Política de Segurança da Informação (PSI)

(Aprovado pela Resolução CONDEL 040/2023, de 29/11/2023)

S U M Á R I O

Política de Segurança da Informação (PSI)

(Aprovado pela Resolução CONDEL 040/2023, de 29/11/2023)

1 INTRODUÇÃO

1.1 Esta norma tem por finalidade atribuir responsabilidades e estabelecer as diretrizes, critérios e regras que devem ser adotadas pela PREVIRB para garantir a segurança das informações institucionais, no que se refere à manipulação de dados e à utilização de recursos computacionais e infraestruturas tecnológicas, especialmente no que tange aos dados pessoais dos Participantes, Assistidos e empregados da Fundação.

2 CONCEITOS:

a) **INFORMAÇÃO** – todo e qualquer conteúdo que tenha valor para a empresa ou pessoa, quer esteja em meio eletrônico, armazenado em recursos computacionais da PREVIRB e trafegando dentro da sua infraestrutura tecnológica, quer esteja em meio físico, em circulação no ambiente institucional da PREVIRB, ou, ainda, repassada através de conversas nos ambientes interno e externo;

b) **SEGURANÇA DA INFORMAÇÃO** – processo de adoção de medidas eficazes para resguardar que as informações institucionais da PREVIRB sejam conhecidas somente por aqueles que devem conhecê-las, evitando seu uso indevido, inadequado, ilegal ou em desconformidade com este Instrumento;

c) **USUÁRIO** – é a identificação pessoal de todos os empregados, dirigentes e membros dos Conselhos e Comitês da Fundação que possuem uma conta de acesso à rede corporativa de computadores e aos recursos computacionais e infraestruturas tecnológicas da PREVIRB;

d) **REDE CORPORATIVA** – conjunto de computadores, aqui denominados estações de trabalho, ligados entre si, com a finalidade de compartilhar dados, aplicativos, recursos tecnológicos e periféricos;

e) **LOGIN** – é a ação necessária para acessar a rede corporativa, mediante a inserção da identificação do usuário e da senha a ela relacionada;

f) ***BACKUP*** (cópia de segurança) – é o ato de copiar dados, de um dispositivo de armazenamento para outro, com o objetivo de recuperar dados, caso existam problemas no futuro;

g) ***DOWNLOAD*** – é o processo de transferir (baixar) um ou mais arquivos de um servidor remoto para um computador local;

h) ***HTTP*** – é um protocolo de comunicação utilizado para transferir dados por intranets e pela internet (*world wide web* – *www*) – significa “Protocolo de Transferência de Hipertexto”;

i) ***HTTPS*** – é uma implementação do protocolo *http* sobre uma camada adicional, que permite que os dados sejam transmitidos através de uma conexão criptografada, em

que se verifique a autenticidade do servidor e do cliente, através de certificados digitais – significa “Protocolo de Transferência Segura de Hipertexto”;

j) **DADO PESSOAL** – informação relacionada à pessoa física identificada ou identificável;

   i. DADO PESSOAL SENSÍVEL – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa física;
   ii. DADO PESSOAL ANONIMIZADO – dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

k) **TITULAR DO DADO PESSOAL** – pessoa física a quem se referem os dados pessoais que são objeto de tratamento, bem como de seus beneficiários e dependentes cadastrados; e

l) **ENCARREGADO (*Data Protection Officer – DPO*)** – pessoa indicada pela Diretoria para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

m) **AGENTES DE TRATAMENTO**:

   i. CONTROLADOR – pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
   ii. OPERADOR – pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;

n) **GESTORES** – pessoas responsáveis por gerir ou administrar equipes, setores e/ou conjunto de atividades;

o) **PARTICIPANTES** – Pessoas vinculadas a Planos de Benefícios da PREVIRB;

p) **PATROCINADORES** – todas as pessoas jurídicas que venham a ser admitidas nesta qualidade, mediante celebração do competente Convênio de Adesão;

q) **TERCEIROS** – estagiários, prestadores de serviços, parceiros comerciais ou qualquer outra pessoa, física ou jurídica, que mantenha relações comerciais com a Fundação.

3 DIRETRIZES

3.1 A segurança da informação caracteriza-se pela preservação da:

a) **CONFIDENCIALIDADE** – garantia de que a informação esteja acessível somente às pessoas autorizadas;
b) **INTEGRIDADE** – garantia de que as informações sejam mantidas íntegras, sem alterações indevidas – intencionais ou não;
c) **DISPONIBILIDADE** – garantia de que apenas os usuários autorizados obtenham acesso à informação sempre que necessário;

d) **AUTENTICIDADE** – garantia de que uma informação provém das fontes anunciadas e que não foi alvo de mutações ao longo de um processo.

3.2 Para assegurar os itens mencionados acima, deve-se gerenciar adequadamente a informação (física, digital ou verbal), sendo protegida contra extravio, acidentes, roubo, fraude, divulgação indevida e outras ameaças.

4 PROPRIEDADE INTELECTUAL

4.1 As informações e os recursos produzidos internamente, a exceção daqueles legalmente protegidos, são de propriedade da PREVIRB, sendo utilizados exclusivamente para atender aos interesses da Fundação e o cumprimento do contrato previdenciário, base legal que autoriza o uso dos dados pessoais dos Participantes e Assistidos pela PREVIRB.

5 CLASSIFICAÇÃO DA INFORMAÇÃO

5.1 É de responsabilidade dos Diretores e Gestores da Fundação definir os níveis de confidencialidade das informações (documentos, relatórios e/ou mídias) geradas por suas áreas, conforme critérios a seguir:

a) **PÚBLICA** – Informação com linguagem e formato próprio à divulgação pública, seja física ou virtual, de caráter informativo ou por exigência legal e destinada aos Participantes e Assistidos ou ao público externo;
b) **RESTRITA** – Informação profissional ou pessoal, de interesse exclusivo dos Patrocinadores, Participantes e Assistidos da Fundação que será feita por meio de Cartas registradas, por meios seguros de trocas de arquivos eletrônicos (p.ex. *FTP*) ou mensagem na área restrita do site;
c) **INTERNA** – Informação para uso interno da Fundação, acessível aos empregados, permanecendo disponíveis na rede ou no site;
d) **CONFIDENCIAL** – Informação crítica para os negócios da Fundação restrita a um grupo específico de pessoas, estando aqui incluídos os dados pessoais sensíveis.

6 REQUISITOS DE ACESSO À REDE CORPORATIVA

6.1 Conta de Usuário

6.1.1 Será atribuída a cada empregado e diretor, pela Gerência de Infraestrutura – GEINF, uma conta de usuário, para acesso (*login*) à rede corporativa, com o nome pelo qual serão identificados no ambiente dos recursos computacionais e infraestruturas tecnológicas.

6.1.2 O usuário é responsável pela correta utilização de sua conta, que não deverá ser utilizada para violar ou transpor as definições contidas nesta norma, bem como por qualquer atividade irregular exercida por outra pessoa de posse de seu nome de usuário.

6.1.3 Ao ser desligado da Fundação, o usuário perderá o acesso a sua conta, no entanto, a conta não será deletada e permanecerá desativada, sob gestão da GEINF.

6.2 Senhas

6.2.1 As senhas para acesso à rede corporativa são pessoais e intransferíveis, de uso exclusivo de cada usuário e de sua total responsabilidade.

6.2.2 A senha deverá ter, no mínimo, 7 caracteres, e deverá ser alterada, obrigatoriamente, a cada 45 dias. O sistema memoriza as 5 últimas senhas, não sendo possível usá-las novamente.

6.2.3 Só serão permitidas 3 tentativas de login com senha errada, por um mesmo usuário; após esse número, o acesso será bloqueado e o desbloqueio deverá ser solicitado à GEINF.

6.2.4 Para maior segurança, é obrigatório:

a) USAR uma senha:
   1) que misture caracteres maiúsculos e minúsculos;
   2) com caracteres não alfabéticos, ou sejam, números e pontuação;
   3) que possa ser digitada facilmente, sem ter que olhar para o teclado;
b) NÃO usar como senha:
   1) o nome de sua conta de usuário, ou qualquer variação do mesmo (invertido, com letras maiúsculas, duplicado, etc);
   2) qualquer um de seus nomes ou sobrenomes, ou qualquer variação destes;
   3) placa de automóvel, número de telefone, marca de seu automóvel, nome de pessoas de sua família, data de nascimento, endereço, etc;
   4) apenas números, ou repetições de uma mesma letra.

7 USO E CONTROLE DE DADOS, INFORMAÇÕES E ARQUIVOS

7.1 Critérios Gerais

7.1.1 Todos os documentos eletrônicos, arquivos, dados e informações relativas às atividades profissionais do usuário são de propriedade da PREVIRB e devem ficar armazenados na rede corporativa, nos respectivos diretórios de trabalho.

7.1.2 A cópia, transferência e/ou remoção de informações institucionais armazenadas em recursos computacionais da PREVIRB, por meio de qualquer meio ou dispositivo de entrada e saída de dados somente serão permitidas com a prévia autorização do superior imediato do usuário.

7.1.3 Não é permitido aos empregados o envio de qualquer arquivo de desenvolvimento (arquivos-fonte), tais como: imagens, textos e/ou códigos de fontes de aplicações ou similares, sem a devida autorização da Diretoria da PREVIRB, com exceção dos arquivos de dados para os Terceiros, com o objetivo de solucionar problemas técnicos, devendo ser comunicado previamente ao Gerente da área.

7.1.3.1 No caso em que seja necessário o envio de arquivo de dados para Terceiros, esse envio deverá obedecer a protocolos de segurança, sob a orientação da GEINF.

7.1.4 Caso seja constatado o envio de qualquer arquivo de propriedade da PREVIRB, sem a devida autorização, o responsável ficará sujeito às sanções estabelecidas nas normas internas e nas Leis nºs 9.279/96, 9.610/98, 9.609/98 e 13.709/2018 e alterações.

7.1.5 O padrão de acesso às informações armazenadas nos recursos computacionais da PREVIRB é estabelecido por perfis que definem os documentos e diretórios que podem ser acessados pelo usuário ou grupo de usuários, bem como os respectivos direitos de utilização, como leitura, escrita, remoção, cópia e salvamento, visando resguardar ao máximo as restrições ao conhecimento de informações confidenciais.

7.1.6 O tratamento dos dados pessoais dos Participantes e Assistidos terá como única finalidade o cumprimento do contrato previdenciário e o tratamento dos dados pessoais dos empregados, para cumprimento do contrato de trabalho.

7.1.7 Em caso do uso dos dados pessoais para fins de empréstimos e simulações será precedido de obtenção de consentimento do Titular do dado pessoal utilizado.

7.1.8 Após o fim do cumprimento do contrato previdenciário, seja pelo desligamento do titular junto à Fundação ou por falecimento, os dados pessoais desses Titulares serão mantidos armazenados pelo tempo necessário à prescrição dos direitos judiciais.

7.1.8.1 Após o cumprimento desse período, os dados serão anonimizados.

7.1.9 O dado sensível referente à filiação em sindicato será utilizado única e exclusivamente para cumprimento de obrigação legal, qual seja, o desconto da mensalidade/taxa na folha salarial ou de benefícios.

7.1.10 O dado sensível referente ao plano médico, licença doença, isenção de imposto de renda, será utilizado pela área administrativa da Fundação e pela área de Seguridade unicamente com o objetivo de cumprimento de obrigação legal.

7.1.11 As Unidades de armazenamento de informações utilizados na PREVIRB são fracionados de acordo com a seguinte classificação:

UNIDADE C	Disco local da estação de trabalho.
UNIDADE P	Disco de rede para uso comum dos usuários.

a) A **UNIDADE C** deverá ser utilizada exclusivamente para a instalação do sistema operacional e programas que integram o computador, não podendo ser usada para armazenar informações relativas aos trabalhos da PREVIRB;
b) A **UNIDADE P**, é o local reservado para armazenamento dos dados da PREVIRB. A área é exclusiva dos usuários e deverá ser utilizada somente para atender às necessidades da PREVIRB.

7.1.12 A GEINF realizará, em periodicidade a seu critério, verificação da utilização das Unidades de armazenamento de informações, utilizados na PREVIRB, visando à otimização de sua capacidade e a correção de eventuais distorções em seu uso.

7.1.13 Compete aos Diretores, em relação a Gerentes e empregados a eles subordinados, e aos Gerentes, em relação a empregados a eles subordinados, conceder ou retirar autorizações de acesso à Unidade, arquivos e à própria rede da PREVIRB.

7.1.14 Periodicamente, os acessos concedidos devem ser revistos pelos responsáveis.

7.2 Uso e Controle de Manuais, Mídias e Licenças

7.2.1 Os manuais, mídias e licenças dos recursos computacionais ou infraestruturas tecnológicas adquiridas pela PREVIRB são para uso exclusivo dos empregados para fins profissionais.

8 GERENCIAMENTO DA REDE CORPORATIVA

8.1 Proteção do Ambiente Tecnológico

8.1.1 A proteção da rede corporativa, do correio eletrônico e dos acessos a Internet é realizada pelo antivírus, AntiSpam e o firewall, que controlam todo o fluxo de arquivos, dados, navegação e programas.

8.1.2 Mitigação de Perda de Dados Digitais

8.1.2.1 É de responsabilidade da GEINF a execução de backups dos arquivos armazenados nas pastas de rede. Esses backups são executados diariamente após às 20h.

8.1.2.2 É de responsabilidade da GEINF a execução anual de testes de vulnerabilidades que deverão ser feitas por empresas especializadas com objetivo de mitigar os riscos de ataques cibernéticos.

8.1.2.3 A equipe da GEINF deverá, mensalmente, aplicar as atualizações de segurança tanto das estações de trabalho como dos servidores e ativos de rede.

8.2 Uso e Controle de *Softwares* e Aplicativos

8.2.1 A PREVIRB disponibiliza para seus empregados um conjunto de *softwares*, aplicativos ou executáveis para desempenho de suas atividades, todos devidamente licenciados, em observância à legislação que proíbe a cópia e a utilização ilegal de *softwares*.

8.2.2 É vedado ao usuário instalar e/ou utilizar programas, aplicativos ou executáveis não homologados pela PREVIRB, sejam obtidos em mídia eletrônica ou pela internet, à exceção dos programas livres, observando a recomendação constante no item a seguir.

8.2.3 A instalação de qualquer *software* não homologado pela PREVIRB nas estações de trabalho, desde que não proibida por lei (programas livres), só poderá ser feita com o prévio conhecimento do responsável pelo setor e com a supervisão da GEINF.

8.2.4 Ao usuário é vedado alterar ou destruir programas, ambientes operacionais, equipamentos de processamento ou comunicações instalados na PREVIRB, de sua propriedade ou de terceiros.

8.2.5 É terminantemente proibido o uso de qualquer software comercial, *freeware*, *shareware* que desrespeite os termos e condições de licenciamento ou que comprometa a segurança do ambiente de rede da Empresa.

8.2.6 O uso dos programas de mensagens eletrônicas é proibido, exceto os softwares homologados e instalados pela GEINF e os programas *de compartilhamento de dados*, são restritos à GEINF, exceto quando há autorização da Diretoria.

8.2.7 Sempre que houver necessidade de instalação de um novo *software*, a GEINF deverá comunicar aos setores e usuários interessados.

8.3 Uso e Controle de *Hardware*, Periféricos e Acessórios

8.3.1 A PREVIRB disponibiliza para seus empregados um conjunto de equipamentos e máquinas para desempenho exclusivo nas atividades profissionais, devidamente registrados no Ativo imobilizado da Empresa.

8.3.2 Não é permitida a instalação de qualquer equipamento, periférico ou acessório que não faça parte do acervo da PREVIRB.

8.3.3 É permitida, exclusivamente aos Diretores e Gerentes, além da equipe da GEINF, a utilização de mídias eletrônicas e outros meios de entrada e saída de dados, tais como *Pen Drive*, os quais poderão autorizar a utilização por outros empregados, em casos excepcionais e para atendimento às necessidades de serviço.

8.3.4 Na utilização dos equipamentos de propriedade da PREVIRB, deverão ser observados os seguintes cuidados:

a) Evitar o uso de pequenos objetos junto ao computador, tais como clipes, grampos, etc.;
b) Não colar adesivos ou qualquer outro material que possa provocar manchas ou danificar o equipamento;
c) Efetuar o bloqueio de tela sempre que se ausentar da sala, evitando que terceiros usem indevidamente e sem autorização o seu nome de usuário;
d) Armazenar sempre na Unidade P os arquivos que necessitem de cópia de segurança;
e) Verificar sua Unidade P (pasta pessoal ou da área), no mínimo semestralmente, e apagar os arquivos que não são mais necessários;
f) Verificar sua Unidade P:\GERAL\Area de Transferência, no mínimo semanalmente, e apagar os arquivos que não são mais necessários.

8.3.5 O usuário poderá modificar a área de trabalho do computador, conforme sua preferência, podendo alterar ponteiros de mouse, tamanhos e tipos de fontes, resolução, cores, etc.

8.3.6 O uso das impressoras é exclusivo para trabalhos que sejam de interesse da PREVIRB.

8.3.6.1 Manter as impressões em preto e branco, exceto quando o trabalho em questão exija variação de cores.

9 USO DE REDES EXTERNAS (*Internet* e Outras)

9.1 O acesso a redes externas é fundamental para o desempenho das atividades relacionadas à Tecnologia da Informação, principalmente a *Internet*, devendo estar voltado para pesquisa de assuntos e informações relacionadas com as atividades de interesse da PREVIRB.

9.2 A navegação nos *sites* da *Internet* somente é permitida através dos navegadores pré-instalados nos computadores individuais, vedada a instalação de outros navegadores, sem a autorização da GEINF.

9.3 O acesso a redes externas será permitido de acordo com as seguintes regras:

a) Da rede corporativa para a Internet a navegação somente poderá ser realizada através dos protocolos *HTTPS*, vedadas outras conexões e protocolos para redes externas;
b) Não é proibido o acesso a sites na internet para pesquisa de assuntos de natureza particular, desde que:
    1) não estejam incluídos nas categorias mencionadas na alínea c;
    2) não estejam sujeitos ao bloqueio seletivo realizado pela GEINF; e
    3) não comprometam o rendimento e a qualidade no desempenho das atividades laborais;
c) É proibida a navegação em sites pertencentes às seguintes categorias:
    1) Pornográfico e de caráter sexual;
    2) Pedofilia;
    3) Terrorismo;
    4) Drogas;
    5) *Hackers*;
    6) Violência e Agressividade (Racismo, Preconceito);
    7) Pirataria;
    8) Áudio e Vídeo;
    9) *WebMail* e *Instant Messenger* (*web* ou *client*);
    10) Conteúdo impróprio, ofensivo, ilegal, discriminatório e similares;
d) Não é permitido o *download* ou a troca de arquivos de imagens, vídeos, música, jogos, livros e outros infoprodutos, mesmo aqueles necessários ao exercício das atividades funcionais, sem a prévia autorização e suporte da GEINF;
e) A navegação nos sites sujeitos ao bloqueio seletivo feito pela GEINF poderá ser liberada diariamente, no período de 12h às 14h, para acesso nos intervalos de almoço e/ou descanso, sob a supervisão e controle dos responsáveis pelos diversos setores da PREVIRB.

10 CORREIO ELETRÔNICO

10.1 O uso do correio eletrônico (*e-mail*) é reconhecido pela PREVIRB como um meio de comunicação institucional, entre os seus usuários e entre a Empresa e o público externo, sendo facultado a todos os empregados.

10.2 Será obrigatório o uso do formato padrão do e-mail dos usuários da PREVIRB: nome.sobrenome@previrb.com.br, no qual o “nome” e “sobrenome” deverá corresponder ao nome de usuário.

10.2.1 As áreas poderão utilizar caixas de e-mail com indicação genérica (Seguridade; GEINF.ADM; GEINF.TI), desde que seja para recebimento de mensagens, sendo possível acesso a todo o grupo de empregados da área. Não será permitida resposta de e-mail sem identificação pessoal, colocando, obrigatoriamente, em cópia, o grupo envolvido.

10.3 No caso de ausência prolongada do usuário, este deverá solicitar a GEINF a configuração para redirecionar as suas mensagens para outra caixa postal interna da PREVIRB, com a seguinte resposta automática:

> Estou ausente do período de xx/xx/xxxx a xx/xx/xxxx. Sua mensagem não está sendo retransmitida automaticamente. Em caso de urgência, favor entrar em contato com: Nome (e-mail@previrb.com.br).

10.4 Todo e-mail enviado por usuários da rede da PREVIRB, seja interna ou externamente, deverá conter, ao final da mensagem, uma assinatura padrão, conforme modelo:

> Nome Completo (em negrito)
> Cargo – Sigla da Área
>
> Av. Mal. Câmara, 160 – Salas 1633/1634 – Centro
> Rio de Janeiro – RJ – CEP 20020-080
> Tel.: (21) 2277-xxxx – www.previrb.com.br

10.4.1 Aviso de Confidencialidade – Visando preservar a confidencialidade do conteúdo dos e-mails enviados por usuários da rede da PREVIRB, todas as suas mensagens deverão conter, ao final, o seguinte aviso:

> As informações contidas nesta mensagem e seus anexos são CONFIDENCIAIS, para uso restrito, sendo seu sigilo protegido por lei. A divulgação, distribuição ou reprodução do teor deste documento depende de autorização do emissor. Caso V.Sa. não seja o destinatário, preposto, ou a pessoa responsável pelo recebimento desta mensagem fica, desde já, notificado que qualquer divulgação, distribuição ou reprodução é estritamente proibida, sujeitando-se o infrator às sanções legais. Caso esta comunicação tenha sido recebida por engano, favor nos avisar imediatamente, respondendo esta mensagem.

10.5 Deverão ser observados os seguintes procedimentos no uso do correio eletrônico (*e-mail*):

a) A conta de *e-mail* corporativa, fornecida pela PREVIRB, deverá ser utilizada, preferencialmente, para o envio e recebimento de mensagens relacionadas aos trabalhos desenvolvidos pelo empregado;
b) Os *e-mails* recebidos pelo endereço institucional privacidade@previrb.com.br, serão tratados pelo Comitê de Privacidade e Proteção de Dados – COPPD, sendo o Encarregado (*DPO*) o responsável de atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
c) Os *e-mails* recebidos pelo endereço institucional etica@previrb.com.br, serão automaticamente redirecionados aos membros do Comitê Ética para o devido tratamento;

d) Qualquer manifestação sobre os assuntos da Fundação, por parte dos empregados, para Participantes ou Terceiros, deverá ter a prévia aprovação do superior imediato;
e) É proibido o uso da conta de *e-mail* corporativo para promover quaisquer tipos discórdia e/ou discussão, ou para constranger, assediar ou ameaçar qualquer pessoa;
f) A conta de *e-mail* não deve ser utilizada para disseminar ou transmitir informações ou imagens de caráter pornográfico ou que violem a legislação em vigor no Brasil, tais como ameaças, difamação, calúnia, injúria ou qualquer tipo de preconceito;
g) É proibido o envio de mensagens ou anexos que possam causar constrangimentos ou expor a intimidade e privacidade do emissor ou do receptor da mensagem;
h) O empregado será responsabilizado pelo uso inadequado de sua conta de e-mail.

11 UTILIZAÇÃO DE EQUIPAMENTOS PARTICULARES OU DE TERCEIROS DENTRO DA EMPRESA

11.1 *Notebooks* de fornecedores para terem acesso à rede de dados da Fundação, abrangida neste documento, precisam ser avaliados pela GEINF.

11.2 Nas ocasiões que se faz necessário um fornecedor acessar a rede da PREVIRB, o acesso é supervisionado pela GEINF, e a PREVIRB fornece o equipamento.

12 DESLIGAMENTO DE USUÁRIO

12.1 A GEINF executará os procedimentos para revogação dos acessos, quando do desligamento de um empregado, estagiário ou dirigente dos quadros da Fundação, bem como os de Terceiros que tenham seu contrato de Prestação de Serviço encerrado.

12.2 A revogação dos acessos deve ser imediata, sendo que a conta de e-mail ficará ativa pelo período de 3 (três) meses, sendo esta direcionada ao superior imediato.

13 INFORMAÇÕES VERBAIS OU EM MEIO FÍSICO E ACESSO AS INSTALAÇÕES

13.1 Recebimento de Documentos

13.1.1 Toda documentação recebida pela PREVIRB passará primeiro pela Recepção da Fundação, onde é identificada a área de destino e despachada ao responsável pelo setor, conforme procedimento “4.7.4 Receber Documentos Enviados à PREVIRB e Distribuir aos Setores Competentes”, estabelecido no Manual de Procedimentos.

13.1.2 No caso de documentos provenientes da justiça, entregues pessoalmente por oficial de justiça, a recepção do documento será feita por membro da Diretoria ou a quem a Diretoria delegar.

13.1.3 Cabe ao Gestor ou ao Diretor, classificar o documento recebido e dar prosseguimento ao assunto.

13.2 Arquivamento

13.2.1 Em relação às informações armazenadas em meio físico, deverão ser adotados procedimentos que preservem os dados ali contidos de qualquer exposição indevida, garantindo a reserva e o sigilo necessários no tratamento de documentos que circulam no ambiente institucional.

13.2.2 Papéis e outros meios de armazenamento contendo informações confidenciais, devem receber o mesmo tratamento de segurança que seu computador, ou seja, estar em local seguro e de acesso restrito.

13.2.2.1 O acesso aos armários onde estão arquivados os documentos, processos ou pastas de participantes, só poderá ser feito por pessoas autorizadas pelos responsáveis dos setores.

13.3 Descarte

13.3.1 Documentos inservíveis deverão ser avaliados, com o objetivo de selecionar o que pode ser descartado em lixo comum e o que deverá ter outra destinação, em função de seu conteúdo, sempre observando a Tabela de Temporalidade de Documentos da PREVIRB (MGC 06.2).

13.3.2 Papéis que necessitem de tratamento especial no descarte deverão ser reunidos, com a finalidade de serem triturados na máquina própria da PREVIRB, de acordo com a orientação e apoio da GEINF.

13.4 Processos

13.4.1 Todos os processos PREVIRB, são inicialmente classificados como RESTRITO, podendo ter esse nível alterado, conforme a necessidade de segurança das informações nele contidas.

13.4.1.1 Ao se incorporar um documento classificado como CONFIDENCIAL em um Processo PREVIRB, esse passa a ter o mesmo status do documento.

13.4.2 Para poder acessar processos PREVIRB marcados como Confidenciais é necessária a autorização por *e-mail* do responsável pela definição desse nível de confidencialidade.

13.4.3 É vedada a retirada de processos das dependências da PREVIRB, independente de seu nível de Confidencialidade, exceto em casos de demanda judicial ou com autorização do Conselho Deliberativo.

13.5 Mesa Limpa

13.5.1 Nenhum processo, pasta ou documento contendo informações da Fundação ou de Participantes deve ser deixado à vista em mesas e armários após o término do expediente ou na ausência do responsável, seja em papel ou em quaisquer dispositivos, eletrônicos ou não.

13.6 Impressões

13.6.1 As impressões somente ocorrerão após o usuário se autenticar na impressora, com login e senha, e aprovar a impressão. Os documentos impressos devem ser retirados imediatamente e não deixados nas bandejas dos equipamentos.

13.6.2 Documentos impressos devem ser protegidos contra perda, cópia e uso não autorizado, ou seja, não podem ser deixados nas impressoras ou em cima das mesas ou armários sem o responsável presente.

13.6.3 Impressões indevidas não poderão permanecer nas impressoras, bandejas de rejeição ou na mesa das pessoas próximas. Devem ser destruídas de imediato.

13.6.4 Documentos abandonados nas impressoras ou bandejas de rejeição, deverão ser destruídos pela GEINF ao final do expediente, quando os equipamentos forem desligados.

13.7 Comunicação Verbal

13.7.1 Atenção ao tratar de assuntos de trabalho dentro e fora da Fundação, principalmente em locais públicos ou próximos a visitantes, seja ao telefone ou com algum colega, ou mesmo prestador de serviços.

13.7.2 Evite tratar de assuntos confidenciais e citar nomes ou dados de pessoas fora da Fundação ou próximo a desconhecidos.

13.7.3 Caso seja imprescindível falar de assuntos confidenciais em locais públicos, fique atento às pessoas a sua volta, evitando assim que as informações sejam utilizadas com o intuito de prejudicar a Fundação.

13.8 Acesso as Instalações da Fundação

13.8.1 Não será permitido o acesso de pessoas não autorizadas, às áreas de armazenamento ou processamento de informações, devendo os Participantes, Assistidos e visitantes serem atendidos nas salas de atendimento ou de reunião.

14 VIOLAÇÃO DA PSI

14.1 Denúncias de violação a esta política serão encaminhadas ao Comitê de Ética para a devida apuração e encaminhamento dos fatos ocorridos aos responsáveis.

14.2 Em casos de violação desta política, poderão ser adotadas sanções administrativas e/ou legais, podendo culminar no desligamento e eventuais processos, se aplicáveis, aos infratores.

15 DISPOSIÇÕES FINAIS

15.1 Os Gestores da PREVIRB são responsáveis pela disseminação das práticas aqui listadas, junto aos seus subordinados, bem como pela verificação do seu cumprimento.

15.2 Esta política entra em vigor na data de aprovação e deve ser revisada sempre que as circunstâncias assim exigirem.

15.3 Os casos omissos ou excepcionais serão resolvidos pela DIREX ou pelo CONDEL, conforme as Competências e Alçadas Decisórias vigentes.

16 TERMO DE CONFIDENCIALIDADE

16.1 Todos os integrantes do quadro funcional da PREVIRB – Dirigentes, Empregados e Estagiários, membros de Conselhos e Comitês devem assinar o Termo de Confidencialidade da Política de Segurança da Informação, renovando as declarações sempre que forem processadas alterações no seu conteúdo, nos moldes a seguir:

16.1.1 Os Termos assinados pelos Conselheiros e membros dos Comitês terão validade enquanto perdurar os respectivos mandatos.

TERMO DE CONFIDENCIALIDADE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Por meio deste Termo, declaro ter lido a Política de Segurança da Informação da PREVIRB, para conhecimento e utilização no desempenho de minhas atividades profissionais.

Declaro, ainda, estar ciente de que todas as informações a mim disponibilizadas em razão do exercício de minhas funções, por serem de propriedade exclusiva da PREVIRB, devem ser tratadas como restritas, internas ou confidenciais, não sendo permitido divulgá-las sob qualquer forma ou pretexto, sem o prévio consentimento da autoridade detentora da competência da Gerência ou Diretoria.

O descumprimento do presente Termo e das normas que constituem a Política de Segurança da Informação caracteriza falta grave, passível de sanções e penalidades legais, sem prejuízo da responsabilidade civil e criminal.

Rio de Janeiro, de de .

(assinatura)
Nome por Extenso