POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO IPRESBS

Art. 1°. A Política de Segurança da Informação tem como objetivo elaborar normativas, estruturar, administrar e garantir segurança da informação por intermédio da utilização dos ativos e recursos de informática do Instituto de Previdência Social dos Servidores Públicos do Município de São Bento do Sul – IPRESBS.

Art. 2°. Esta política norteará a implementação de medidas de proteção de dados que deverão ser aplicadas a toda e qualquer informação, com vistas ao resguardo da imagem e das finalidades institucionais do IPRESBS. As normativas devem ser lidas, entendidas e seguidas em todos os níveis hierárquicos para que a informação tenha o grau de confidencialidade, integridade e segurança exigidos e aplicados aos níveis:

- Estrutura física: Relacionada à segurança dos ativos computacionais, instalações prediais e documentos em meio físico abrangendo, também, o controle de acesso de pessoas às instalações do IPRESBS;
- Estrutura lógica: Relacionada a toda e qualquer informação em meio digital, seja em equipamentos, tráfego de informações pela rede, correio eletrônico ou armazenado em estações de trabalho;
- Recursos humanos: Relacionada à educação e conscientização de cada usuário sobre a responsabilidade para com a segurança da informação, por meio de sugestões e ações educativas.

Art. 3°. Toda informação produzida, recebida ou derivada da atividade profissional pelos usuários pertence ao IPRESBS. As exceções deverão ser explícitas e formalizadas previamente.

Art. 4°. Os equipamentos de informática, comunicação, sistemas, correio eletrônico, internet e intranet deverão ser utilizados exclusivamente para as atividades de interesse do IPRESBS, sendo vedado:

- O acesso a sites não confiáveis, impróprios ou que não estejam relacionados ao desempenho de atividades-fim do Instituto;
- O uso de contas particulares de correio eletrônico para fins institucionais;
- O uso e a instalação de jogos ou o download de arquivos que comprometam o tráfego da rede (vídeos, imagens, músicas, etc.), para fins particulares;
- O uso de dispositivos móveis de armazenamento sem aplicação de antivírus, incluindo-se unidades de armazenamento portáteis, aparelhos celulares e dispositivos eletrônicos.
- A duplicação de softwares ou licenças;
- A instalação não autorizada de softwares, extensões e plug-ins nos computadores ou que façam uso da rede do IPRESBS
- O acesso, armazenamento, edição ou distribuição de qualquer material de cunho sexual ou preconceituoso;
- O armazenamento de arquivos pessoais e/ou não pertinentes a atividade-fim do IPRESBS nos computadores e na rede de dados do Instituto;
- Uso indevido de impressoras para fins particulares;
- A retirada de equipamentos eletrônicos ou arquivos físicos da sede do IPRESBS sem a autorização da autoridade competente.

Art. 5º. Os e-mails encaminhados pelo correio eletrônico institucional deverão adotar assinatura padrão com as seguintes informações:

I – Nome completo do servidor;
II – Cargo, registro no órgão fiscalizador da profissão, setor e certificações (se houver);
III – Nome do Instituto, por extenso;
IV – Telefones do IPRESBS;

Art. 6°. Fica vedada a divulgação ou reprodução de informações produzidas ou recebidas como resultado de atividade com o IPRESBS, sem a autorização da autoridade competente.

Art. 7°. Os usuários deverão ser cientificados da existência da Política de Segurança da Informação e sobre o uso correto dos ativos disponibilizados ao estabelecerem vínculo com o Instituto, de forma a minimizar os possíveis riscos de segurança, bem como garantir o conhecimento de suas responsabilidades.

I – Os servidores efetivos, cedidos, comissionados, estagiários conselheiros e membros do comitê de investimentos ficam cientes de que os ambientes, sistemas, computadores e redes do IPRESBS poderão ser monitorados e gravados, mediante prévia informação.

Art. 8°. Deverá ser constituído um comitê multidisciplinar responsável pela gestão da segurança da informação, doravante designado como Comitê de Segurança da Informação – CSI.

I – O comitê deve ser formalmente constituído por colaboradores de setores diferentes, contendo pelo menos um membro de cada setor

II – Deverá o CSI reunir-se formalmente pelo menos uma vez a cada seis meses, reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou definição relevante para o IPRESBS.

III – O Comitê de Segurança da Informação, também referido como CSI, poderá utilizar especialistas internos ou externos para apoiarem nos assuntos que exijam conhecimento técnico específico.

IV – Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, ou sempre que algum fato relevante ou evento motive sua revisão antecipada, conforme análise e decisão do Comitê de Segurança da Informação

Art. 9°. O IPRESBS adotará providências no sentido de garantir:

I – Que os equipamentos estejam em bom estado de conservação para atender as demandas do Instituto e não comprometam a segurança das informações produzidas;

II – O backup das informações armazenadas de forma automatizada por meio de software especifico, preferencialmente em unidades de memória distintas.

III – A definição e manutenção de regras de acesso e navegação.

IV – O monitoramento e armazenamento de históricos de acessos na rede interna e Internet.

V – A segurança no compartilhamento de arquivos.

VI – A identificação de usuários e acessos.

Art. 10°. O IPRESBS exime-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos, serviços e informações, reservando-se o direto de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

I – O usuário que tomar conhecimento de qualquer irregularidade sobre a Política de Segurança da Informação deverá comunicar imediatamente a autoridade competente do IPRESBS.

II – O descumprimento dos requisitos previstos nesta Política de Segurança da Informação sujeitará o usuário às medidas administrativas e legais cabíveis previstos no Estatuto dos Servidores Públicos de São Bento do Sul.

Art. 11º. A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade (Anexo I). Sendo de responsabilidade:

I – Dos colaboradores:

a) Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes do Instituto poderão ser monitorados e

gravados, com prévia informação, conforme previsto nas leis brasileiras. Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao IPRESBS e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

b) É também obrigação de cada colaborador se manter atualizado em relação a esta Política de segurança da informação e aos procedimentos e normas relacionadas, buscando orientação de seu superior ou autoridade competente sempre que não estiver absolutamente seguro quanto a aquisição, uso e/ou descarte de informações.

c) Manter comportamento ético e responsável quanto a utilização de equipamentos, informações e segurança da informação nas atividades laborais de sua função.

II – Dos Gestores de Pessoas e Processos:

a) Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

b) Atribuir aos colaboradores, na fase de ingresso em cargo público, contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da Política de Segurança da Informação do IPRESBS.

c) Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do IPRESBS.

d) Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

e) Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

III – Do responsável técnico da área de informática:

a) Manter e fazer cumprir a Política de Segurança da Informação;

b) Garantir que equipamentos, computadores, rede, softwares e backup estejam em pleno funcionamento, atendendo aos requisitos e diretrizes desta Política de Segurança da Informação;

c) Elaborar e implementar planos de contingência e continuidade dos principais sistemas e serviços, devendo ser testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação;

d) Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;

e) Administrar, proteger e testar as cópias de segurança dos dados relacionados aos processos críticos e relevantes para o IPRESBS;

f) Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física;

g) Definir as regras formais para instalação de software e hardware em ambiente corporativo, exigindo o seu cumprimento dentro do Instituto.

h) Realizar auditorias periódicas de configurações técnicas e análise de riscos;

i) Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos do IPRESBS;

j) Garantir que todos os servidores, estações de trabalho e demais dispositivos com acesso à rede Instituto operem dentro das diretrizes desta Política de Segurança da Informação;

k) Monitorar o ambiente de informática e informação, gerando indicadores de:

- Uso da capacidade instalada da rede e dos equipamentos;
- Tempo de resposta no acesso à internet e aos sistemas críticos do IPRESBS;
- Períodos de indisponibilidade no acesso à internet e aos sistemas críticos do IPRESBS;

- Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- Atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

IV – Do Comitê de Segurança da informação:

a) Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;

b) Propor alterações nas versões da Politica de Segurança da Informação e a inclusão, a eliminação ou a mudança de normas complementares;

c) Avaliar os incidentes de segurança e propor ações corretivas;

d) Definir as medidas cabíveis nos casos de descumprimento desta Política de Segurança da Informação.

Art. 12º. Para garantir o atendimento das diretrizes mencionadas nesta resolução, o IPRESBS poderá:

I – Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede. Sendo armazenado o histórico que poderá ser disponibilizado para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

II – Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação;

III – Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

IV – Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

Art. 13°. O IPRESBS utilizará de diferentes políticas de acesso e de identificação de usuários nos equipamentos, rede, compartilhamento de arquivos e sistemas.

I – Para acesso aos computadores e compartilhamento na rede do IPRESBS será aplicado identificação de usuários com privilégios diferenciados de acordo com as diretrizes desta Política de Segurança da Informação e ou necessidades individuais, desde que aprovadas pelo Conselho de Segurança da informação, podendo estes estarem ou não vinculados ao domínio de rede ou a aplicação de credenciais de rede.

a) A identificação se dará através de nome de Usuário vinculado a um funcionário o qual não poderá ser alterado. Senhas inicialmente serão criadas pelo responsável técnico da área de informática e posteriormente alterada pelo usuário/funcionário.

b) No caso de aplicação de privilégios de usuários:

- Administrador (Adiciona e remove usuários, programas e privilégios, controle total, leitura e gravação);
- Gestor (Adiciona e remove programas, Controle total, leitura e gravação)
- Usuário (Somente acesso, leitura e gravação).
- Visitante (Somente acesso à internet).

c) Privilégios e Usuários poderão ser alterados conforme demanda do IPRESBS ou solicitação do Conselho de Segurança da Informação.

II – Para acesso a rede o IPRESBS utilizará de Serviços de DNS e DHCP em servidor interno assim com servidor de Proxy e Firewall para a identificação de usuários, restrição e histórico de navegação.

a) O usuário será identificado pelo nome, vinculado a um servidor do IPRESBS, uma senha será criada pelo responsável técnico da área de informática competente e posteriormente alterada pelo usuário;

b) A identificação de usuário e senha do proxy de rede é individual e intransferível;

c) A responsabilidade pela utilização da rede e histórico de navegação que está vinculada ao usuário e é de total responsabilidade do mesmo;

d) O IPRESBS poderá monitorar o comportamento de rede do usuário para garantir o atendimento das diretrizes desta Política de Segurança da Informação ou quanto solicitado pelo Conselho de Segurança da Informação;

e) O IPRESBS poderá realizar bloqueios de usuários e acesso a sites de acordo com as normas desta PSI, solicitação do CSI e ou demandas do instituto.

III – Sistemas:

a) A identificação de usuário e senha de acesso são intransferíveis e de responsabilidade do Usuário titular.

b) Em caso de dificuldade no acesso ou esquecimento dos dados de acesso o responsável técnico da área de informática poderá ser consultado.

c) Todo usuário de acesso deve estar vinculado a uma pessoa física, sendo este funcionário ou manter vínculo com o IPRESBS.

Art. 14°. Para garantir o atendimento das normativas desta resolução, quanto a gravação, armazenamento, disponibilidade e segurança da informação o IPRESBS adotará medidas que assegurem a segurança no armazenamento ou descarte de unidades de memória e documentos impressos.

I – Unidades de armazenamento:

a) Se enquadram como unidades de armazenamento:

- Pen Drive;
- Cartão de memória;
- Disco rígido;
- CD;

- DVD;
- Disquetes;
- Dispositivos eletrônicos com capacidade de armazenamento de dados.

b) Serão mantidos o armazenamento e o backup de dados enquanto houver o interesse do IPRESBS e obrigações legais sobres estes dados.

c) O backup será realizado em unidade de armazenamento distinta, de igual tamanho ou superior e armazenado nas dependências do IPRESBS ou em local indicado pela diretoria do IPRESBS.

d) O Backup dos bancos de dados e informações contidas ou acessadas através da rede mundial de computadores, serão armazenados e mantidos pela empresa contratada, fornecedora do serviço, garantindo o acesso e o armazenamento de dados dentro das normas de segurança estabelecidas em contrato e respeitando as normativas estabelecidas nesta Política de Segurança da Informação.

e) O descarte de unidades de memória e armazenamento será realizado mediante a autorização da diretoria do IPRESBS e a inutilização da capacidade de armazenamento, gravação e leitura das unidades de memória.

f) Sempre que necessária a inutilização de unidades de armazenamento, será solicitada a autorização da diretoria do IPRESBS.

g) O IPRESBS usará de meios cabíveis e adequados para garantir a segurança das informações gravadas em unidades de armazenamento, assim como no descarte destas unidades, visando atendimento das diretrizes dispostas nesta Política de Segurança da Informação.

II – Mídias impressas:

a) Serão consideradas mídias impressas os documentos impressos ou copiados nas dependências do IPRESBS ou de responsabilidade deste.

b) As cópias e impressões serão mantidas e armazenadas enquanto houver interesse ou obrigações legais do IPRESBS quanto a estes materiais.

c) O descarte será realizado somente após a inutilização da impressão através de processo de fragmentação do papel em equipamento específico.

d) O IPRESBS usará de meios cabíveis e adequados para garantir a segurança da informação em seu arquivo físico, assim como no descarte de

arquivos impressos, visando atendimento das diretrizes dispostas nesta Política de Segurança da Informação.

Art. 15°. O IPRESBS realizará, sempre que julgar necessário, ações preventivas e educativas visando garantir a aplicação da Política de Segurança da Informação.

1ª Versão. São Bento do Sul, 21/02/2020, Documento aprovado pelo Conselho Deliberativo em 18/02/2020, publicado no DOM em 21/02/2020 através da portaria 001/2020 IPRESBS.

ANEXO I – TERMO DE COMPROMISSO

Este termo de compromisso aplica-se a todos os usuários de ativos de tecnologia da informação do INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES PÚBLICOS DO MUNICÍPIO DE SÃO BENTO DO SUL – IPRESBS.

Termo de Compromisso: Declaro que li e estou de acordo com a Política de Segurança da Informação do IPRESBS tendo ciência de todo o seu conteúdo. Declaro, ainda, estar ciente de que incidentes contrários à política de segurança resultarão em medidas que poderão inclusive sujeitar abertura de processo administrativo, à quebra de contrato, aos processos judiciais ou a outras medidas pertinentes. Comprometo-me a preservar a integridade, a disponibilidade e a confidencialidade das informações obtidas durante a vigência do contrato ou vínculo com o IPRESBS, mesmo após o seu encerramento. Em sendo prestador de serviço terceirizado comprometo-me igualmente no cumprimento das regras e diretrizes previstas nesta Política.

PREENCHIMENTO SE FUNCIONÁRIO:

Nome:_____

CPF: _____

R.G:_____ Unidade: _____

Tel./Ramal:_____

PREENCHIMENTO SE PRESTADOR DE SERVIÇOS

Nome:_____

CPF:_____Unidade/Depto:_____

Empresa:_____

Telefone Com: ( ) _____

E-mail:_____

Início e Término do Contrato: De _____/_____/_____ a_____/_____/_____

São Bento do Sul – SC,

Data:_____/_____/_____

Assinatura:_____