RESOLUÇÃO N.º 03, DE 25 DE JULHO DE 2019

Institui a Política de Segurança da Informação no âmbito do VALIPREV – Instituto de Previdência Social dos Servidores Municipais de Valinhos na forma que especifica.

EDMILSON VANDERLEI BARBARINI, Presidente do CONSELHO DE ADMINISTRAÇÃO do VALIPREV - Instituto de Previdência Social dos Servidores Municipais de Valinhos, usando das atribuições que lhe são conferidas pelo art. 153, XIV, da Lei n° 4.877/2013, e

CONSIDERANDO que a informação é um ativo essencial da organização e precisa ser protegida quanto a eventuais ameaças, preservando e minimizando os riscos para a continuidade dos serviços prestados pelo RPPS;

CONSIDERANDO que a adoção de procedimentos que garantam a segurança das informações deve ser prioridade constante do RPPS, reduzindo os riscos de falhas, danos e prejuízos que possam comprometer os objetivos da instituição;

CONSIDERANDO o disposto no Manual do PRÓ-GESTÃO, aprovado pela Portaria da Secretaria da Previdência nº 3, de 31 de janeiro de 2018;

CONSIDERANDO a deliberação do Conselho Administrativo na reunião ordinária realizada em 25 de julho de 2019; e

CONSIDERANDO os elementos constantes nos autos do processo administrativo VALIPREV n° 277/2019

R E S O L V E:

Art. 1º. Fica instituída a Política de Segurança da Informação no âmbito do VALIPREV - Instituto de Previdência Social dos Servidores Municipais de Valinhos, na forma do anexo único da presente Resolução.

Art. 2º. Esta Resolução entra em vigor na data de sua publicação.

Valinhos, 25 de julho de 2019.

EDMILSON VANDERLEI BARBARINI
Presidente do Conselho de Administração

ANEXO ÚNICO – RESOLUÇÃO Nº 03/2019

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO VALIPREV

CAPÍTULO I - DAS DISPOSIÇÕES INICIAIS

Art. 1º. A Política de Segurança da Informação no âmbito do VALIPREV - norteará a implantação de medidas de proteção que deverão ser aplicadas a toda e qualquer informação do Instituto de Previdência Social dos Servidores Municipais de Valinhos, independentemente de sua localização, forma ou conteúdo, visando o resguardo da imagem e dos objetivos institucionais da entidade.

§ 1°. As disposições da Política de Segurança da Informação do VALIPREV devem ser cumpridas por todos os integrantes do Instituto, em todos os níveis hierárquicos, para que o maior patrimônio da entidade, qual seja, a informação, tenha o grau de autenticidade, disponibilidade, confidencialidade e integridade exigidos.

§ 2°. A Política de Segurança da Informação do VALIPREV foi elaborada com fundamento nas seguintes normas:

I. Resolução MPS/CGPC Nº 13, de 01 de outubro de 2004, que "estabelece princípios, regras e práticas de governança, gestão e controles internos a serem observados pelas entidades fechadas de previdência complementar – EFPC";

II. Norma NBR ISO/IEC 27001: Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Requisitos, 28 de agosto de 2006;

III. Norma NBR ISO/IEC 27002: Tecnologia da Informação – Técnicas de Segurança – Código de prática para a gestão da segurança da informação, 10 de setembro de 2007;

IV. Norma aprovada pelo Conselho Deliberativo da Fundação de Previdência Complementar do Servidor Público Federal do Poder Judiciário na 9ª Sessão Ordinária, de 6 de setembro de 2016, disponível em http://www.funprespjud.com.br/wp-content/uploads/2017/01/Politica-de-Seguranca-da-Informacao-Funpresp-Jud_2016.pdf.

Art. 2°. O escopo desta Política de Segurança da Informação do VALIPREV abrange todo o Instituto de Previdência dos Servidores Municipais de Valinhos, de ora em diante denominado, puro e simplesmente VALIPREV.

Art. 3°. A Política de Segurança da Informação e os documentos que a compõem aplicam-se aos servidores, conselheiros e dirigentes do Instituto, bem como a estagiários, aprendizes, fornecedores e parceiros, doravante denominados usuários.

CAPÍTULO II - DOS OBJETIVOS

Art. 4°. A Política de Segurança da Informação do VALIPREV pretende estabelecer diretrizes que permitam ao Instituto a proteção de seus ativos de informação com eficiência e eficácia, de modo seguro e transparente, garantindo a disponibilidade, integridade, autenticidade, legalidade e sigilo, de forma alinhada aos requisitos legais e exigências dos órgãos regulatórios existentes.

Parágrafo único. Para alcançar os objetivos propostos, a Política de Segurança da Informação do VALIPREV apresenta os seguintes tópicos:

I. Diretrizes Gerais;
II. Responsabilidades;
III. Autenticação;
IV. Uso dos Ativos de Tecnologia;
V. Mobilidade;
VI. Acesso Remoto;
VII. Uso do Correio Eletrônico (EMAIL);
VIII. Uso da Internet;
IX. Mídias Sociais;
X. Segurança Física;
XI. Telefonia;
XII. Processo Disciplinar;
XIII. Referências.

CAPÍTULO III – DAS DIRETRIZES GERAIS

Art. 5°. São estabelecidos como princípios da Política de Segurança da Informação do VALIPREV, visando nortear a implementação de regras, procedimentos e ferramentas complementares necessárias ao seu cumprimento:

I. Alterações: o VALIPREV deve garantir que as alterações da Política de Segurança da Informação sejam comunicadas aos seus usuários, sendo responsabilidade de cada usuário a consulta esporádica e voluntária para identificar possíveis atualizações dos instrumentos;

II. Ambientes Lógicos: o VALIPREV deve garantir que os ambientes dos sistemas e processos que suportam os seus ativos sejam confiáveis, íntegros e disponíveis, a quem deles necessite para execução de suas atividades profissionais;

III. Confidencialidade: o VALIPREV deve garantir que a informação, quando necessário, esteja acessível apenas a determinados usuários e/ou processos e seja protegida do conhecimento e/ou acesso alheio, salvo por determinação legal;

IV. Conformidade: o VALIPREV deve instituir e manter um programa de revisão e atualização de sua Política de Segurança da Informação, visando a garantia de que todos os requisitos de segurança implementados estejam sendo cumpridos;

V. Controle de Acesso: o VALIPREV deve controlar o acesso aos seus ativos, devendo garantir que cada usuário possua uma credencial de uso individual, intransferível e de conhecimento exclusivo, além de orientar seus usuários sobre a responsabilidade quanto ao uso e sigilo, além de coibir o compartilhamento de credenciais, sob qualquer hipótese;

VI. Disponibilidade: o VALIPREV deve garantir que a informação e/ou ativo esteja acessível sempre que necessário, mediante autorização para seu acesso e/ou uso;

VII. Integridade: o VALIPREV deve garantir que a informação esteja correta, verdadeira e que não tenha perdido suas características originais;

VIII. Monitoramento: o VALIPREV deve comunicar os seus usuários sobre o monitoramento, inclusive de forma remota, de todo acesso a seus ativos, além de seus ambientes, físicos e lógicos, para verificação da eficácia dos controles implantados, proteção de seu patrimônio e reputação, rastreando eventos críticos e evidenciando possíveis incidentes;

IX. Propriedade: As informações geradas, acessadas, manuseadas, armazenadas ou descartadas por um usuário no exercício de suas atividades, bem como os ativos disponibilizados, são de propriedade e/ou direito de uso exclusivo do VALIPREV e devem ser empregados unicamente para fins profissionais, limitado às atribuições de cargo e/ou função desempenhadas pelo usuário, que deve cumpri-las de acordo com o padrão de conduta ética estabelecido pelo VALIPREV;

X. Sigilo: o VALIPREV deve orientar seus usuários para não revelar, publicar ou divulgar quaisquer informações de propriedade ou sob a responsabilidade do Instituto sem prévia autorização, salvo com autorização legal;

XI. Terceirização, Prestação de Serviços e Cooperação: todos os relacionamentos e contratações em que haja o compartilhamento de informações do VALIPREV e/ou a concessão de qualquer tipo de acesso aos seus ambientes e ativos devem ser precedidos por cláusulas de Confidencialidade, quando aplicável;

XII. Transparência: o VALIPREV deve assegurar uma gestão transparente da informação por meio de medidas efetivas que proporcionem o acesso e a sua divulgação da informação de acordo com a legislação vigente;

XIII. Utilização dos Recursos: o VALIPREV deve assegurar que seus ativos sejam utilizados de modo licito e ético.

Art. 6°. Os usuários devem adotar comportamento seguro e consciente, com o objetivo de preservar e proteger as informações de propriedade e/ou responsabilidade do VALIPREV, com destaque para as diretrizes abaixo:

I. Não divulgar informações privilegiadas e/ou sigilosas sem autorização prévia;

II. Evitar modificação, despersonalização ou perda da informação;

III. Evitar o descarte inseguro das informações;

IV. Não armazenar, transmitir ou compartilhar conteúdo indevido ou ilegal nos ativos de propriedade e/ou responsabilidade do VALIPREV;

V. Não acessar, sem a devida autorização, a estrutura lógica, física e demais ativos compartilhados do VALIPREV;

VI. Não utilizar de forma indevida os ativos de propriedade e/ou responsabilidade do VALIPREV.

Art. 7°. Toda informação gerada ou custodiada pelo VALIPREV deve ser preservada de acordo com a necessidade de serviço ou determinação legal.

CAPÍTULO IV – DAS COMPETÊNCIAS

Art. 8°. Compete às unidades administrativas do VALIPREV:

I. analisar criticamente e de forma periódica a Política de Segurança da Informação, avaliando seu conteúdo e recomendando os aprimoramentos necessários;

II. divulgar, oferecer orientação e gerenciar o cumprimento da Política de Segurança da Informação para os seus respectivos usuários;

III. fiscalizar as regras de proteção dos equipamentos de infraestrutura estabelecidas pela Política de Segurança da Informação;

IV. controlar o acesso e os privilégios de seus usuários internos e remotos;

V. garantir a correta aplicação dos níveis de acessos indicados pelos gestores;

VI. autorizar a aquisição, instalação, remoção, homologação, monitoramento, dos ativos existentes ou em interação com os ambientes e informações do VALIPREV, sejam eles físicos ou lógicos (*hardware* e *software*), realizando verificações e inspeções;

VII. monitorar o tráfego de informações e sistemas, a utilização dos ativos e dispositivos de armazenamento sob sua responsabilidade, com o propósito de verificar o cumprimento dos padrões de segurança, sempre que for necessário e sem aviso prévio;

VIII. disponibilizar e controlar a conexão de ativos de terceiros na rede corporativa do VALIPREV;

IX. gerenciar o padrão de acessos mínimos para criação de conta na rede e aplicações do VALIPREV;

X. propor e manter políticas, regulamentos, processos e procedimentos referentes ao uso de ativos de tecnologia, regras de licenciamento e direitos de propriedade de *softwares* do VALIPREV;

XI. analisar e avaliar as ocorrências de violações e demais eventos negativos relativos à segurança da informação tratados no VALIPREV, acionando a área responsável pelo ativo ou outras áreas impactadas/responsáveis quando necessário.

Art. 9°. Compete aos usuários:

I. cumprir a Política de Segurança da Informação, através do uso de forma responsável, profissional, ética e legal dos ativos, respeitando os direitos e as permissões de uso concedidas pelo VALIPREV, limitados às atribuições de cargo e/ou função;

II. buscar orientação junto aos superiores hierárquicos em caso de dúvidas relacionadas à Política de Segurança da Informação;

III. comunicar ao gestor imediato qualquer irregularidade ou desvio das regras da Política de Segurança da Informação, podendo sugerir medidas preventivas e corretivas.

CAPÍTULO V – DA AUTENTICAÇÃO

Art. 10. Os usuários do VALIPREV, mediante autorização prévia da Diretoria do Instituto, receberão credenciais de acessos aos ativos da Entidade.

Art. 11. As credenciais de acessos estão ligadas a um ativo e definem os direitos de acesso de cada usuário, de acordo com o cargo ocupado, função desempenhada, período de acesso e área em que esteja realizando suas atividades.

Art. 12. Um mesmo usuário pode acessar um número diferenciado de ativos, possuindo credenciais correspondentes, cada qual com os direitos de acesso necessários para o desempenho suas atividades.

Art. 13. O administrador dos sistemas deve fornecer uma senha temporária juntamente com a credencial do usuário, de forma a possibilitar o primeiro acesso a determinado ativo.

§ 1°. O usuário deve efetuar a alteração de sua senha temporária, imediatamente após o primeiro acesso ao ativo ou após solicitar a redefinição de senha.

§ 2°. O usuário deve criar uma senha segura e de qualidade e deve evitar a utilização de nomes, datas especiais e sequências óbvias de números e letras.

§ 3°. A senha criada pelo usuário é pessoal, sigilosa e intransferível. O usuário é responsável pela segurança e integridade, evitando sua anotação em suportes físicos ou transmissão pela rede.

Art. 14. O usuário deve solicitar o bloqueio de sua senha ou da senha temporária, caso venha a tomar conhecimento ou haja suspeita de que o sigilo de qualquer das senhas foi comprometido.

Art. 15. O acesso por parte do usuário a qualquer dos dispositivos poderá ser bloqueado e registrada a operação, após tentativas frustradas de acesso.

Art. 16. O usuário deve solicitar o fornecimento de nova senha temporária, em caso de esquecimento ou bloqueio de sua senha.

Art. 17. Para fins de segurança o usuário deve modificar as suas senhas a cada 180 dias, ou quando entender conveniente, não sendo recomendável, independentemente do processo automático do recurso, a reutilização das duas últimas senhas.

Art. 18. Apenas o usuário ou gestor imediato podem requisitar, formalmente, a redefinição da senha, acionando os administradores dos sistemas.

Art. 19. Nas férias, dispensas e licenças de quaisquer espécies em que o usuário deva abster-se do uso de suas credenciais de acesso aos sistemas do VALIPREV, inclusive acesso remoto, a inatividade deve ser formalmente comunicada aos administradores dos sistemas, visando o bloqueio das credenciais de acessos até o prazo em que durar o período de inatividade do usuário, salvo em casos autorizados pelo Instituto.

Art. 20. O cancelamento das credenciais de acessos do usuário deve ser formalmente comunicado aos administradores dos sistemas.

Art. 21. A responsabilidade de acesso aos ativos de infraestrutura e servidores do VALIPREV, manutenção dos registros de todas as alterações e configurações, é exclusivo da área de Tecnologia da Informação do Instituto.

Art. 22. Os roteadores e firewalls do VALIPREV, os filtros de conteúdo e as regras de acesso devem ser estudados para cada caso e implementados quando necessário, cabendo ao responsável pela área de TI a melhor definição em conjunto com os Diretores do Instituto.

Parágrafo único. Podem ser utilizados aplicativos de gerenciamento para os ativos de infraestrutura e servidores do VALIPREV, que visam notificar o responsável pela TI em casos de anomalias ou mau funcionamento do ativo.

Art. 23. O VALIPREV deve utilizar credencial de acesso segregada para acessar os ativos de infraestrutura e servidores em modo de administração, além de habilitar somente os protocolos necessários para realizar esta atividade, quando em ambiente externo.

Art. 24. Todo acesso realizado em um ativo do VALIPREV deverá ser registrado e armazenado de forma segura e protegida de acessos não autorizados, para fins de auditoria, quando permitido pelo sistema e/ou ativo.

Art. 25. Os privilégios de uso e acesso aos recursos do VALIPREV são atrelados ao cargo, função ou atividade que o usuário exerce no ato da concessão de acesso, podendo ser revistos a qualquer tempo.

CAPÍTULO VI – DO USO DOS ATIVOS DE TECNOLOGIA

Art. 26. Os ativos de tecnologia do VALIPREV são destinados para finalidades profissionais e restritas às atividades do usuário, podendo ser utilizados para fins pessoais com a aplicação de critérios de razoabilidade e responsabilidade.

Art. 27. Todo conteúdo produzido através dos ativos, bem como qualquer programa desenvolvido por seus usuários, é de propriedade do VALIPREV.

Art. 28. Todo e qualquer processo de manutenção, instalação, configuração, desinstalação, substituição ou remanejamento de qualquer ativo, ainda que parcial, deve ser realizado pelo responsável pela área de TI.

Art. 29. O usuário deve utilizar apenas programas, aplicativos, recursos, ferramentas ou *plugins* homologados, sejam eles gratuitos, livres ou licenciados.

Art. 30. Todo usuário ao receber ou utilizar um ativo deve verificar o seu estado de conservação, sendo responsável por utilizá-lo com zelo e cuidado.

Art. 31. Todo usuário deve bloquear sua estação de trabalho ao ausentar-se por tempo prolongado de seu posto de trabalho.

Art. 32. A gestão e guarda dos suportes físicos (mídias) e a instalação de qualquer recurso, seja *software* ou *hardware*, de todos os ativos é atribuição do responsável pela área de TI do VALIPREV.

Art. 33. O usuário, independentemente do cargo ou função que ocupe, ou da área em que esteja alocado, está impedido de:

I. proceder o manuseio de qualquer ativo pertencente ao VALIPREV visando a realização de qualquer tipo de reparo;
II. utilizar dispositivos de comunicação (*modens,* celulares e similares) de origem externa nos ativos do VALIPREV, exceto nos casos previamente autorizados;
III. desinstalar programas, aplicativos, recursos, ferramentas ou *plugins* do VALIPREV, sem a prévia autorização e acompanhamento do responsável;
IV. remover das dependências do VALIPREV qualquer ativo de propriedade do Instituto, sem a prévia autorização do responsável;
V. visualizar, acessar, baixar (efetuar *download*), utilizar, instalar, armazenar, divulgar,

repassar, subir (efetuar *upload*) e transpor para mídia física (imprimir, gravar em CD, DVD, *pendrive* etc.) qualquer material, conteúdo, serviço ou recurso que não seja compatível com as atribuições e objetivos do VALIPREV, na seguinte conformidade:

a. que desrespeite os direitos de propriedade intelectual do Instituto ou de terceiros, incluindo a proteção de suas marcas e patentes;
b. com fins de propaganda política local, nacional ou internacional;
c. programas de compartilhamento de arquivos;
d. programas ou *plugins* de camuflagem de navegação, deleção de histórico de navegação, de desvio de *proxy* e/ou tunelamento de navegação;
e. programas de comunicação instantânea não autorizados;
f. programas, aplicativos, recursos, ferramentas, arquivos ou *plugins* de origem duvidosa, pirata e/ou não homologados previamente;
g. utilizar ativos de propriedade particular com a finalidade de burlar as restrições estabelecidas na Política de Segurança da Informação.

Art. 34. Quando ocorrer o desligamento do usuário, as informações armazenadas nos ativos em sua posse devem ser analisadas pelo seu gestor imediato para determinar quem será o novo responsável pelas informações.

§ 1°. O ativo que se encontra sob a responsabilidade do usuário deve ser restituído ao VALIPREV.

§ 2°. Todos os ativos devolvidos devem ser submetidos a um processo de avaliação técnica de estado de conservação pelo responsável da área de TI.

CAPÍTULO VII – DA MOBILIDADE

Art. 35. Os dispositivos móveis pessoais que não façam parte dos ativos do VALIPREV somente devem ser conectados à rede corporativa através da rede sem fios, utilizando acesso específico para este fim, o qual deve ser obtido junto ao responsável pela área de TI.

Art. 36. O VALIPREV é o proprietário das informações geradas no ambiente interno e daquelas desenvolvidas através de atividades remotas realizadas para o Instituto, salvo exceções previamente definidas.

Art. 37. A concessão de uso de dispositivos de mobilidade deve ser realizada de modo a atender aos objetivos do VALIPREV, limitada às atribuições, cargo e/ou funções do usuário, podendo ser revogada a qualquer tempo.

§ 1°. O usuário não deve alterar qualquer configuração nos dispositivos móveis de propriedade do VALIPREV, em especial os referentes à segurança, criptografia de dados, acesso ou registros realizados pela área de TI.

§ 2°. Quando o dispositivo móvel for fornecido pelo VALIPREV, periodicamente, haverá a necessidade de atualização das rotinas de segurança dos mesmos.

§ 3°. A instalação e/ou configuração dos dispositivos deve ser somente realizada pelos técnicos designados pelo VALIPREV, sendo de responsabilidade do usuário a má utilização do ativo.

Art. 38. O usuário deve informar imediatamente ao VALIPREV quando ocorrer avaria, dano ou defeito no dispositivo de mobilidade em uso.

Art. 39. No caso da ocorrência de furto ou roubo do dispositivo de propriedade do VALIPREV, o usuário deve comunicar imediatamente o Instituto e lavrar Boletim de Ocorrência, encaminhando uma cópia ao Instituto.

Art. 40. O usuário deve devolver imediatamente e em perfeitas condições de uso e funcionamento o referido dispositivo no caso de rescisão ou término de sua prestação de serviço ao VALIPREV.

CAPÍTULO VIII – DO ACESSO REMOTO

Art. 41. A concessão de acesso remoto deve ser expressamente autorizada pelo VALIPREV, através de justificativa técnica do responsável pela área de TI, podendo ser revogada a qualquer tempo.

Art. 42. A concessão de uso de acesso remoto deve ser realizada de modo a atender aos objetivos do Instituto, limitada às atribuições, cargo e/ou funções do usuário.

Art. 43. O usuário que utiliza os recursos de acesso remoto ao ambiente corporativo do VALIPREV deve proteger suas credenciais de acessos e realizar o encerramento da sessão ao término de suas atividades.

Art. 44. O usuário deve utilizar os serviços de acesso remoto em ambientes seguros de conexão, especialmente quando estiver em deslocamento, podendo ainda fazer uso de mecanismos de criptografia homologados pelo VALIPREV.

Art. 45. Os usuários estão cientes de que o VALIPREV monitora todo acesso e uso de suas informações, bem como de seus ambientes, por perímetro físico e/ou lógico, visando a proteção de seu patrimônio e reputação, bem como daqueles que se relacionam com o Instituto.

Art. 46. O VALIPREV pode desabilitar ou restringir as condições de acesso remoto de qualquer usuário que descumprir as disposições da Política de Segurança da Informação ou demonstrar incapacidade ou negligência no uso desta facilidade tecnológica.

CAPÍTULO IX – DO USO DO CORREIO ELETRÔNICO

Art. 47. O recurso de correio eletrônico corporativo do VALIPREV é destinado para finalidades profissionais e restrito às atividades do usuário.

Parágrafo único. Os endereços de correio eletrônico corporativos e o conteúdo das caixas postais disponibilizadas aos usuários são de propriedade do VALIPREV.

Art. 48. A concessão da caixa de e-mail corporativa ao usuário é efetuada por seu superior hierárquico.

Art. 49. A critério do VALIPREV, o acesso remoto ao e-mail corporativo poderá ser autorizado.

Art. 50. O acesso à caixa postal corporativa é realizado através de senha de caráter pessoal e intransferível, sendo vedado ao usuário fornecê-la para terceiros ou anotá-la em suportes físicos.

Art. 51. A caixa postal corporativa possui um limite máximo pré-definido pelo VALIPREV para o armazenamento das mensagens.

§ 1°. O usuário deve efetuar, periodicamente, a limpeza de sua caixa postal corporativa, com a exclusão das mensagens desnecessárias, para não exceder o limite de armazenamento.

§ 2°. O VALIPREV auxiliará o usuário na gestão e arquivamento das mensagens, com o propósito de garantir o *backup* das informações necessárias.

Art. 52. Os usuários podem realizar a sincronização de sua respectiva caixa postal corporativa em seus dispositivos pessoais, mediante autorização prévia do VALIPREV.

Art. 53. No uso do correio eletrônico corporativo, é vedado ao usuário:

I. enviar mensagem cujo conteúdo possa gerar, de forma direta ou indireta, riscos à imagem do VALIPREV;
II. enviar mensagem a partir de endereço diferente do seu próprio, ou se fazendo passar por outra pessoa;
III. utilizar endereço de correio eletrônico corporativo que o usuário não esteja autorizado;
IV. abrir mensagens consideradas suspeitas ou caracterizadas como *spam* e *phishing scam*;
V. produzir, armazenar, transmitir ou divulgar mensagem que:
    a. não seja compatível com a missão, visão e valores do VALIPREV;
    b. represente uma quebra da confidencialidade de informações relacionadas ao VALIPREV ou aos terceiros com as quais mantenham relação;
    c. seja ofensiva ao VALIPREV ou terceiros;
    d. caracterize invasão da privacidade e/ou intimidade de terceiros;
    e. onstitua violação de direitos de propriedade intelectual do VALIPREV ou de

terceiros;

f. incorpore *software* malicioso.

Art. 54. O bloqueio da caixa postal do usuário deve ser realizado quando da ocorrência do seu desligamento ou do encerramento de seu contrato junto ao VALIPREV, sendo realizado pelo responsável pela área de TI do Instituto.

CAPÍTULO X – DO USO DA INTERNET

Art. 55. O ativo corporativo de acesso à internet do VALIPREV é destinado para finalidades profissionais e restritas às atividades do usuário, podendo ser utilizados para fins pessoais com a aplicação de critérios de razoabilidade e responsabilidade.

Parágrafo único**.** Os Termos e Condições de Uso e a Política de Privacidade dos *sites* acessados devem ser lidos antes de qualquer inscrição ou atividade.

Art. 56. Não é permitido aos usuários no uso dos ativos corporativos de acesso à internet visualizar, utilizar, armazenar, divulgar, repassar e imprimir qualquer material, conteúdo, serviço ou recurso que não sejam compatíveis com as atividades do VALIPREV, precipuamente:

I. com fins de propaganda política local, nacional ou internacional;

II. com arquivos executáveis, com a extensão .exe, ou equivalentes, não autorizados previamente pelo VALIPREV;

III. *sites* constantes na lista de proibidos pelo VALIPREV, incluindo-se os *sites* contendo pornografia, pedofilia, incitação ao terrorismo ou qualquer outro conteúdo que atente contra as leis vigentes e a ordem pública;

IV. com jogos *on-line* ou *stand-alone* (sem conexão de Internet);

V. programas:

a. de compartilhamento de arquivos (tais como *BitTorrent*, por exemplo);

b. ou *plugins* de camuflagem de navegação, deleção de histórico de navegação, de desvio de *Proxy* e/ou tunelamento de navegação;

c. de comunicação instantânea não autorizados;

d. aplicativos, recursos, ferramentas, arquivos ou *plugins* de origem duvidosa,

pirata e/ou não homologados previamente pelo VALIPREV;

VI. efetuar *upload* indevido de qualquer conteúdo de propriedade do VALIPREV;

VII. obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades em sistemas internos ou externos do VALIPREV;

VIII. tentar indevidamente obstruir, desativar ou alterar os controles de segurança e os parâmetros estabelecidos nos ativos pelo VALIPREV;

IX. tentar interferir em um serviço, sobrecarregá-lo ou desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos do VALIPREV.

Art. 57. A ausência de bloqueio de um *site* pelo VALIPREV não valida seu acesso, devendo ser observadas as restrições estabelecidas pela Política de Segurança da Informação.

Art. 58. O usuário pode solicitar formalmente a liberação de acesso a um *site* bloqueado cujo conteúdo esteja em conformidade com a Política de Segurança da Informação do VALIPREV, mediante justificativa.

CAPÍTULO XI – DAS MÍDIAS SOCIAIS

Art. 59. O acesso e o uso de mídias sociais a partir da conexão corporativa do VALIPREV é passível de restrição em caso de uso indevido ou sem a aplicação de critérios de razoabilidade.

Art. 60. O acesso às mídias sociais para fins profissionais deverá ser previamente autorizado pelo VALIPREV.

Art. 61. Caso o usuário detecte algum conteúdo publicado que afete diretamente a imagem do VALIPREV, o fato deverá ser comunicado ao Instituto.

Art. 62. Os usuários que possuem o acesso corporativo autorizado às mídias sociais devem fazer o seu uso apenas no âmbito de suas competências e atividades profissionais.

Art. 63. Os usuários que não possuem o acesso corporativo autorizado às mídias sociais, estão impedidos de publicar:

I. conteúdo ou opinião nas mídias sociais em nome do VALIPREV;
II. conteúdo sobre o VALIPREV, parceiros, fornecedores e servidores, com exceção das informações de conhecimento público;
III. conteúdos audiovisuais, como fotos, imagens, vídeos ou áudios relacionados ao âmbito interno do VALIPREV, exceto quando autorizados formalmente ou no caso de informações de conhecimento público;
IV. assuntos profissionais internos ou específicos do VALIPREV ligados à atividade exercida ou que estejam protegidos por sigilo profissional;

Parágrafo único. Os usuários referidos no *caput* devem evitar publicar conteúdo durante o período de suas atividades no VALIPREV.

CAPÍTULO XII – DA SEGURANÇA FÍSICA

Art. 64. O VALIPREV fornecerá as autorizações de acesso às instalações de TI ao responsável pela administração do campo de informática do Instituto.

Parágrafo único. O acesso ao *datacenter* do VALIPREV é restrito aos seus servidores e terceiros autorizados.

Art. 65. É responsabilidade do Departamento competente monitorar e controlar os serviços residentes no *datacenter* do Instituto e autorizar o acesso físico às suas instalações.

Art. 66. O VALIPREV instalará câmeras e gravará imagens de todos os ambientes que compõe sua sede, inclusive das áreas externas.

§ 1°. O acesso às gravações das imagens internas e externas do Instituto será exclusivo da Diretoria Executiva, mediante justificativa fundamentada.

§ 2°. As gravações efetuadas serão retidas pelo prazo mínimo de quinze dias.

CAPÍTULO XIII – DA TELEFONIA

Art. 67. O sistema de telefonia do VALIPREV visa proporcionar segurança, agilidade e transparência nas ligações realizadas e recebidas.

Art. 68. O usuário é responsável pelas ligações efetuadas a partir de seu ramal em seu horário de expediente, considerando que o sistema de telefonia é destinado ao uso exclusivamente profissional.

CAPÍTULO XIV – DO DESCUMPRIMENTO

Art. 69. O descumprimento desta Política de Segurança da Informação poderá implicar em ações disciplinares, nos termos da legislação pertinente, bem como em sanções previstas nas normas internas do VALIPREV ou no contrato de prestação de serviços com terceiros.