BOTUPREV
REGIME PRÓPRIO DE PREVIDÊNCIA SOCIAL
BOTUCATU

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI

Institui a Política de Segurança da Informação - PSI do INSTITUTO DE PREVIDÊNCIA SOCIAL DOS SERVIDORES DE BOTUCATU - BOTUPREV, e dá outras providências.

1. INTRODUÇÃO

A Política de Segurança da Informação, ou simplesmente "PSI" é um documento que orienta e estabelece as diretrizes corporativas do BOTUPREV para a proteção dos ativos de informação e prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas.

A presente Política de Segurança da Informação está baseada nas recomendações da norma ABNT NBR ISO/IEC 27005:2008, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

A informação é um ativo de grande valor para a BOTUPREV, por isso, necessita ser adequadamente protegida.

2. OBJETIVOS

Estabelecer diretrizes que permitam aos servidores, fornecedores e prestadores de serviços do BOTUPREV seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades operacionais e de proteção legal da instituição e do indivíduo.

Garantir que os recursos computacionais e serviços de Tecnologia da Informação - TI serão utilizados de maneira adequada. O usuário deve conhecer as regras para utilização da informação de maneira segura, evitando exposição que possa prejudicar o BOTUPREV, colaboradores e terceiros.

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento. Deve implementar controles para preservar os interesses do BOTUPREV contra danos que possam ser consideradas como violação ao uso dos serviços e, portanto, considerados proibidos.

Preservar as informações do BOTUPREV quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Caso os procedimentos ou normas aqui estabelecidos sejam violados por usuários, a Diretoria Administrativa informará aos órgãos competentes de forma que sejam tomadas medidas cabíveis.

Para efeito do disposto nesta Política de Segurança da Informação, consideram-se:

- Usuário: pessoa expressamente autorizada a operar equipamentos de informática do BOTUPREV, em conformidade com as diretrizes institucionais.
- Equipamento de informática e comunicação: dispositivo eletrônico de processamento de informações, incluindo desktop, notebook, tablet, servidor de rede, impressora, scanner, switches, roteadores, smartphones, telefones fixos, e sistemas PABX, bem como seus componentes e acessórios.
- Dispositivos externos de dados: equipamentos destinados ao intercâmbio de dados com equipamentos de informática, tais como pendrives, cartões de memória, HDs e SSDs externos, smartphones, leitores e gravadores de CD/DVD, tablets, entre outros com funcionalidade semelhante.
- Infraestrutura de Rede: conjunto de equipamentos de informática interconectados nas instalações do BOTUPREV, formando uma rede local.
- Login: Processo de autenticação, exclusivo e pessoal, para acesso a sistemas informatizados restritos, realizado mediante credenciais registradas previamente.
- Arquivo: conjunto estruturado de informações armazenável em meio digital.
- Assinatura Digital: tecnologia de autenticação de documentos eletrônicos, como arquivos em PDF, por meio de chaves criptográficas associadas a um certificado digital, conferindo validade jurídica conforme o artigo 7º da Lei Federal nº 14.129/2021. Aplica-se a contratos, procurações, atestados e outros documentos, assim como, transações eletrônicas.
- Área de Trabalho: espaço lógico na rede local ou em discos locais da estação de trabalho reservado para armazenamento exclusivo de arquivos sujeitos a cópia de segurança (backup).
- Software: conjunto de instruções lógicas, codificadas em linguagem específica, para execução em equipamentos de informática e comunicação, incluindo softwares não autorizados pela equipe de Tecnologia da Informação do BOTUPREV, conhecidos como piratas.
- Sistemas Corporativos: sistemas de uso coletivo e finalidades institucionais do BOTUPREV.
- Programa de Código Malicioso: software criado com o objetivo de comprometer a segurança de equipamentos de informática, explorando vulnerabilidades, como malwares, spywares, vírus, entre outros.
- Acesso Remoto: conexão estabelecida por software específico para manutenção de sistemas ou trabalho remoto (Home Office).
- Log de dados: registro de eventos relevantes em sistemas computacionais, usado para restaurar configurações originais, auditorias e diagnósticos de problemas.
- Portal (Site ou Sítio): conjunto integrado de informações, identificado por um domínio, acessível via Internet.
- Comunicadores Instantâneos: programas para troca de mensagens e arquivos em tempo real, incluindo comunicação por texto, voz ou vídeo, como WhatsApp, Spark, entre outros.
- Correio Eletrônico (e-mail): serviço de troca de mensagens digitais. O *e-mail corporativo* é fornecido ao usuário para assuntos institucionais, podendo ser monitorado. O *e-mail particular*

é criado e acessado exclusivamente pelo próprio usuário, e possui restrição de seu uso no ambiente corporativo.

- Redes Sociais (Facebook, Instagram ou quaisquer outras destinados a esses fins): plataformas virtuais de interação e compartilhamento de conteúdo. *Perfis corporativos e páginas corporativas* são destinados a assuntos institucionais, podendo ser monitorados.
- Intranet: rede local interna do BOTUPREV, conectando equipamentos e sistemas de informática.
- Internet: rede global de computadores, externa ao BOTUPREV.
- Rede de Conexão Wifi: rede de acesso à Internet mediante autenticação, temporariamente disponibilizada para segurados e fornecedores nas dependências do BOTUPREV.

3. APLICAÇÕES

As diretrizes estabelecidas deverão ser seguidas por todos os servidores, bem como os fornecedores e prestadores de serviço que se aplicam à informação em qualquer meio ou suporte.

Consideram-se usuários dos recursos de Tecnologia da Informação do BOTUPREV todas as pessoas que, independentemente de serem servidores do instituto, mantenham qualquer vínculo formal com a administração. A autorização de uso é pessoal, exclusiva e intransferível, responsabilizando-se cada usuário pelas atividades realizadas com seu login. Cabe ao usuário a obrigação de preservar a confidencialidade de sua senha, sendo passível de sanções administrativas e legais em caso de mau uso.

Esta política dá ciência a cada servidor, fornecedor e prestador de serviços de que os ambientes, sistemas, computadores e redes poderão ser monitorados e gravados, conforme previsto nas leis brasileiras.

É também obrigação de cada servidor se manter atualizado em relação a esta política e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da área de tecnologia de informação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Qualquer exceção às diretrizes desta política deve ser expressamente formalizada e registrada entre as partes. Os equipamentos de informática e comunicação, bem como os sistemas e informações do BOTUPREV, são disponibilizados exclusivamente para o exercício das atividades profissionais de seus usuários. O uso pessoal desses recursos é permitido apenas de forma restrita e dentro de limites razoáveis, desde que não comprometa a eficiência dos sistemas e a continuidade dos serviços institucionais.

Toda informação produzida ou recebida pelos servidores como resultado da atividade profissional contratada pelo BOTUPREV pertence ao referido instituto.

O BOTUPREV, por meio de sua equipe de Tecnologia da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

4. DAS RESPONSABILIDADES ESPECÍFICAS

DOS SERVIDORES E FORNECEDORES EM GERAL

Entende-se por servidor toda e qualquer pessoa física, nomeada por concurso público que exerça alguma atividade dentro ou fora da instituição.

Entende-se por fornecedor o prestador de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Compete ao usuário:

- Zelar pela confidencialidade de sua senha de acesso, abstendo-se de anotá-la ou deixá-la visível a terceiros;
- Zelar pela segurança das informações, bloqueando ou fechando as telas de equipamentos de informática e softwares ao deixá-los desassistidos, evitando acessos não autorizados.;
- Informar imediatamente à equipe de Tecnologia da Informação sobre qualquer suspeita de ações realizadas em seu nome;
- Evitar o uso de dispositivos que possam conter programas maliciosos (código malicioso), que comprometam a integridade dos recursos institucionais;
- Manter-se atento a tentativas de manipulação por terceiros visando a obtenção de informações para acessos não autorizados, e observar rigorosamente a Lei Geral de Proteção de Dados Pessoais (LGPD) em operações de transferência de dados;
- Submeter exclusivamente à equipe de Tecnologia da Informação quaisquer dúvidas de ordem técnica relativas aos recursos de tecnologia da informação e comunicação; e
- Informar à equipe de Tecnologia da Informação, com antecedência mínima de 10 (dez) dias, qualquer mudança de localização que envolva adaptações técnicas nos recursos de Tecnologia da Informação e Comunicação.

Configura uso inadequado dos recursos de Tecnologia da Informação do BOTUPREV:

- Fornecer, por qualquer razão, seu login e senha de acesso a terceiros ou utilizar as credenciais de outro usuário;
- Utilizar arquivos ou softwares que infrinjam direitos autorais, de propriedade intelectual ou outras proteções legais;
- Incluir ou executar programas maliciosos em equipamentos de propriedade ou responsabilidade do BOTUPREV, incluindo dispositivos locados;
- Empregar hardware ou software para desativar ou burlar os sistemas de segurança da informação do BOTUPREV.

Cada usuário será plenamente responsável por qualquer prejuízo ou dano causado ao BOTUPREV ou a terceiros devido à inobservância das diretrizes e normas estabelecidas nesta política.

DOS SERVIDORES EM REGIME DE EXCEÇÃO (TEMPORÁRIOS E ESTAGIÁRIOS):

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto na Política de Segurança de Informações - PSI.

A concessão de acesso poderá ser revogada a qualquer tempo se for verificado que a motivação de sua concessão não mais compensa o risco em mantê-lo, ou se o usuário que o recebeu não estiver cumprindo as condições definidas nesta política.

DOS GESTORES DE PESSOAS E/OU PROCESSOS:

Adotar e manter uma postura exemplar em relação à segurança da informação, servindo de modelo de conduta para os servidores sob sua gestão e reforçando a cultura de segurança institucional.

Estabelecer, durante a fase de contratação e formalização de contratos individuais de trabalho com servidores, prestadores de serviços ou parceiros, a responsabilidade pelo cumprimento integral da Política de Segurança da Informação do BOTUPREV.

Exigir que todos os servidores assinem o Termo de Compromisso e Ciência, assumindo o compromisso de observar as normas estabelecidas e mantendo o sigilo e a confidencialidade dos ativos informacionais do BOTUPREV, inclusive após o desligamento.

Assegurar, de forma célere, mediante solicitação formal à equipe de Tecnologia da Informação, o bloqueio imediato dos acessos de usuários em casos de afastamento definitivo de servidores e estagiários, incidentes, investigações ou quaisquer outras situações que demandem restrições de acesso para a proteção dos ativos do BOTUPREV.

Garantir que as normas, processos, procedimentos e sistemas sob sua responsabilidade estejam em conformidade com esta Política de Segurança da Informação, realizando adaptações necessárias para assegurar sua efetiva implementação.

DA EQUIPE DE TECNOLOGIA DA INFORMAÇÃO:

Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Configurar os equipamentos, ferramentas e sistemas concedidos aos servidores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta Política de Segurança da Informação.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários.

Segregar as funções administrativas e operacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o BOTUPREV.

Quando ocorrer movimentação interna dos ativos de Tecnologia da Informação, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas do BOTUPREV.

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, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário;

- os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Promover a conscientização dos servidores em relação à relevância da segurança da informação para as atividades precípuas do BOTUPREV.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

5. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política de Segurança da Informação - PSI, o BOTUPREV, por meio de sua equipe de Tecnologia da Informação, poderá:

- 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 que a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;

- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial ou solicitação dos gestores;

- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;

- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança da informação e dos perímetros de acesso.

CONTROLE DO USO DE E-MAIL:

O objetivo é informar aos servidores do BOTUPREV quais são as atividades permitidas e proibidas quanto ao uso do e-mail corporativo.

A responsabilidade pelo uso do e-mail corporativo do BOTUPREV é atribuída objetivamente a cada usuário que dele faça uso, cabendo a cada membro responder integralmente pelas ações realizadas a partir de sua conta de e-mail institucional.

O e-mail corporativo do BOTUPREV deve ser utilizado exclusivamente para fins institucionais, relacionados às atividades e aos interesses da instituição.

O uso de serviços de e-mail pessoais para fins particulares é restritivamente permitido, desde que realizado com bom senso, sem prejudicar as operações do BOTUPREV nem impactar o desempenho e o tráfego da rede.

É vedado aos servidores o uso do e-mail institucional do BOTUPREV para:

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;

- enviar mensagem por e-mail pelo endereço de seu departamento, usando o nome de usuário de outra pessoa, ou endereço de correio eletrônico que não esteja autorizado a utilizar;

- enviar qualquer mensagem por meios eletrônicos que torne seu remetente ou o BOTUPREV vulneráveis a ações civis ou criminais;

- divulgação não autorizada de informações, capturas de tela e sistemas, documentos ou quaisquer ativos de informação sem a devida solicitação do legítimo detentor do referido ativo, ou seu representante legal. A disponibilização de tais documentos, deve ser requerida preferencialmente por meio das plataformas oficiais do site do BOTUPREV. Também é permitido em caso de cumprimento de obrigações legais ou regulamentares, sempre garantindo a proteção dos direitos do titular dos dados.

- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- apagar mensagens pertinentes de correio eletrônico quando o BOTUPREV estiver sujeito a algum tipo de investigação;

- realizar cadastros pessoais, incluindo em redes sociais ou outras plataformas, exceto quando estritamente necessário para finalidades profissionais e vinculado diretamente às atividades institucionais do BOTUPREV;

- produzir, transmitir ou divulgar mensagem que:
    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do BOTUPREV;

    - contenha ameaças eletrônicas, como: spam, mail *bombing*, vírus, etc.;

    - contenha arquivos com código executável (exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;

    - vise obter acesso não autorizado a outro computador, servidor ou rede;

    - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- vise burlar qualquer sistema de segurança;
- vise vigiar secretamente ou assediar outro usuário;
- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- contenha anexo(s) superior(es) a 25 MB para envio (interno e internet) e 25 MB para recebimento (internet), exceto com autorização prévia do gestor da área;
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental, ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);
- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

CONTROLE DO USO DE INTERNET:

Todas as regras atuais do BOTUPREV visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o BOTUPREV, em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O BOTUPREV, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer servidor, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas

poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

O uso de sites de notícias ou serviços na internet é considerado aceitável, desde que não comprometa a largura de banda da rede, não interfira no desempenho das atividades institucionais, e não implique conflitos de interesse com os objetivos do BOTUPREV.

Somente servidores expressamente autorizados podem se manifestar publicamente em nome do BOTUPREV em qualquer meio de comunicação, seja por e-mail, entrevista online, podcast, redes sociais, ou por documentos físicos.

Apenas os servidores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos, redes sociais ou qualquer outra tecnologia correlata que venha surgir na internet.

Servidores com acesso à internet estão proibidos de realizar o download de qualquer programa, mesmo que relacionado às atividades institucionais, sem prévia comunicação à equipe de Tecnologia da Informação, por e-mail institucional, e sua autorização formal. Cabe ao servidor responsável pelo download garantir a regularização de licenças e registros dos programas necessários.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela área de tecnologia de informação.

Os servidores não poderão em hipótese alguma utilizar os recursos do BOTUPREV para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Servidores com acesso à internet não poderão efetuar upload de qualquer software licenciado ao BOTUPREV, ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os servidores não poderão utilizar os recursos do BOTUPREV para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares *peer-to-peer* (Kazaa, BitTorrent e afins) não serão permitidos.

Serviços de streaming (como rádios online e canais de broadcast) e de comunicação instantânea (como Skype, WhatsApp e redes sociais) poderão ser acessados pelos servidores. No entanto, esses serviços poderão ser bloqueados a critério do gestor de cada setor ou da equipe de Tecnologia da Informação, especialmente em casos de uso indevido.

Não é permitido acesso a sites de proxy.

É estritamente proibido a qualquer usuário o acesso a sites de jogos online e sites de apostas, em qualquer dispositivo conectado à rede interna do BOTUPREV.

O uso de ferramentas de inteligência artificial, especialmente as generativas, é permitido de forma restrita, sendo o usuário integralmente responsável por garantir o cumprimento dos direitos de licença dessas ferramentas e garantir que o conteúdo gerado não viole a legislação vigente.

CONTROLE DE ACESSO À INFORMAÇÃO SENSÍVEL DE MEIO FÍSICO:

O objetivo é prevenir o acesso não autorizado as informações sensíveis de meio físico de posse e competência do BOTUPREV, evitando danos e interferências.

O acesso à área em que são processadas e armazenadas as informações sensíveis de meio físico são controlados e restrito às pessoas autorizadas. O acesso não autorizado não será permitido.

O controle de retirada e/ou consulta das informações será controlado por responsável designado que fará monitoramento por meio de emissão de protocolos. As informações contidas no protocolo contam com no mínimo:

- nome e visto do servidor responsável emissor do protocolo;
- nome e visto do servidor interessado ao acesso da informação sensível de meio físico;
- a data e hora da retirada e/ou consulta da informação sensível de meio físico;
- a data e hora da devolução da informação sensível de meio físico e
- observações complementares.

A retirada de informações sensíveis de meio físico sem a devida emissão do protocolo não será autorizada.

Toda a informação sensível de meio físico será conferida no ato da devolução, estando sujeito a emissão de ocorrências em caso de desorganização, desleixo ou ausência de documentos.

São considerados os casos de desorganização e desleixo:

- Desordem na numeração das folhas do processo;
- Rasuras, anotações e amassados;
- Sujeiras de alimentos e bebidas.

Não é permitido a retirada de qualquer folha objeto de complemento ao arquivo de informação.

A possibilidade de fotocópia será permitida somente com a emissão do protocolo, onde deverá ser preenchido no item “Observações Complementares” as folhas que foram objeto da fotocópia.

Não é permitido a locomoção de informações sensíveis de meio físico fora as dependências do BOTUPREV.

6. IDENTIFICAÇÃO:

Os dispositivos de identificação e senhas protegem a identidade do servidor usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o BOTUPREV e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307–falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os servidores.

Todos os dispositivos de identificação utilizados no BOTUPREV, como o número de registro do colaborador, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos devem estar associados a uma única pessoa física.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal). Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o BOTUPREV e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

A equipe de Tecnologia da Informação responde pela criação da identidade lógica dos servidores na instituição.

Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser registradas ou armazenadas em arquivos eletrônicos (como editores de texto ou planilhas) em formato legível ou acessível por linguagem humana, ou seja, sem o uso de criptografia adequada.

Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Caso o servidor esqueça sua senha, ele deverá requisitar formalmente a troca, ou comparecer à área técnica responsável para cadastrar uma nova.

7. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos de informática fornecidos pelo BOTUPREV aos seus servidores, são bens da instituição e devem ser utilizados exclusivamente para o desempenho das atividades laborais. O usuário deverá utilizar os equipamentos e sistemas de informação de forma cuidadosa e responsável, observando as normas e procedimentos internos estabelecidos pelo BOTUPREV.

A fim de garantir a segurança das informações e o bom funcionamento dos sistemas, o BOTUPREV poderá realizar, a qualquer tempo, inspeções nos equipamentos e sistemas. Inspeções mais detalhadas, como a análise de logs de acesso ou a busca por arquivos específicos, poderão ser realizadas mediante autorização expressa do Superintendente ou de outro gestor designado, em caso de suspeita de uso indevido ou de ocorrência de incidentes de segurança.

O usuário que utilizar indevidamente os equipamentos e sistemas de informação estará sujeito às penalidades previstas na legislação vigente e nas normas internas do BOTUPREV.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um servidor da equipe de Tecnologia da Informação, ou de quem este determinar.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes às atividades do BOTUPREV não deverão ser copiados movidos para os drives de rede, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente sem comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos servidores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os servidores do BOTUPREV e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da equipe de Tecnologia da Informação.

No uso dos computadores, equipamentos e recursos de informática, devem ser observadas as seguintes normas:

- Os servidores devem informar qualquer identificação de dispositivo estranho conectado ao seu computador;

- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado pela equipe de Tecnologia da Informação, ou por terceiros devidamente contratados para o serviço;

- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores e da equipe de Tecnologia da Informação;

- O usuário deve manter a configuração original do equipamento fornecido pelo BOTUPREV, atendendo rigorosamente aos controles de segurança exigidos pela Política de Segurança da

Informação e pelas normas institucionais específicas, sendo responsável pela guarda e integridade das informações sob sua responsabilidade;

- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados;

- Todos os recursos tecnológicos adquiridos pelo BOTUPREV devem ter imediatamente suas senhas padrões alteradas.

Situações em que é proibido o uso de computadores e recursos tecnológicos do BOTUPREV:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;

- Burlar quaisquer sistemas de segurança;

- Acessar informações confidenciais sem explícita autorização do proprietário;

- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers);

- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública;

- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

8. PRIVACIDADE DA INFORMAÇÃO

Define-se como necessária a proteção da privacidade das informações, aquelas que pertencem aos seus segurados e/ou beneficiários e que são manipuladas ou armazenadas nos meios às quais o BOTUPREV detém total controle administrativo, físico, lógico e legal.

As diretrizes a seguir refletem os valores institucionais do BOTUPREV, reafirmando o compromisso com a melhoria contínua das práticas de proteção e segurança da informação:

- Toda operação de coleta de dados - incluindo a inclusão, modificação, exclusão e transferência, tanto em formato físico quanto digital - deve observar os preceitos da Lei Federal nº13.709/2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), complementada pelo Decreto Municipal nº 12.462/2021, assegurando a conformidade legal e a proteção dos titulares de dados;

- As informações são coletadas de maneira ética e em conformidade com a legislação, com o pleno conhecimento do segurado ou beneficiário. A finalidade de uso é especificada de forma clara e informada previamente ao titular;

- O acesso às informações é estritamente limitado a colaboradores ou terceiros expressamente autorizados, capacitados e habilitados, garantindo o uso adequado e seguro dos dados;

- Quando necessário, as informações podem ser compartilhadas com empresas contratadas para prestação de serviços específicos ao BOTUPREV, sendo obrigatória a conformidade dessas organizações com as diretrizes de segurança e privacidade de dados estabelecidas pela nossa política;

- O fornecimento de dados a terceiros ocorre exclusivamente mediante autorização expressa da Superintendência, condicionada à apresentação de requerimento formal, preferencialmente por meio das plataformas online oficiais do site do BOTUPREV ou presencialmente. Também é permitido em caso de cumprimento de obrigações legais ou regulamentares, sempre garantindo a proteção dos direitos do titular dos dados;

- Informações e dados contidos nos cadastros do BOTUPREV, bem como outras solicitações de cunho legal, serão disponibilizados somente ao próprio interessado, ou seu representante legal. O acesso somente será concedido mediante à apresentação de requerimento formal, preferencialmente por meio das plataformas online oficiais do site do BOTUPREV ou presencialmente, e em conformidade com os requisitos legais vigentes.

9. DISPOSITIVOS MÓVEIS

Visando facilitar a mobilidade e o acesso às informações, o BOTUPREV poderá fornecer dispositivo móvel aos seus servidores, para utilização em casos específicos.

Quando se descreve “dispositivo móvel” entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido pela área de tecnologia de informação, como: notebooks, smartphones e pendrives.

O objetivo é estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os servidores que utilizem tais equipamentos.

O BOTUPREV, na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

O servidor, portanto, assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no BOTUPREV, mesmo depois de terminado o vínculo contratual mantido com a instituição.

Todo servidor deverá realizar periodicamente cópia de segurança (backup) dos dados de seu dispositivo móvel. Deverá, também, manter estes backups separados de seu dispositivo móvel, ou seja, não os carregar juntos.

Em caso de necessidade de suporte técnico para dispositivos móveis de propriedade do BOTUPREV e aos seus usuários, primeiramente deverá ser comunicado a equipe de Tecnologia da Informação, que fará o possível para atender à solicitação no menor prazo possível, priorizando as demandas que impactem diretamente nas atividades laborais.

Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação, autorização e sem a condução, auxílio ou presença de um servidor da equipe de Tecnologia da Informação.

O servidor deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela equipe de Tecnologia da Informação.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante. É permitido o uso de rede banda larga de locais conhecidos pelo usuário como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do servidor, no caso de furto ou roubo de um dispositivo móvel fornecido pelo BOTUPREV, notificar imediatamente o seu gestor e a equipe de Tecnologia da Informação.

O servidor deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao BOTUPREV e/ou a terceiros.

10. DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema de fonte de autenticação. Por exemplo: tranca, cadeado, fechadura eletrônica, biometria, cartão magnético, entre outros.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um servidor da equipe de Tecnologia da Informação, ou de um servidor autorizado.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Serviços Gerais.

Não é permitida a entrada de nenhum alimento, bebida, produto fumígeno ou inflamável.

A temperatura, umidade e ventilação das instalações que abrigam equipamentos de informática e de comunicações, devem estar de acordo com os padrões técnicos especificados pelos fabricantes dos equipamentos.

No caso de perdas de chaves de departamentos, ou laboratórios, o gestor responsável deve ser informado imediatamente para que possa providenciar a troca das fechaduras.

11. PROCEDIMENTOS DE BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento para que sejam preferencialmente executados fora do horário comercial, nas chamadas “janelas de backup”, períodos em que não há pouco ou nenhum acesso de usuários, ou processos automatizados aos sistemas de informática.

Os servidores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência em etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do uso recomendado pelo fabricante.

A restauração de backups deve ser realizada conforme a política de retenção de dados e a criticidade das informações. Os procedimentos para restauração de backups devem ser seguidos rigorosamente, a fim de garantir a integridade e a disponibilidade dos dados.

A frequência de restauração de backups varia de acordo com a criticidade das informações e a política de retenção de dados estabelecida pela organização. Os testes de restauração serão realizados periodicamente, conforme cronograma da equipe de Tecnologia da Informação, especialmente para dados críticos, a fim de verificar a eficácia dos procedimentos e identificar possíveis problemas.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas mediante justificativa de necessidade.

Os arquivos de backup devem estar disponíveis em servidores externos de arquivo, como segunda fonte.

12. VIOLAÇÃO DA POLÍTICA, ADVERTÊNCIA E PUNIÇÕES

Ao detectar uma violação da política, a primeira coisa a fazer é determinar a sua razão, ou seja, verificar se a violação ocorreu por negligência, acidente, erro ou por desconhecimento da política vigente.

Nos termos da Política de Segurança da Informação, a Diretoria Administrativa procederá ao bloqueio do acesso ou ao cancelamento do usuário, caso seja detectado uso indevido com o intuito de prejudicar o andamento do trabalho ou pôr em risco a imagem da instituição.

É recomendado o treinamento dos usuários em Segurança da Informação, por meio de cartilhas, com o intuito de divulgar e conscientizar os funcionários e demais colaboradores sobre a Política de Segurança da Informação a ser seguida por todos. O programa de treinamento em segurança deve fazer parte do programa de integração de novos usuários. Os treinamentos de reciclagem devem ser previstos quando necessários.

Caso seja necessário advertir o usuário pelo não cumprimento das normas estabelecidas neste documento, devem ser informados o superior imediato e o departamento de Recursos Humanos para interagir e manterem-se informados da situação.

Conforme previsto no Estatuto dos Servidores Públicos de Botucatu, o funcionário colaborador poderá ser aplicado a penalidade no caso de irregularidade comprovada.

De acordo com a infração cometida, as seguintes punições serão: comunicação de descumprimento, advertência ou suspensão e demissão por justa causa.

Fica desde já estabelecido que não há progressividade como requisito para a configuração da dispensa por justa causa, podendo a Diretoria, no uso do poder diretivo e disciplinar que lhe é atribuído, aplicar a pena que entender devida quando tipificada a falta grave.

13. DAS DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do BOTUPREV. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes.

A elaboração desta Política é de responsabilidade da Diretoria Administrativa, devendo sua revisão ocorrer anualmente e ser submetida para aprovação ao órgão superior competente.

As normas aqui estabelecidas poderão ser modificadas sempre que necessário, sendo tais alterações registradas pela Diretoria Administrativa, aprovadas pelo órgão superior competente, e comunicadas pela própria Diretoria no âmbito da estrutura organizacional do BOTUPREV, considerando o tempo necessário para a implementação de eventuais medidas.

Casos omissos ou excepcionais a esta Política de Segurança da Informação deverão ser encaminhados para análise e parecer da Superintendência, que poderá se apoiar em informações fornecidas pela equipe de Tecnologia da Informação.

14. TERMO DE CIÊNCIA E CONHECIMENTO

TERMO DE CIÊNCIA E CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI DO BOTUPREV

Declaro que recebi a Política de Segurança da Informação - PSI do BOTUPREV, estando ciente de seu conteúdo e da sua importância para o bom exercício funcional do próprio BOTUPREV.

A assinatura do presente Termo, anexo a referida Política de Segurança da Informação, é manifestação de minha concordância e do meu compromisso em cumpri-lo integralmente.

Walner Clayton Rodrigues

Superintendente

Revisão do texto realizada em 26 de novembro de 2024.