LAPAPREVI	**Manual de Segurança da Tecnologia da Informação**	**Versão 1.0** **Março/2025**

1. OBJETIVO DO MANUAL

Este documento tem como principal objetivo a manualização do processo de Segurança da Tecnologia da Informação do Instituto de Previdência dos Servidores Públicos do Município de Lapa, Estado do Paraná.

Atualmente O Instituto LAPAPREVI depende intensamente das informações armazenadas em seus sistemas informatizados, pois todos os colaboradores da Organização trabalham com informações estratégicas e têm, portanto, a obrigação de zelar pela confidencialidade, integridade e disponibilidade das informações colocadas sob sua responsabilidade.

A elaboração de Política de Segurança da Informação é o início do processo de mudança de cultura e assimilação de todos os funcionários e colaboradores, nas atitudes e procedimentos que ela determina.

O objetivo deste Manual é definir as diretrizes que orientarão as normas, procedimentos e padrões que tratam da segurança da informação quanto aos aspectos de confidencialidade, disponibilidade e integridade, abrangendo sua geração, utilização, armazenamento, recuperação, distribuição e destruição.

2. DOCUMENTOS COMPLEMENTARES

- Lei de criação do instituto: Lei nº 1577/2001 – Autarquia;
- Segregação de massa: Lei nº 2183/2008 e suas alterações;
- Regulamenta PSI LAPAPREVI: Portaria n° 266/2022;
- Lei Federal n° 12527/2011
- Lei Federal nº 13709/2018;
- Decreto Municipal nº 25.408 de 25/08/2021;
- Norma ABNT NBR ISO/IEC 27002:2005.

3. RESPONSABILIDADES

As responsabilidades pelo uso das informações e recursos informatizados do Instituto LAPAPREVI estão definidas por níveis de acesso para cada camada funcional:

- Dos Colaboradores em Geral;
- Dos Colaboradores em Regime de Exceção (Temporários);
- Dos Gestores de Pessoas e/ou Processos;
- Dos Custodiantes da Informação.

3.1 RESPONSABILIDADES ESPECÍFICAS

a) Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada por regime da CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao Instituto LAPAPREVI e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

b) Dos Colaboradores em Regime de Exceção (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no aceite concedido pela Diretoria Executiva.

A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

c) Dos Gestores de Pessoas e/ou Processos

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

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do Instituto LAPAPREVI.

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

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

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

d) Dos Custodiantes da Informação e da Área de Segurança 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 colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.

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

usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

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.

Garantir segurança especial para sistemas com acesso público, fazendo guarda de evidências que permitam a rastreabilidade para fins de auditoria ou investigação.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

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

Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela Diretoria Executiva, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, para que tenha a alternativa de alterá-lo antes que a informação seja definitivamente descartada pelo custodiante.

Quando ocorrer movimentação interna dos ativos de TI, 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 de negócio.

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 servidor/funcionário.

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

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.

Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro do Instituto LAPAPREVI.

Realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

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

Garantir que todos os servidores, estações e demais dispositivos com acesso à rede do Instituto operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.

Monitorar o ambiente de TI, gerando indicadores e históricos de:

• Uso da capacidade instalada da rede e dos equipamentos; tempo de resposta no acesso à internet e aos sistemas críticos;

• Períodos de indisponibilidade no acesso à internet e aos sistemas críticos;

• Incidentes de segurança (vírus, trojans, furtos, acessos indevidos);

• atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros).

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.

Propor e apoiar iniciativas que visem à segurança dos ativos de informação do Instituto LAPAPREVI.

Publicar e promover as versões da PSI e as Normas de Segurança da Informação aprovadas pelo Conselho de Administração.

Promover a conscientização dos colaboradores em relação à relevância da segurança da informação, mediante campanhas, palestras, treinamentos e outros meios de *endomarketing*.

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

4. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, O Instituto LAPAPREVI 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 - 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, solicitação do Diretor Presidente ou Membro da Diretoria Executiva;

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

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

5. CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores do Instituto LAPAPREVI quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do Instituto LAPAPREVI é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o Instituto LAPAPREVI e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do Instituto LAPAPREVI:

• Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo do Instituto;

• Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou 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 e/ou o Instituto LAPAPREVI vulnerável a ações civis ou criminais;

• Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;

• 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 Instituto LAPAPREVI estiver sujeito a algum tipo de investigação.

• Produzir, transmitir ou divulgar mensagem que:

a) Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Instituto LAPAPREVI;

b) Contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; 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;

c) Vise obter acesso não autorizado a outro computador, servidor ou rede;

d) Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

e) Vise burlar qualquer sistema de segurança;

f) Vise vigiar secretamente ou assediar outro usuário;

g) Vise acessar informações confidenciais sem explícita autorização do proprietário;

h) Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;

i) Inclua imagens criptografadas ou de qualquer forma mascaradas;

j) Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet);

k) Tenha conteúdo considerado impróprio, obsceno ou ilegal;

l) Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

m) Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; tenha fins políticos locais ou do país (propaganda política);

n) Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

• Nome do colaborador

• Gerência ou departamento

• Nome da empresa

• Telefone(s)

• Correio eletrônico

6. INTERNET

Todas as regras atuais do Instituto LAPAPREVI visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa do instituto 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 Instituto LAPAPREVI, 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 do Instituto, 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 Instituto LAPAPREVI, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, 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 o Instituto cooperará ativamente com as autoridades competentes.

A internet disponibilizada pelo Instituto aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos no Instituto.

Como é do interesse do Instituto LAPAPREVI que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome do Instituto LAPAPREVI para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pelo Instituto poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, 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 ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o *download* (baixa) somente de programas ligados diretamente às suas atividades no Instituto LAPAPREVI e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Diretoria Executiva.

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 Diretoria Executiva.

Os colaboradores não poderão em hipótese alguma utilizar os recursos do Instituto LAPAPREVI 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.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao Instituto LAPAPREVI ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos do Instituto LAPAPREVI 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. Já os serviços de streaming (rádios on-line, canais de broadcast e afins) serão permitidos a grupos específicos após análise da Diretoria Executiva. Porém, os serviços de comunicação instantânea (MSN, ICQ e afins) serão inicialmente disponibilizados a usuários que se fizerem necessários mediante execução de suas atividades com autorização prévia do respectivo gestor. Não é permitido acesso a sites de proxy.

7. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o Instituto LAPAPREVI 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 colaboradores.

Todos os dispositivos de identificação utilizados no Instituto LAPAPREVI, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira. O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante o Instituto 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 Instituto LAPAPREVI 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 Diretoria Executiva do Instituto LAPAPREVI é a responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Diretoria Executiva responde pela criação da identidade lógica dos colaboradores no Instituto, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários.

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.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

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 anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como "abcdefgh", "87654321", entre outras.

Após 3 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Diretoria Executiva. Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).

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.

A periodicidade máxima para troca das senhas é 45 (quarenta e cinco) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a

instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 90 (noventa) dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

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

Portanto, assim que algum usuário for demitido ou solicitar demissão, a Diretoria Executiva deverá imediatamente deverá tomar providências quanto a exclusão do referido usuário. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

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

8. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade do Instituto LAPAPREVI, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse do Instituto, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pela Diretoria responsável.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da Diretoria Executiva, ou de quem esta determinar. Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar a Diretoria Executiva mediante registro de chamado no *servicedesk.*

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 ao negócio do Instituto LAPAPREVI (fotos, músicas, vídeos, etc..) 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 por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores do Instituto 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 colaboradores do Instituto LAPAPREVI 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 Diretoria Executiva.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

• Todos os computadores de uso individual deverão ter senha de Bios para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Diretoria Executiva do Instituto LAPAPREVI, que terá acesso a elas para manutenção dos equipamentos;

• Os colaboradores devem informar à Diretoria Executiva 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 por um técnico do Instituto LAPAPREVI 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 da Diretoria Executiva;

• É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos;

• O colaborador deverá manter a configuração do equipamento disponibilizado pelo Instituto, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações;

• Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Norma de

Autenticação, todos os terminais de computador e impressoras quando não estiverem sendo utilizados;

• Todos os recursos tecnológicos adquiridos pelo Instituto LAPAPREVI devem ter imediatamente suas senhas padrões (default) alteradas;

• Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso;

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos do Instituto LAPAPREVI:

• 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.

9. DISPOSITIVOS MÓVEIS

O Instituto LAPAPREVI deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade do Instituto, ou aprovado e permitido por sua Diretoria Executiva, como: notebooks, smartphones e pendrives.

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

O Instituto LAPAPREVI, 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 colaborador, 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 Instituto LAPAPREVI, mesmo depois de terminado o vínculo contratual mantido com o Instituto.

Todo colaborador 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 carregá-los juntos.

O suporte técnico aos dispositivos móveis de propriedade do Instituto LAPAPREVI e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pelo Instituto.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. 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 e a autorização da área responsável e sem a condução da Diretoria Executiva.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados pela Diretoria Executiva do Instituto LAPAPREVI.

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pelo Instituto 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 colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo Instituto LAPAPREVI, notificar imediatamente seu gestor direto e a Diretoria

Executiva. Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador 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 Instituto LAPAPREVI e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do Instituto LAPAPREVI deverá submeter previamente tais equipamentos ao processo de autorização da Diretoria Executiva.

Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

10. BACKUP

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

Os colaboradores 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).

As mídias de *backup* devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com 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 prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de *backup* nos termos do Procedimento de Controle de Mídias de *Backup*.

As mídias de *backups* históricos ou especiais deverão ser armazenadas em instalações seguras.

Os *backups* imprescindíveis, críticos, para o bom funcionamento dos negócios do Instituto LAPAPREVI, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

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 nos termos do Procedimento de Controle de *Backup* e *Restore*.

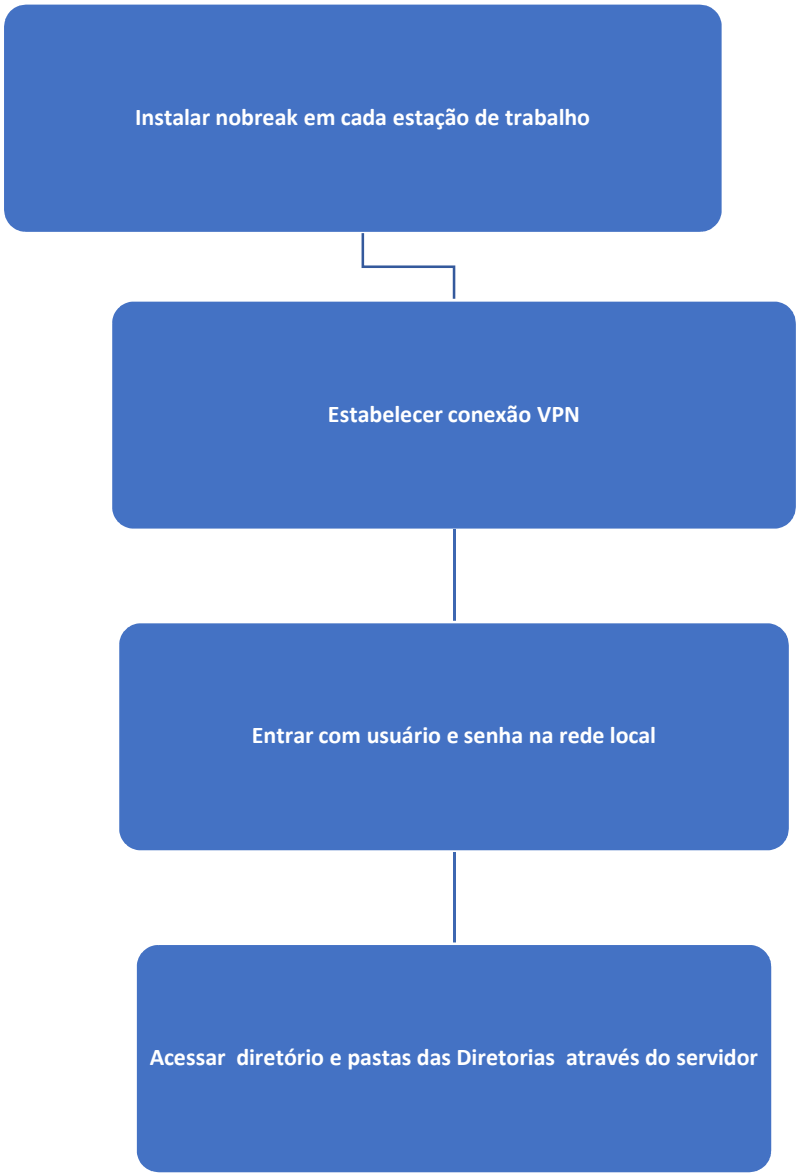
Quaisquer atrasos na execução de *backup* ou *restore* deverão ser justificados formalmente pelos responsáveis nos termos do Procedimento de Controle de Mídias de *Backup*. Testes de restauração (*restore*) de *backup* devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de *backups* e *restores*, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pelo coordenador de infraestrutura, nos termos do Procedimento de Controle de *Backup* e *Restore*.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

11. DAS DISPOSIÇÕES FINAIS

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

FLUXOGRAMA
SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO