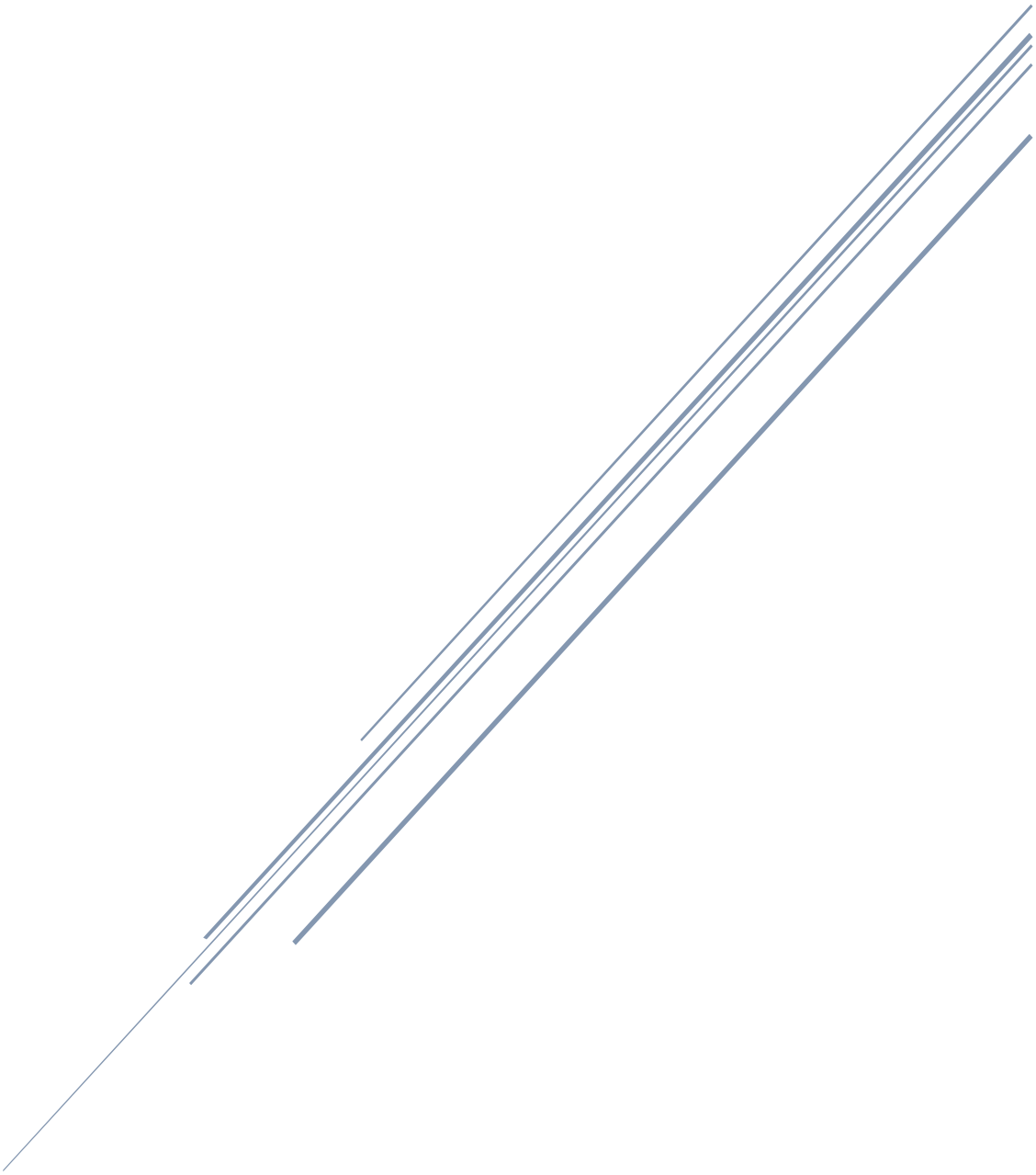
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

Fundo de Previdência social de Barra Mansa – PREVIBAM.



Política de Segurança da Informação – PSI

As políticas, normas e procedimentos que buscam garantir a segurança da informação devem ser prioridades constantes do Fundo de Previdência Social de Barra Mansa – PREVIBAM.

Assim, com o intuito de reduzir os riscos de falhas, danos e prejuízos que venham a comprometer a imagem e os objetivos do fundo previdenciário.

A Política de Segurança da Informação, apresenta as diretrizes, os limites e o direcionamento que a PREVIBAM deseja para os controles que serão implantados na proteção de suas informações e responsabilidades legais para todos os servidores, usuários e terceiros que prestem serviços ao fundo previdenciário, devendo ser cumprida e aplicada em todas as áreas do Instituto.

OBJETIVOS

A presente política visa estabelecer e definir as normas, processos, procedimentos e controles específicos de segurança da informação, a fim de preservar as informações quanto à:

Confidencialidade: toda informação, até que se torne pública, deve ser acessada somente por quem de direito e deve assegurar-se que informações confidenciais e críticas não sejam subtraídas dos sistemas organizacionais da PREVIBAM, entre outras práticas: por meio de ciberataques, espionagem, etc.

Integridade: preservação da precisão, consistência e confiabilidade das informações e sistemas.

Disponibilidade: Garantia de acesso à informação durante o ciclo de sua existência.

Conformidade: Toda informação deve estar em conformidade com os padrões, regras e, especialmente, com a legislação vigente.

ABRANGÊNCIA

A Política de segurança da informação, na PREVIBAM, aplica-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento do fundo previdenciário ou acesso a informações pertencentes ao PREVIBAM. Todo e qualquer usuário de sistemas e recursos computadorizados do fundo previdenciário tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

Configura-se como violação desta política de segurança qualquer ato que:

Exponha o Fundo de Previdência Social de Barra Mansa – PREVIBAM a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados e/ou de informações ou ainda cause a dano em sistema ou equipamento.

Envolva a revelação de dados confidenciais, cadastrais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.

Envolva o uso de dados para propósitos estranhos ao objeto do instituto ou ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

DEVERES

1- É DEVER DE TODOS no Fundo de Previdência Social de Barra Mansa – PREVIBAM considerar a informação como sendo um bem da Autarquia, um dos recursos críticos para a realização dos objetivos do fundo previdenciário, que possui grande valor e deve sempre ser tratada profissionalmente, em estrita conformidade com os limites das competências funcionais de cada servidor da PREVIBAM.

2- A CLASSIFICAÇÃO DA INFORMAÇÃO, salvo disposição legal, é de responsabilidade do Diretor/Chefe/Responsável de cada área conforme a previsão estatutária e estes deverão estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias), identificando o que pode ser público ou confidencial.

3- Toda informação decorrente dos objetivos da PREVIBAM e resguardado os direitos de terceiros, deve ser regida pelo princípio da ‘Publicidade’, todavia no

ciclo de sua existência é obrigação do Ente Público tratá-la com sigilo e confidencialidade, segundo a legislação vigente.

4- Nos casos de processos administrativos disciplinares ou sindicâncias, resguardado o direito ao contraditório, que resultem em punições ou mesmo desligamentos, o setor de Recursos Humanos da PREVIBAM comunicará o fato o mais rapidamente possível aos responsáveis e demais prestadores de serviços de sistemas para que o servidor, comissionado ou estagiário afastado/suspenso/exonerado seja bloqueado nos sistemas e acessos que exijam esse procedimento enquanto perdurar a situação.

DADOS DOS FUNCIONÁRIOS

5- A gestão da PREVIBAM não solicitará, acumulará ou manterá intencionalmente dados pessoais de servidores, comissionados e estagiários além daqueles relevantes e exigidos na forma da lei.

6- Os dados pessoais de servidores, comissionados e estagiários não serão transferidos para terceiros, exceto quando exigido pela legislação vigente, necessidade premente decorrente do exercício de suas atribuições ou por determinação judicial, incluindo-se, neste caso a lista de endereços eletrônicos (e-mails) usados pelos funcionários.

EQUIPAMENTOS

7- Os servidores, comissionados e estagiários serão cientificados pela Chefia imediata e por meio de declaração escrita, salvo com prévia e expressa autorização por parte da diretoria do fundo de previdência, deverão se comprometer a não armazenar dados pessoais lícitos nas instalações dos equipamentos de informática da PREVIBAM.

8- Mesmo que seja autorizado o armazenamento destes dados, a PREVIBAM não se responsabiliza por eles, nem tampouco pelo seu conteúdo e pela segurança, devendo permanecer no HD do desktop, tais dados jamais poderão ser armazenados nos diretórios e pastas dos Servidores da PREVIBAM, não podendo fazer parte da rotina de backup.

ADMISSÃO E DEMISSÃO DE SERVIDORES/COMISSIONADOS/ ESTAGIÁRIOS

9- O setor de Recursos Humanos da PREVIBAM informará à área de TI e demais prestadores de serviços de sistemas acerca das admissões de servidores e/ou estagiários, para que os mesmos possam ser cadastrados ou excluídos no sistema da PREVIBAM, inclusive o fornecimento de senha (password) e registro do nome como usuário no sistema.

10- A PREVIBAM, por meio do responsável pela Gestão da Segurança da Informação, comunicará à área de TI e demais prestadores de serviços de sistemas sobre as rotinas e alçadas a que o novo contratado terá direito de acesso. No caso de estagiários informará o tempo em que os mesmos prestarão serviços, para que na data de desligamento possam ser encerradas as atividades relacionadas ao acesso ao sistema.

11- O setor de Recursos Humanos dará conhecimento e obterá as devidas assinaturas de concordância dos novos admitidos em relação à Política de Segurança da Informação da PREVIBAM.

PROGRAMAS ILEGAIS

12- A PREVIBAM respeita os direitos autorais dos programas que usa, sendo vedado o uso de programas não licenciados.

13- Os usuários não podem, salvo autorização da diretoria para programas licenciados, instalar software (programa) nos equipamentos da PREVIBAM. Periodicamente, a área de TI deverá fazer verificações nos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz. Caso sejam encontrados programas não autorizados, a diretoria da PREVIBAM deverá ser notificada para as providências necessárias.

14- Além das medidas administrativas cabíveis, a responsabilidade é pessoal e objetiva para aqueles que instalarem programas não autorizados em seus computadores de trabalho e, respeitado o direito ao contraditório, serão responsabilizados por quaisquer problemas ou prejuízos causados, estando sujeitos às sanções previstas na legislação vigente e especialmente neste documento.

PERMISSÕES E SENHAS

15- Todo usuário para acessar os dados da rede da PREVIBAM, possuirá login e senha previamente cadastrados.

COMPARTILHAMENTO DE DADOS

16- Caso a PREVIBAM opte por hospedar servidores de rede em sua sede, não será permitido o compartilhamento de pastas e arquivos através dos computadores e desktops, todos os dados deverão ser armazenados nos servidores da rede.

17- Os compartilhamentos de impressoras devem estar sujeitos às autorizações de acesso. Não são permitidos na PREVIBAM o compartilhamento de pastas e arquivos na rede através de dispositivos móveis tais como pendrives e outros. A exceção são as disponibilizações de cópias digitais de processos aos seus devidos interessados, antecedidas de requerimento próprio ou em cota no processo, outras destinações para o uso de dispositivos móveis deverão ser precedidas de autorização devidamente justificada e documentada por membro da Diretoria Executivo da PREVIBAM.

CÓPIAS DE SEGURANÇA DE ARQUIVOS EM DESKTOPS

18- A elaboração de cópias de segurança ("backups") de dados e outros arquivos ou documentos desenvolvidos pelos servidores em suas estações de trabalho que não sejam considerados de fundamental importância para a continuidade da operação da PREVIBAM são de responsabilidade dos próprios usuários.

19- No caso das informações consideradas de fundamental importância para a continuidade dos objetivos da PREVIBAM, a Coderp ou Área de TI disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações, mediante análise técnica, econômica e financeira. Estas informações serão incluídas na rotina diária de backup da Informática.

SEGURANÇA E INTEGRIDADE DOS DADOS

20- O gerenciamento do (s) banco (s) de dados administrados pela área de TI e demais prestadores de serviços de sistemas deverão ter segurança e integridade, assim

como a manutenção, alteração e atualização de equipamentos e programas mantidos pelas mesmas.

ACESSO INTERNET

21- Será autorizado para os usuários que necessitarem da mesma para o desempenho das suas atividades profissionais na PREVIBAM. Sites que não contenham informações que agreguem conhecimento profissional e/ou para operação das atividades inerentes às funções não devem ser acessados.

22- Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

De conteúdo pornográfico ou relacionados a sexo;

Que defendam atividades ilegais;

Que menosprezem, depreciem ou incitem ao racismo, ao preconceito e a violência;

Que veiculem ideologias, filosofias e crenças;

Que promovam a participação em salas de discussão de assuntos não relacionados a PREVIBAM;

Que promovam discussão pública sobre assuntos internos da PREVIBAM, a menos que autorizado pela Diretoria.

Que possibilitem a distribuição de informações de nível “Confidencial”.

Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

USO DO CORREIO ELETRÔNICO (E-MAIL)

23- O correio eletrônico fornecido pela PREVIBAM é um instrumento de comunicação interna e externa para a realização das atividades relativas ao fundo previdenciário. As mensagens devem ser escritas em linguagem profissional, não

devem comprometer a imagem da PREVIBAM, não podem ser contrárias à legislação vigente e nem aos princípios éticos da PREVIBAM.

24- O uso do correio eletrônico é de caráter pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

Contenham declarações difamatórias, obscenas e linguagem ofensiva;

Façam apologia a ilícitos, crenças, filosofias e de cunho político-partidária;

Possam trazer prejuízos a outras pessoas;

Sejam hostis e inúteis, considerando a ética e a moral comum aos cidadãos;

Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;

Possam prejudicar a imagem da PREVIBAM;

Possam prejudicar a imagem de outras empresas ou entes públicos;

Sejam incoerentes com as políticas da PREVIBAM.

Para incluir um novo usuário no correio eletrônico, a PREVIBAM encaminhará pedido formal à área de TI, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado.

25- A área de TI poderá, visando evitar a entrada de vírus na PREVIBAM, bloquear o recebimento de e-mails provenientes de sites gratuitos ou mensagens detectadas como SPAM e/ou MALWARE e outras definições para mensagens que possam prejudicar o funcionamento dos sistemas da PREVIBAM.

USO DE NOTEBOOK NA PREVIBAM

26- Os usuários que tiverem direito ao uso de computadores pessoais (notebook), ou qualquer outro equipamento computacional, de propriedade da PREVIBAM devem estar cientes de que:

Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.

Observados todos os protocolos disciplinados nesta PSI, a proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.

É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.

O usuário não deve alterar a configuração do equipamento recebido e não instalar programas para compartilhamento de arquivos;

Em caso de furto, deverá ser registrada a ocorrência em uma delegacia de polícia;

Comunique ao seu superior imediato ou área de TI;

Envie uma cópia da ocorrência para a área de TI.

RESPONSABILIDADE DOS SUPERIORES HIERÁRQUICOS

27- Os diretores, chefes e assessores são responsáveis pelas definições dos direitos de acesso de seus subordinados aos sistemas e informações da PREVIBAM, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política. Será definida a hierarquia necessária para realização desta tarefa em cada setor.

28- A área de TI fará auditorias periódicas do acesso dos usuários às informações, verificando:

Que tipo de informação o usuário pode acessar;

Quem está autorizado a acessar determinada rotina e/ou informação;

Quem autorizou o usuário a ter permissão de acesso à determinada rotina ou informação;

USO DE ANTIVÍRUS

29- Todo arquivo em mídia proveniente de entidade externa a PREVIBAM deve ser verificado por programa antivírus. Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus. Todas as estações de trabalho devem estar protegidas por antivírus.

30- A atualização do antivírus será automática, via rede. O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

PENALIDADES

31- O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar em: advertência formal, suspensão, rescisão do contrato, exoneração, outra ação disciplinar e/ou processo civil ou criminal, nos termos da legislação vigente.

Barra Mansa, 20 de fevereiro de 2024.

DENISE SANTOS GOMES:11008488780

Assinado de forma digital por DENISE SANTOS GOMES:11008488780
Dados: 2025.09.26 11:10:38 -03'00'

Denise Santos Gomes
Presidente do PREVIBAM