoais, também devem ser reportadas a qualquer tempo pelo usuário. As demandas informadas acima devem ser direcionadas para o **e-mail: soc@byseven.com.br ou contato@byseven.com.br.**

14. EXCLUSÃO DE INFORMAÇÃO

As informações armazenadas em sistemas de informação, dispositivos ou em qualquer outra mídia de armazenamento deve ser excluída quando não forem mais necessárias. Ao realizar o descarte/exclusão de informações, é importante seguir algumas diretrizes. Em primeiro lugar, identifique os dados que não são mais necessários para as operações da empresa. Isso inclui registros de clientes, documentos financeiros, registros de transações e outros dados sensíveis.

Em seguida, avalie a melhor forma de destruir essas informações. Métodos comuns incluem a destruição física de documentos por meio de trituradoras ou a contratação de serviços especializados em destruição segura. Para dados eletrônicos, é necessário utilizar técnicas de exclusão segura, como a formatação segura dos discos rígidos ou o uso de software de limpeza de dados conforme tópico de descarte de mídias.

15. MÍDIAS REMOVÍVEIS

Os acessos a mídias removíveis (celulares, “pendrives”, cartões de memória, fitas, cds, dvd etc.) fica restrito a usuários específicos através de aprovação gerencial, registrada no “service desk”, sendo proibidos a utilização de dispositivos na rede interna sem autorização.

16. PROPRIEDADE INTELECTUAL

A propriedade da informação gerada pelos colaboradores em qualquer mídia e parceiros contratados é da empresa, desta forma fica proibido a utilização desta informação por terceiros sem a expressa permissão da empresa. O uso da informação sem autorização implica em sanções disciplinares e/ou judiciais conforme a legislação vigente.

17. BLOQUEIOS DE SEGURANÇA CORPORATIVO

Existem bloqueios de segurança estabelecidos dentro da empresa para proteger os recursos tecnológicos como internet, e-mail, estações de trabalho, servidores e serviços. O acesso à internet é limitado e monitorado. A utilização de meios para transpor esses limites estabelecidos implica em sanções disciplinares, pois pode expor a empresa a riscos desnecessários.

Convém que os sistemas de gestão de autenticação das estações sejam bloqueados os sistemas em 5 minutos de inatividade, porém, podem ser insuficientes em caso de um ataque, portanto, os usuários são responsáveis pelo bloqueio manual da sua estação quando ausentes de seu computador.

18. GESTÃO DE MUDANÇA

Toda alteração sistêmica que possa trazer algum impacto para a organização, deve ser devidamente registrada e submetida a critérios de alinhamento e aprovação, observando os princípios de Segurança da Informação.

19. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Um incidente é um evento que pode mudar as características da informação como confidencialidade, integridade e disponibilidade (CID).

Em caso de eventos de segurança da informação, incluindo incidente que envolver dados pessoais, o usuário deve registrar o caso no “service desk” ou entrar em contato com o departamento segurança da informação, pelos canais abaixo informados, para as devidas providências:

- E-mail: **soc@byseven.com.br;**
- Telefone: 47 34329000.

20. HISTÓRICO DE VERSÕES

Data	Versão	Autor	Descrição da Alteração
15/01/2024	0.1	Nelson de Souza	Criação do documento
15/01/2024	1.0	Gabriel D. Lopes	Aprovação de documento