Política de Segurança da Informação (PSI)

(Aprovado pela Resolução CONDEL 021/2026, de 3/9/2026)

S U M Á R I O

Política de Segurança da Informação (PSI)

(Aprovado pela Resolução CONDEL 021/2026, de 3/9/2026)

1 OBJETVO E ABRANGÊNCIA

1.1 Esta Política de Segurança da Informação tem por objetivo estabelecer princípios, diretrizes e controles que devem ser observados pela PREVIRB para a gestão da segurança da informação, de modo a assegurar proteção, uso adequado e tratamento seguro dos ativos informacionais ao longo de todo o seu ciclo de vida.

1.2 Esta Política se aplica a todas as informações, ativos, processos, sistemas, ambientes, pessoas e tecnologias empregados nas atividades da PREVIRB, devendo ser observada por colaboradores, administradores e terceiros que acessem, tratem ou armazenem informações em nome da PREVIRB, em conjunto com os demais normativos internos e demais instrumentos de governança corporativa.

2 DEFINIÇÕES

a) **ACESSO REMOTO:** acesso à rede e a recursos corporativos a partir de locais externos às instalações da PREVIRB, mediante mecanismos aprovados (por exemplo, VPN);

b) **AMEAÇA**: causa potencial de um incidente indesejado que pode resultar em dano a um ativo de informação;

c) **ANPD:** Agência Nacional de Proteção de Dados;

d) **AUTENTICAÇÃO MULTIFATOR (MFA)**: método de autenticação que requer a combinação de dois ou mais fatores (conhecimento, posse, inerência) para validar a identidade do usuário;

e) ***BACKUP* (cópia de segurança):** cópia de dados realizada com o objetivo de recuperação em caso de perda, dano ou indisponibilidade;

f) **CLASSIFICAÇÃO DA INFORMAÇÃO:** processo de categorização da informação segundo seu nível de sensibilidade e impacto, adotando-se as classes Pública, Interna, Restrita e Confidencial/Sigilosa:

   i. **Pública**: Informações destinadas à divulgação externa sem restrições (ex: relatórios anuais publicados, comunicações legais obrigatórias à participantes, beneficiários e assistidos);
   ii. **Interna:** Informações para usos internos que, se divulgadas indevidamente, causariam impacto mínimo (ex: comunicados internos não sigilosos);
   iii. **Restrita:** Informações cujo acesso é limitado a grupos específicos, cuja exposição pode causar impacto operacional ou reputacional (ex: documentos gerenciais, planilhas de controles setoriais);
   iv. **Confidencial /Sigilosa (inclui dados pessoais e sensíveis):** Informações de alto risco, cuja divulgação indevida pode causar impacto elevado, sendo necessários requisitos reforçados de proteção e guarda (ex: Ex.: dados pessoais de participantes, projeções atuariais, contratos estratégicos);

g) **COLABORADORES:** pessoas físicas que exerçam atividades, representem ou atuem em nome da PREVIRB, independente do vínculo jurídico, incluindo, mas não se limitando a conselheiros, diretores, empregados, estagiários, aprendizes e membros dos Comitês;

h) **CONDEL**: Conselho Deliberativo da PREVIRB;

i) **CONFI**: Conselho Fiscal da PREVIRB;

j) **COINT**: Comitê de Controles Internos da PREVIRB;

k) **CREDENCIAIS DE ACESSO:** meios de autenticação vinculados ao usuário (por exemplo, identificador, senha, *token*, biometria) para acesso a recursos corporativos;

l) **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;

m) **DIREX**: Diretoria Executiva da PREVIRB;

n) **DLP (*Data Loss Prevention*)**: conjunto de ferramentas e processos para prevenir vazamento, exfiltração ou uso indevido de dados;

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

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

q) **IDS/IPS**: sistemas de detecção e prevenção de intrusões que monitoram e/ou bloqueiam atividades suspeitas em rede e em host;

r) **INCIDENTE DE SEGURANÇA DA INFORMAÇÃO:** evento adverso, confirmado ou sob suspeita, que comprometa ou possa comprometer a confidencialidade, a integridade ou a disponibilidade da informação, dos sistemas ou serviços;

s) **INFORMAÇÃO**: todo e qualquer conteúdo que que possua valor para a PREVIRB ou para pessoas a ela vinculadas, independentemente do suporte (físico ou digital) e do meio de circulação;

t) **LOGIN:** ato de autenticar-se na rede corporativa por meio de credenciais válidas;

u) **METADADOS:** conjunto de dados estruturados que descrevem, contextualizam, identificam ou facilitam o gerenciamento, a localização, o uso e a preservação da informação, incluindo, entre outros, dados sobre autoria, data de criação, classificação, formato, nível de acesso, histórico de alterações e demais características associadas, independentemente do suporte (físico ou digital);

v) **MÍDIAS REMOVÍVEIS**: dispositivos físicos de armazenamento móvel (por exemplo, USB, discos externos), cujo uso é controlado e excepcional;

w) **PARTICIPANTES**: pessoas vinculadas a Planos de Benefícios da PREVIRB;

x) **PATROCINADORES:** pessoas jurídicas admitidas nesta qualidade, mediante celebração de Convênio de Adesão;

y) **PLANO DE CONTINUIDADE DE TI**: documento que define estratégias e procedimentos para manter processos críticos operacionais diante de interrupções;

z) **REDE CORPORATIVA:** conjunto de estações de trabalho, servidores, dispositivos e serviços interconectados para compartilhamento de dados, aplicativos, recursos tecnológicos e periféricos;

aa) **REPOSITÓRIOS CORPORATIVOS**: locais e serviços oficialmente aprovados pela área de tecnologia da informação para armazenamento e compartilhamento de informações institucionais, com controle de acesso e trilhas de auditoria;

bb) **RISCO**: combinação da probabilidade de ocorrência de um evento e das suas consequências sobre os objetivos organizacionais e os ativos de informação;

cc) **RPO (*Recovery Point Objective*)**: ponto-alvo máximo de perda aceitável de dados, medido pelo tempo entre a última cópia utilizável e o evento de interrupção;

dd) **RTO (*Recovery Time Objective*)**: tempo-alvo máximo para restabelecer um processo/sistema após uma interrupção;

ee) **SEGURANÇA DA INFORMAÇÃO:** conjunto de medidas administrativas, técnicas e físicas destinadas a 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 esta Política;

ff) **SERVIÇOS EM NUVEM**: serviços de computação providos por terceiros, sob modelos de responsabilidade compartilhada, sujeitos a requisitos de segurança, privacidade, continuidade e portabilidade;

gg) **TERCEIROS:** prestadores de serviços, fornecedores e seus respectivos colaboradores, administradores e prepostos a eles vinculados, conforme previsão contratual, parceiros comerciais ou qualquer outra pessoa, física ou jurídica, que mantenha relações comerciais com a PREVIRB;

hh) **TITULAR DO DADO PESSOAL:** pessoa natural a quem se referem os dados pessoais objeto de tratamento, inclusive beneficiários e dependentes cadastrados;

ii) **TRATAMENTO DE RISCOS**: processo de selecionar e implementar medidas para modificar o risco (mitigar, aceitar, transferir ou evitar);

jj) **TRILHAS DE AUDITORIA (logs)**: registros de eventos relevantes de segurança e de operação (por exemplo, autenticações, mudanças de configuração, bloqueios), destinados a suporte a investigação, compliance e melhoria contínua;

kk) **USUÁRIO:** identificação pessoal de colaboradores, administradores ou terceiros, que possuem conta de acesso à rede corporativa e demais infraestruturas tecnológicas da PREVIRB;

ll) **VULNERABILIDADE**: fragilidade que pode ser explorada por uma ameaça para causar impacto a um ativo de informação;

mm) **VPN (Rede Privada Virtual)**: tecnologia que estabelece canal seguro e autenticado para acesso remoto aos recursos corporativos.

3 DIRETRIZES

3.1 Os princípios que norteiam a Política de Segurança da Informação da PREVIRB são:

a) **Finalidade e Uso Adequado da Informação**: As informações, incluindo dados pessoais, devem ser tratadas e utilizadas somente para finalidades legítimas, específicas e compatíveis com

as atividades previdenciárias, administrativas, atuariais, financeiras, jurídicas e regulatórias da entidade, vedado qualquer uso indevido ou não autorizado;

b) **Confidencialidade:** Assegurar que as informações sejam acessadas apenas por pessoas autorizadas, com adoção de controles, mecanismos de autenticação e restrições baseadas no princípio do menor privilégio, prevenindo acesso, divulgação ou uso indevido;

c) **Integridade:** Garantir a exatidão, consistência e completude das informações, protegendo-as contra alteração acidental, indevida, não autorizada ou fraudulenta, por meio de controles técnicos, administrativos e mecanismos de auditoria e rastreabilidade;

d) **Disponibilidade:** Assegurar que as informações, sistemas, serviços e recursos críticos estejam acessíveis aos usuários autorizados sempre que necessário, mediante mecanismos de continuidade, contingência, recuperação de desastres e prevenção de interrupções;

e) **Necessidade e Minimização**: Limitar coleta, tratamento, armazenamento e compartilhamento de informações ao mínimo necessário para o atendimento das finalidades institucionais, com retenção pelo tempo estritamente requerido por obrigações legais, regulatórias ou operacionais;

f) **Segurança, Prevenção e Gestão de Riscos**: Adotar medidas técnicas, administrativas e organizacionais para proteger informações e ativos contra ameaças internas e externas, intencionais ou acidentais, incluindo prevenção, detecção, resposta e tratamento de incidentes, com base em práticas de gestão de riscos de segurança da informação;

g) **Ciclo de Vida da Informação:** Garantir o adequado gerenciamento da informação em todas as suas fases – criação, classificação, uso, armazenamento, compartilhamento, retenção e descarte – conforme requisitos legais, regulatórios, contratuais e internos;

h) **Transparência, Capacitação e Comunicação Adequada:** Promover continuamente a conscientização e o treinamento dos colaboradores, administradores e terceiros, de forma clara e acessível, sobre regras, controles, responsabilidades e diretrizes de segurança da informação, respeitando-se sigilo legal e classificação da informação.

4 DIRETRIZES GERAIS DE ACESSO À REDE CORPORATIVA

4.1 Todos os dados, informações, documentos, registros e metadados produzidos para ou pela PREVIRB, em quaisquer meios (físicos ou digitais), bem como contas, logs e demais artefatos gerados pelos sistemas corporativos, são propriedade da PREVIRB e devem ser armazenados em repositórios corporativos aprovados com controle de acesso por perfis e trilhas de auditoria, vedado o armazenamento permanente em discos locais de estações, exceto cache temporário ou cópias de trabalho estritamente necessárias, a serem removidas ao final da atividade.

4.2 A área de tecnologia da informação manterá a relação oficial de repositórios autorizados, seus requisitos de uso e os controles mínimos de segurança aplicáveis.

4.3 O compartilhamento externo (envio para terceiros) de informações institucionais dependerá de autorização prévia do responsável da área, com observância da classificação da informação, uso de criptografia e registro do envio (conteúdo, destinatário, finalidade, base legal e responsável) em meio aprovado pela PREVIRB.

4.4 É vedado aos usuários o envio de artefatos de desenvolvimento (p. ex., código-fonte, textos, scripts, componentes de build ou bibliotecas internas) para qualquer parte externa sem autorização expressa da Diretoria Executiva ou do gestor da área, exceto quando estritamente necessário o envio de arquivos de dados a terceiros para solução de problemas técnicos, mediante registro nos termos do item 4.3.

4.5 As informações da PREVIRB devem ser classificadas conforme seu nível de sensibilidade, impacto e necessidade de proteção, independente do meio de divulgação (físico ou virtual) e destinatário final (público interno ou externo), conforme critérios (pública, interna, restrita e/ou confidencial/sigilosa).

4.6 Os equipamentos, celulares corporativos, *softwares*, licenças, serviços em nuvem e demais ativos fornecidos para armazenamento, processamento, acesso e controle devem ser utilizados exclusivamente para fins institucionais, sendo vedada cópia, subversão técnica, uso não autorizado ou em desconformidade com licenças e contratos.

4.7 O tratamento de dados pessoais observará as bases legais, os princípios e as medidas de segurança previstas na LGPD, com adoção de medidas técnicas e administrativas aptas a protegê-los contra acessos não autorizados e incidentes de segurança.

4.8 O uso de dados pessoais de participantes e assistidos será limitado ao cumprimento do contrato previdenciário e de obrigações legais e regulatórias; o uso para simulações ou ofertas de produtos dependerá da base legal aplicável, inclusive consentimento quando exigido.

4.9 Dados pessoais sensíveis serão tratados estritamente para o atendimento de obrigações legais e finalidades específicas, com controles reforçados.

4.10 Após o término do relacionamento, os dados pessoais serão mantidos para o cumprimento de obrigações legais e, ao final, eliminados ou anonimizados.

4.11 Na ocorrência de incidente de segurança com risco ou dano relevante aos titulares, observar-se-á a comunicação à ANPD e aos titulares, em prazo razoável e com as informações mínimas exigidas pela legislação vigente.

4.12 Será atribuída a cada colaborador, administrador e eventuais terceiros com necessidades de acessos, contas de usuários individuais, administrada pela área de tecnologia da informação, para autenticação na rede corporativa e demais recursos tecnológicos.

4.13 É vedado o compartilhamento de credenciais e o uso de credenciais genéricas, salvo contas técnicas de serviço, que deverão ter propósito explícito, escopo mínimo e monitoramento reforçado.

4.14 O padrão de acesso a informações armazenadas em recursos corporativos será estabelecido por perfis que definem quais documentos e diretórios podem ser acessados por usuário ou grupo, bem como os direitos correspondentes (leitura, escrita, remoção, cópia, salvamento).

4.15 A concessão, revisão e revogação de acessos será formalizada e revista minimamente anualmente pela área de tecnologia da informação em conjunto com os gestores das áreas de negócio.

4.16 O titular da conta é responsável pelo seu uso adequado e pela guarda de suas credenciais, respondendo por atos praticados sob seu identificador até comunicação de suspeita de comprometimento.

4.17 Em casos de afastamentos previdenciários, durante o período de ausência, os acessos serão suspensos pela área de tecnologia da informação em até 24 horas, e o e-mail será redirecionado ao gestor e configurada resposta automática de e-mail, a fim de assegurar a continuidade operacional.

4.18 Nos casos de desligamento ou cessação de vínculo, os acessos serão revogados pela área de tecnologia da informação imediatamente, devendo a conta permanecer desativada, visando à preservação de evidências e à continuidade operacional.

4.18.1 Mediante solicitação do gestor, o endereço de e-mail poderá ser redirecionado este pelo período de 90 dias, quando será configurada resposta automática de e-mail e disponibilizada cópia do histórico de e-mails.

4.19 Para a consecução dos itens 4.17 e 4.18, é de responsabilidade da área de Recursos Humanos informar à área de tecnologia da informação, os casos de afastamento previdenciário, desligamento e/ou cessação de vínculo.

4.20 Para os usuários de celulares corporativos, nas hipóteses de (i) cessação do vínculo, (ii) substituição do equipamento ou (iii) quando da desnecessidade de uso, o dispositivo fornecido pela PREVIRB e seus acessórios deverão ser devolvidos em perfeitas condições, observados os procedimentos definidos pela área de tecnologia da informação para a retirada segura de perfis e dados corporativos.

4.21 A PREVIRB adotará autenticação multifator (MFA) para o acesso externo aos sistemas e informações classificados como restritos ou confidenciais, e para todo acesso remoto.

4.22 As senhas são pessoais e intransferíveis e devem:

a) possuir no mínimo 10 (dez) caracteres;
b) combinar letras maiúsculas e minúsculas, números e caracteres especiais;
c) não conter informações óbvias ou relacionadas ao usuário;
d) não ser reutilizadas dentre as 10 (dez) últimas;
e) ser alteradas quando do primeiro acesso, a cada 45 dias e sempre que houver suspeita de comprometimento.

4.23 Após 5 (cinco) tentativas de autenticação malsucedidas, a conta será bloqueada, devendo o desbloqueio ser solicitado à área de tecnologia da informação pelos canais oficiais.

5 GERENCIAMENTO DA REDE CORPORATIVA

5.1 A PREVIRB manterá camadas de proteção tecnológicas, incluindo, no mínimo, *firewall*, *anti-malware*/*antispam*, filtro de navegação (*web filtering*), IDS/IPS e segmentação de rede, com monitoramento contínuo proporcional ao risco.

5.2 A área de tecnologia da informação manterá inventário atualizado de ativos de rede e segurança, contemplando versões, níveis de correção e responsáveis técnicos.

5.3 A PREVIRB manterá processo contínuo de gestão de vulnerabilidades, com varreduras internas e externas em periodicidade mínima semestral e testes de intrusão anuais por empresa especializada, podendo ocorrer execuções adicionais diante de mudanças relevantes ou ameaças críticas.

5.3.1 O planejamento, escopo e os resultados das varreduras de vulnerabilidades e dos testes de intrusão deverão ser formalmente documentados, incluindo o racional adotado, os testes definidos, os ativos avaliados (ex: sistemas, aplicações e infraestruturas), mantendo registros formais dos relatórios, evidências, resultados e reportes internos após a realização das atividades.

5.4 A área de tecnologia da informação aplicará correções de segurança (patch management) de forma tempestiva, com prazos definidos por criticidade em norma técnica interna, no mínimo mensal para atualizações regulares e imediata para correções críticas que afetem a segurança.

5.5 Eventos relevantes de segurança (p. ex., autenticações, elevação de privilégio, mudanças de configuração, bloqueios e detecções) serão registrados, correlacionados e monitorados, mediante registro por logs.

5.6 A área de tecnologia da informação executará rotinas de backup de dados e sistemas críticos com política de retenção definida, criptografia, cópias fora de linha ou imutáveis quando aplicável, e testes periódicos de restauração para assegurar os objetivos de RTO e RPO definidos no Plano de Continuidade de TI.

5.7 As credenciais e repositórios de *backup* terão registro de operações e verificações de integridade.

5.8 As janelas operacionais de *backup* seguirão cronograma formal da área de tecnologia da informação, devendo preferencialmente ocorrer diariamente, em períodos de menor uso da rede corporativa, podendo ser ajustadas por necessidade operacional.

5.8.1 A PREVIRB disponibilizará aos usuários equipamentos e o conjunto oficial de softwares para o desempenho das atividades, cujas novas instalações homologadas serão comunicadas previamente pela área de tecnologia da informação aos setores e usuários impactados.

5.9 Somente *softwares* homologados e devidamente licenciados poderão ser instalados, devendo as exceções serem formalmente aprovadas pela área de tecnologia da informação, após a avaliação do risco de instalação.

5.10 É vedada a alteração ou destruição não autorizada de programas, ambientes operacionais, equipamentos e/ou configurações de rede, de propriedade da PREVIRB ou de terceiros.

5.11 O uso dos programas de mensagens eletrônicas é proibido, exceto os *softwares* homologados e instalados pela área de tecnologia da informação, sendo os programas de compartilhamento de dados restritos à área de tecnologia da informação, exceto quando houver autorização formal da Diretoria para utilização.

5.12 É vedada a instalação de equipamentos, periféricos ou acessórios que não façam parte do acervo da PREVIRB sem autorização prévia da área de tecnologia da informação.

5.13 O uso de mídias removíveis (p. ex., *USB*, *pen drives*, *hardware* externo) é restrito e excepcional à equipe da área de tecnologia da informação, os quais poderão autorizar o uso de mídias removíveis por outros colaboradores e/ou terceiros, em casos excepcionais e para atendimento a necessidades de serviço, com o devido registro formal da autorização.

5.14 O uso de serviços em nuvem obedecerá a avaliação e contratação prévias com requisitos de segurança, privacidade e continuidade, e controles equivalentes ou superiores aos ambientes internos, incluindo criptografia, gestão de identidades (*MFA*), *logging*, residência e localização de dados, bem como plano de saída/portabilidade.

5.15 As informações institucionais que demandem cópia de segurança deverão ser armazenadas exclusivamente nos repositórios corporativos autorizados, sendo responsabilidade do usuário manter apenas arquivos necessários e atualizados, promovendo periodicamente a exclusão de documentos obsoletos ou desnecessários, inclusive em áreas destinadas à transferência temporária de arquivos.

5.16 O acesso remoto à rede corporativa, por colaboradores ou terceiros, ocorrerá exclusivamente por meios aprovados (p. ex., *VPN* corporativa), com autenticação multifator (*MFA*) e verificação de postura do dispositivo (*antimalware* ativo, criptografia de disco e correções aplicadas).

5.17 Alterações em infraestrutura, sistemas, aplicações e controles de segurança seguirão processo formal de gestão de mudanças, com registro, aprovações, testes e plano de *rollback*, minimizando impactos na continuidade operacional.

5.18 A área de tecnologia da informação comunicará aos usuários, com antecedência razoável, janelas de manutenção, atualizações relevantes e mudanças com potencial impacto operacional; mudanças emergenciais observarão rito específico, com comunicação posterior.

5.19 O uso de equipamentos particulares ou de terceiros para acesso a recursos da PREVIRB dependerá de autorização prévia da área de tecnologia da informação e do atendimento aos requisitos de segurança definidos nesta Política e em normas correlatas, devendo os dispositivos autorizados possuir *antimalware* ativo, atualizações aplicadas e bloqueio de tela configurado.

6 USO DE REDES EXTERNAS (Internet e Outras)

6.1 O acesso a redes externas destina-se a fins institucionais e deverá ocorrer por meio de navegadores homologados, observados os controles corporativos de segurança e monitoramento.

6.2 É vedado utilizar mecanismos que contornem os controles da PREVIRB (p. ex., proxies não autorizados, VPNs pessoais ou navegadores não aprovados).

6.3 A navegação em redes externas priorizará protocolos e canais seguros e será encaminhada por *proxy*/*firewall* com filtro de conteúdo (*web filtering*) e proteção *antimalware*, proporcionais à classificação e ao risco.

6.4 Admite-se uso de redes externas para fins pessoais, de forma moderada, sem prejuízo às atividades laborais e em conformidade com bloqueios e monitorações estabelecidos pela área de tecnologia da informação.

6.5 Categorias de alto risco e conteúdos ilegais ou incompatíveis com o ambiente corporativo permanecerão bloqueados por política, abrangendo, no mínimo, pornografia (incluídas variantes ilícitas como exploração/abuso infantil), incitação à violência/ódio, terrorismo, drogas ilícitas, pirataria, distribuição de *malware*, *phishing*, domínios maliciosos e assemelhados.

6.5.1 A relação de categorias e subcategorias será mantida e atualizada pela área de tecnologia da informação, com base em inteligência de ameaças e requisitos legais/regulatórios.

6.5.2 Serviços de streaming de áudio/vídeo, *webmail* externo e mensagerias não corporativas serão proibidos por padrão; exceções dependerão de justificativa de negócio, avaliação de risco, aprovação formal e registro, podendo ser aplicadas janelas de acesso por avaliação da área de tecnologia da informação.

6.6 Downloads e uploads estarão sujeitos a controles automáticos de *antimalware*, DLP e bloqueio por tipo de arquivo/extensão para executáveis, scripts e formatos de risco, podendo exigir autorização prévia e registro em casos excepcionais.

7 CORREIO ELETRÔNICO

7.1 O correio eletrônico corporativo é meio oficial de comunicação e deverá ser utilizado preferencialmente para assuntos institucionais, em conformidade com esta Política e com as diretrizes de classificação e transferência de informações.

7.2 É vedado o uso do e-mail corporativo para envio de mensagens e/ou imagens com conteúdo ilícito, assédio, discriminação, ofensas ou divulgação de conteúdo impróprio, sujeitando o infrator às sanções cabíveis.

7.3 Serão adotados mecanismos de proteção contra *phishing*, *malware* e *spam*, devendo mensagens que contenham informação classificada como restrita ou confidencial utilizar criptografia e canais aprovados.

7.4 É vedado o encaminhamento automático de mensagens para caixas externas ao domínio corporativo; exceções dependerão de avaliação de risco, mediante autorização formal da área de tecnologia da informação.

7.5 Somente serviços corporativos homologados de mensagens poderão ser utilizados, devendo eventuais integrações com serviços externos serem previamente avaliados e aprovados formalmente pela área de tecnologia da informação.

7.6 Em casos de ausência prolongada, é obrigatória a configuração de mensagem automática temporária, com indicação do substituto responsável pelo atendimento das demandas durante o período.

7.7 O acesso e o uso desses recursos serão restringidos conforme previsto na Norma de Atos Administrativos, cabendo à área de Recursos Humanos suspender, limitar ou reativar os acessos sempre que necessário para garantir a segurança da informação e a continuidade das atividades.

7.8 São vedadas respostas sem a identificação pessoal do responsável pelo retorno de e-mails encaminhados a caixas funcionais genéricas (p. ex: Seguridade; GEINF.ADM; GEINF.TI).

8 SEGURANÇA FÍSICA E PROTEÇÃO DE INFORMAÇÕES

8.1 O sistema de videomonitoramento (CFTV) da PREVIRB será utilizado exclusivamente para fins de segurança patrimonial e das pessoas, observados os princípios desta Política, bem como a legislação aplicável à proteção de dados pessoais.

8.1.1 As câmeras não possuirão captação de áudio, sendo vedada a gravação de imagens em banheiros e sanitários, áreas de alimentação, salas de reunião ou em quaisquer locais que impliquem expectativa elevada de privacidade.

8.1.2 A gravação, quando existente, limitar-se-á às áreas de acesso controlado e/ou de segurança, estritamente na medida necessária à mitigação de riscos compatíveis com a finalidade aqui estabelecida.

8.1.3 O acesso ao sistema e às imagens será restrito a pessoas formalmente autorizadas, devendo todas as atividades realizadas serem registradas por meio de trilhas de auditoria (*logs*), e as imagens mantidas apenas pelo prazo necessário ao atendimento das finalidades institucionais e obrigações legais., com descarte seguro ao término do período de retenção.

8.1.4 A PREVIRB assegurará a transparência quanto à existência do videomonitoramento por meio de sinalização adequada.

8.2 Áreas de processamento/armazenamento de informação terão acesso restrito e controle de visitantes, quando aplicável, evitando qualquer exposição indevida, garantindo a reserva e o sigilo necessários no tratamento de documentos que circulam no ambiente institucional.

8.3 Documentos físicos contendo informação classificada devem ser mantidos em locais de acesso controlado (armários/arquivos), com registros de retirada/devolução quando cabível.

8.4 Todos os processos da PREVIRB serão inicialmente classificados como RESTRITOS, podendo ter o nível elevado ou reduzido mediante avaliação do responsável pela informação, conforme a necessidade de segurança das informações neles contidas.

8.4.1 A incorporação de qualquer documento CONFIDENCIAL a um processo elevará o processo ao mesmo nível do documento mais restritivo, até decisão em contrário, mediante reavaliação formal.

8.4.2 O acesso a processos classificados como RESTRITOS ou CONFIDENCIAIS será concedido exclusivamente a pessoas autorizadas, por aprovação formal do proprietário da informação/gestor da área, em ambiente controlado vedado fotografar, copiar ou extrair conteúdo sem autorização; quando se tratar de processos digitais, o acesso deverá ser realizado por meio de perfis e trilhas de auditoria (*logs*).

8.5 Documentos inservíveis contendo informação classificada serão descartados por meios seguros (p. ex., fragmentação), observada a tabela de temporalidade e os requisitos de proteção de registros.

8.6 É obrigatória a prática de mesa limpa e tela limpa, evitando a exposição indevida de documentos e informações da PREVIRB na ausência do responsável, independente do seu nível de classificação.

8.7 Na utilização dos equipamentos de propriedade da PREVIRB, os usuários deverão adotar cuidados que preservem a integridade física dos ativos e a segurança das informações neles tratadas, evitando ações que possam causar danos, mau funcionamento ou exposição indevida de dados.

8.8 O uso das impressoras é exclusivo para trabalhos que sejam de interesse da PREVIRB, devendo as impressões serem realizadas em preto e branco, exceto quando o trabalho exija variação de cores, e retiradas imediatamente do equipamento após impressão.

8.8.1 Não é permitido o abandono de documentos em impressoras ou bandejas de rejeição, devendo estes ser devidamente destruídos pelo usuário responsável pela emissão.

8.9 Assuntos confidenciais não devem ser tratados em locais públicos ou na presença de pessoas não autorizadas, em observância a proteção de dados pessoais e informações estratégicas.

8.10 Os celulares corporativos deverão possuir mecanismos de bloqueio por senha e/ou biometria, criptografia de armazenamento, bloqueio automático de tela e atualizações de segurança ativas, sendo vedada qualquer alteração que comprometa tais controles.

8.10.1 O acesso a informações e sistemas corporativos deverá ocorrer exclusivamente por aplicativos e soluções homologadas, sendo proibido o armazenamento de informações institucionais em aplicativos, contas ou serviços pessoais.

8.10.2 Em caso de perda, roubo, extravio ou suspeita de comprometimento do dispositivo, o fato deverá ser comunicado imediatamente à área de tecnologia da informação, para adoção das medidas cabíveis.

9 TREINAMENTO

9.1 O Programa de Treinamento da PREVIRB deverá contemplar cursos sobre os temas abordados nesta Política, tendo como objetivo sensibilizar seus colaboradores, administradores e terceiros, em nível de detalhamento compatível com as funções desempenhadas e com a criticidade das informações acessadas, abrangendo temas como princípios de segurança da informação, boas práticas de uso dos recursos tecnológicos, responsabilidades individuais na manutenção dos controles internos, preservação da confidencialidade, integridade e disponibilidade das informações, além da necessidade de identificação, prevenção e comunicação imediata de incidentes de segurança, acessos não autorizados, compartilhamentos indevidos ou qualquer suspeita de violação das diretrizes desta Política.

9.2 No momento da contratação, integração ou assunção de cargo, colaboradores, administradores e terceiros deverão assinar o Termo de Conhecimento e Responsabilidade com a Política de Segurança da Informação, reconhecendo suas obrigações e responsabilidades no uso adequado dos recursos corporativos, no tratamento seguro das informações às quais tiverem acesso e no cumprimento integral das normas aqui estabelecidas, renovando os termos sempre que forem processadas alterações no conteúdo desta Política.

9.3 Esta Política deverá ser amplamente divulgada ao público, no mínimo anualmente, e sempre que sofrer atualizações ou quando houver necessidade de reforçar a cultura organizacional de segurança da informação.

10 DISPOSIÇÕES FINAIS

10.1 Os gestores da PREVIRB são responsáveis por divulgar, viabilizar e acompanhar o cumprimento desta Política em suas equipes e processos.

10.2 Esta política entra em vigor na data de aprovação permanecendo válida até que haja sua revogação ou inclusão de novas disposições, devendo, preferencialmente, ser revisada a cada 3 (três) anos, sem prejuízo de revisões extraordinárias em caso de alterações relevantes na legislação, na estrutura organizacional ou nos processos da PREVIRB.

10.3 A revisão ordinária é de responsabilidade do COMTI (Comitê de Tecnologia da Informação), que proporá as eventuais alterações à DIREX, cabendo a aprovação ao CONDEL (Conselho Deliberativo).

10.4 Exceções deverão ser justificadas, avaliadas quanto ao risco, aprovadas e registradas para fins de auditoria.

10.5 O envio não autorizado de arquivos, o descumprimento das regras de armazenamento, classificação, acesso e compartilhamento ou qualquer violação desta Política sujeitará o responsável às medidas disciplinares e contratuais cabíveis, sem prejuízo das responsabilidades civil, administrativa e penal previstas em normas internas e na legislação vigente.

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

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