Tipo do Documento	Código	Página	Versão
POLÍTICA	**PLUMAS-001**	**1 de 25**	**1.2**

Título:

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Este é um documento inicial para análise e aprovação do comitê gestor de Privacidade.

Política de Segurança da Informação-2021

Versão	Data	Descrição da Alteração	Elaboração	Verificação
0.0	**19/10/2021**	**Documento Original**	**Kaue Gomes**	
1.0	**26/10/2021**	**Análise de Documento Original**	**Kaue Gomes**	**Comitê Gestor**
1.1	**05/11/2021**	**PSI Aprovada**	**Kaue Gomes**	**Comitê Gestor**
1.2	**09/11/2021**	**Realizada Alteração nas Diretrizes**	**Kaue Gomes**	**Comitê Gestor**
1.3				

Índice

1. INTRODUÇÃO

1.1 A Política de Segurança da Informação, também reconhecida como PSI, é um documento que orienta e estabelece as diretrizes corporativas da PLUMAS, matriz e filiais, para a proteção dos seus ativos de informação e a prevenção de responsabilidades legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da empresa.

1.2 Esta Política de Segurança da Informação visa preservar a confidencialidade, a integridade e a disponibilidade da informação. É aprovado e divulgado pelo Comitê Gestor de Privacidade, que fomentam e apoiam os objetivos e diretrizes de segurança aqui estabelecidos.

1.3 Este documento é público e está disponível no sítio eletrônico da PLUMAS (www.plumascontabil.com.br), na Intranet Local (interna) e encaminhado via correio eletrônico a todos os colaboradores.

2. OBJETIVOS

2.1 Estabelecer diretrizes e orientar a definição de mecanismos de segurança que garantam o cuidado, a legalidade, a credibilidade e imagem da PLUMAS na prestação de seus serviços e que preservem a continuidade de seus negócios.

2.2 Permitir aos colaboradores, prestadores de serviço e clientes da PLUMAS seguirem padrões de comportamento relacionados à Segurança da Informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

2.3 Preservar os dados e documentos da PLUMAS quanto à:

- **Integridade:** garantia de se manter os dados e documentos em seu estado original, protegendo-o, na guarda e transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso aos dados e documentos seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso aos dados, documentos e aos ativos correspondentes sempre que necessário.

3. ABRANGÊNCIA E VALIDADE

3.1 Esta política aplica-se a todos os colaboradores de todos os departamentos, bem como à Diretoria e Gerência da PLUMAS, prestadores de serviços, fornecedores, parceiros e quaisquer outras partes envolvidas com a PLUMAS.

3.2 Esta política dá ciência a todos os colaboradores de que os ambientes, sistemas, computadores e rede da empresa poderão ser monitorados e gravados, com prévio aviso, conforme previsto nas leis brasileiras.

3.3 É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos, processo e normas relacionadas do seu gestor de departamento ou do Comitê de Privacidade da PLUMAS sempre que achar necessário ou que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de dados e documentos.

3.4 Esta política se aplica a todas as unidades, Matriz e filiais, da PLUMAS e tem prazo de validade indeterminado. Portanto, sua vigência se estenderá até a edição de outro documento de Política de Segurança da Informação que o atualize ou revogue.

4. REQUISITOS

4.1 Esta PSI deverá ser comunicada a todos os colaboradores da PLUMAS, Matriz e filiais, a fim de que a política seja cumprida dentro e fora da empresa.

4.2 Deverá haver um comitê responsável por gerir a Segurança da informação e esse comitê foi designado e nomeado como Comitê de Privacidade.

4.3 Este documento bem como as normas internas deverão ser periodicamente revistos e atualizados, e deverá acontecer sempre que for relatado um incidente de segurança conforme análise do Comitê de Privacidade e aprovação por meio do Comitê Gestor.

4.4 Todos são responsáveis em relação a Segurança da Informação e deve ser comunicado na fase de contratação dos colaboradores por meio da integração realizada no primeiro dia de trabalho. Todos devem ser orientados dos procedimentos de segurança, bem como uso correto dos ativos, a fim de reduzir possíveis riscos e ameaças. Todos devem assinar um termo de responsabilidade e confidencialidade.

4.5 Todo incidente que afete a segurança da informação deverá inicialmente ser comunicado ao Comitê de Privacidade, que fará uma análise inicial e irá encaminhar ao DPO. Este irá fazer as tratativas necessárias e comunicará ao Comitê Gestor.

4.6 A PLUMAS não se responsabiliza pelo uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas em processos investigatórios, bem como adotar as medidas legais cabíveis.

4.7 Esta PSI é implementada na PLUMAS por procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

4.8 O não cumprimento dos requisitos previstos nesta PSI acarretará violação das regras internas da empresa e sujeitará o usuário às medidas administrativas e legais cabíveis.

5. CONCEITOS E DEFINIÇÕES

5.1 Os conceitos e definições constantes neste item se aplicam de forma a auxiliar a interpretação da Política de Segurança da Informação da PLUMAS e para estabelecer futuras normas complementares.

5.2 A informação é um ativo essencial para os negócios da PLUMAS e consequentemente necessita ter uma proteção adequada, em especial nos ambientes de internet onde é crescente o número e a variedade de ameaças e vulnerabilidades.

5.3 Para os fins dessa política, considera-se:

5.3.1 **Ameaça:** Qualquer coisa que possa explorar uma vulnerabilidade, intencional ou acidentalmente, e obter, danificar ou destruir um ativo.

5.3.2 **Vulnerabilidade:** Qualquer fragilidade dos sistemas de computadores ou de qualquer ativo da informação que permita a exploração maliciosa e acessos indesejáveis ou não autorizados.

5.3.3 **Ativos:** Qualquer coisa que tenha valor para a empresa.

5.3.4 **Ativos da Informação:** Qualquer informação que tenha valor pela empresa seja físico, natural ou digital.

5.3.5 **Responsável pela Informação:** Gestor da área onde a informação é gerada. Define o nível de classificação da informação. (Também é conhecido como proprietário dos ativos ou proprietário da informação de acordo com a ABNT NBR ISO/IEC 27002:2005).

5.3.6 **Incidente de Segurança:** Qualquer evento não planejado que pode acarretar prejuízos a empresa ou mesmo violar as regras de segurança.

5.3.7 **Colaboradores:** Diretores, gerentes, gestores, empregados, estagiários, fornecedores, terceirizados ou quaisquer outras pessoas que sejam usuários de informações.

5.3.8 **Usuário:** Pessoa que acessa ou utiliza de forma legítima e autorizada sistemas e informações.

5.3.9 **Prestadores de serviços:** Pessoas que prestam serviço e podem possuir acesso às instalações e recursos de informação da PLUMAS.

5.3.10 **Áreas sensíveis:** São áreas ou setores que concentram uma quantidade considerável de informações estratégicas para o negócio.

5.3.11 **Confidencialidade:** Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.

5.3.12 **Integridade:** Garantia da exatidão, completeza da informação e dos métodos de processamento.

5.3.13 **Disponibilidade:** Garantia de que os usuários autorizados obtenham acesso a informações e aos ativos do qual tem permissões.

6. AUDITORIA E CONFORMIDADE

6.1 A área de Tecnologia da Informação (TI) deverá manter registros e procedimentos, por meio de auditorias e monitoramento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, rede interna e ativos da PLUMAS.

6.2 Auditar significa conferir a cultura de conformidade e o grau de comprometimento dos profissionais, sendo uma atividade independente, de avaliação objetiva e de consultoria, destinada a acrescentar valor e melhorar as operações da PLUMAS. Além disso, consiste na avaliação da eficácia da gestão de riscos, do controle e dos processos de Governança de TI.

6.3 A auditoria efetua verificação de forma aleatória e temporal por meio de amostragens para certificar-se do cumprimento das diretrizes e processos instituídos pelo Comitê Gestor.

6.4 A conformidade é um conjunto de regras para fazer cumprir as diretrizes, processos e procedimentos estabelecidos para o negócio e para as atividades da PLUMAS, bem como evitar, detectar e tratar qualquer não conformidade que venha a ocorrer.

6.5 Ao usuário de informações não é dado o direito de desconhecimento da PSI, sendo um dever seguir rigorosamente as regras dispostas e aqui definidas.

6.6 Esta política deve ser comunicada e amplamente divulgado internamente na empresa para que todos a conheçam e a pratiquem.

6.7 O usuário que não cumprir as políticas e normas de segurança aqui descritos, estará sujeito a sanções internas e, nos casos cabíveis, às leis vigentes.

7. MONITORAMENTO

7.1 Visando garantir as diretrizes, processos e procedimentos mencionados nesta PSI, a PLUMAS poderá realizar o monitoramento de seus ativos.

7.2 A PLUMAS poderá implantar sistemas de monitoramento nas estações de trabalho, servidores, e-mail, conexões com a internet e outros componentes de rede. As informações geradas por esses equipamentos e sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como identificar toda e qualquer atividade realizada internamente em seu ambiente.

7.3 Poderá tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação dos Gestores (ou superior) ou por determinação do Comitê Gestor e do Comitê de Privacidade.

7.4 Poderá realizar, em qualquer momento e sem prévio aviso, inspeção física ou lógica nos equipamentos de sua propriedade.

7.5 A PLUMAS poderá instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações, acessos e dos ativos.

8. DEVERES E RESPONSABILIDADES

8.1 Dos Colaboradores

8.1.1 Entende-se por colaborador toda e qualquer pessoa física, contratada CLT pela PLUMAS, que exerça alguma atividade dentro ou fora da empresa.

8.1.2 Será de inteira responsabilidade de cada colaborador , todo prejuízo ou dano causado a PLUMAS e/ou a terceiros , em decorrência da não obediência às diretrizes e normas aqui referidas, sob pena de receber sanções disciplinares e legais cabíveis.

8.1.3 Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os equipamentos de informática disponibilizados para a realização do seu trabalho.

8.1.4 Utilizar recursos e sistemas de informações da PLUMAS somente para fins profissionais e todas as informações transitadas internamente ou externamente devem ser feitas através dessas ferramentas corporativas, sendo proibido o uso de ferramentas particulares sob pena de receber sanções disciplinares e legais cabíveis.

8.1.5 É dever e responsabilidade do colaborador comunicar por e-mail ao seu Gestor imediato (superior), o conhecimento de qualquer irregularidade, desvio ou incidente encontrado.

8.2 Dos Diretores, Gerentes e Gestores

8.2.1 Ter postura exemplar em relação a Segurança da Informação, servindo de modelo de conduta para os colaboradores sob sua gestão, atribuindo a eles a responsabilidade do cumprimento dessa PSI, fazendo com que sigam as normas estabelecidas e mantenham sigilo e confidencialidade sobre todos os ativos de informações da PLUMAS.

8.2.2 Identificar as irregularidades, desvios ou incidentes encontrados e adotar as medidas corretivas apropriadas, bem como comunicar ao Comitê de Privacidade e ao DPO da PLUMAS essas situações.

8.2.3 Impedir o acesso de empregados demitidos aos ativos da empresa.

8.2.4 Zelar e garantir, em nível físico e lógico, que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger as informações, os ativos de informação e de processamento de dados da PLUMAS relacionados a sua área de atuação.

8.2.5 Comunicar formalmente ao setor de TI (Tecnologia da Informação) da PLUMAS, que efetua a concessão de privilégios a usuários, que acessos e permissões devem ter os colaboradores sob sua supervisão.

8.2.6 Comunicar formalmente ao setor de TI (Tecnologia da Informação) da PLUMAS, que efetua a concessão de privilégios a usuários, quais os colaboradores demitidos ou transferidos, para exclusão de permissões no cadastro de usuários.

8.2.7 Comunicar formalmente ao setor de TI (Tecnologia da Informação) da PLUMAS, que efetua a concessão de privilégios a usuários, aqueles que estejam licenciados, independente do motivo, para inabilitação no cadastro dos usuários.

8.3 Dos Prestadores de Serviço

8.3.1 Devem estar previstas nos contratos, cláusulas que contemplem a responsabilidade dos prestadores de serviços no cumprimento desta Política de Segurança da Informação, suas normas e procedimentos.

8.4 Da Área de Tecnologia da Informação (TI)

8.4.1 Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança estabelecidos por esta PSI.

8.4.2 Aos colaboradores da área de TI é permitido acessar os arquivos e dados de outros usuários, desde que para execução de suas atividades operacionais sob suas responsabilidades quando necessário como, por exemplo, a manutenção de

computadores, sistemas e ferramentas, realização de backups, auditorias ou testes no ambiente.

8.4.3 Administrar, proteger e testar os backups dos programas, sistemas e dados relacionados ao negócio relevante para a PLUMAS.

8.4.4 Quando ocorrer movimentação interna de ativos de TI, garantir que as informações de um usuário não sejam repassadas para outro usuário, e que não sejam removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

8.4.5 Atribuir a cada conta ou dispositivo de acesso a computadores, sistemas, base de dados ou qualquer outro ativo de informação a um responsável único, sendo que os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

8.4.6 Proteger todos os ativos da empresa continuamente contra código malicioso e que somente sejam colocados em produção após realizar testes e estarem livres de código malicioso ou indesejado.

8.4.7 Definir regras formais para instalação de softwares e hardwares em ambiente de produção da empresa, exigindo o seu cumprimento, além de realizar auditorias periódicas de configurações técnicas e análises de riscos.

8.4.8 Garantir, de forma mais rápida possível, com solicitação formal, o bloqueio de acesso de colaboradores que forem desligados, incidentes, investigação ou qualquer outra medida restritiva com o objetivo de cuidar dos ativos.

8.4.9 Garantir que todos os equipamentos de informática operem com os horários sincronizados com o horário padrão do governo brasileiro, que estejam sempre atualizados garantindo assim uma maior segurança.

8.4.10 Monitorar o ambiente de TI, mantendo inventário atualizado gerando indicadores e históricos de:

8.4.10.1 Cada ativo dentro da rede e suas configurações e capacidade (HD, memória, processador etc.).

8.4.10.2 Permissões e acessos de usuários por departamento ou setor na rede ou em qualquer outro sistema.

8.4.10.3 Incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e outros).

8.4.10.4 Atividade de todos os colaboradores durante os acessos a internet (Sites visitados, e-mails, upload/download de arquivos e outros).

8.5 Da Área de Segurança da Informação e DPO

8.5.1 Propor e apoiar iniciativas, metodologias e processos específicos que visem a segurança dos ativos de informação, avaliação de riscos e classificação da informação.

8.5.2 Publicar e promover as versões desta PSI e as Normas de Segurança da Informação aprovadas pelo Comitê Gestor.

8.5.3 Promover a conscientização de todos os colaboradores da PLUMAS, terceiros e fornecedores, em relação à segurança da informação por meio de campanhas, palestras, treinamentos ou outros meios de endomarketing.

8.5.4 Analisar criticamente incidentes que venham a ocorrer em conjunto com o Comitê de Privacidade e Comitê Gestor.

8.5.5 Realizar, apresentar e guardar atas e resumos de reuniões realizadas com o Comitê de Privacidade e Comitê Gestor, destacando os assuntos que exijam intervenção destes Comitês.

8.5.6 Buscar um alinhamento com as diretrizes corporativas e dessa PSI, além de manter uma comunicação constante com o Comitê de Privacidade sobre assuntos que afetem ou possam afetar a PLUMAS.

8.6 Do Comitê de Privacidade (CP)

8.6.1 Deverá ser formalmente constituído por colaboradores com nível hierárquico mínimo gerencial, ou que tenham poder de decisão, nomeados para participar do grupo pelo período mínimo de 1 ano.

8.6.2 Esse Comitê deverá ser composto por um colaborador de cada setor ou departamento da empresa, que são: Consultores, Contabilidade, Comercial, Financeiro, Legalização, Marketing, Pessoal, RH, Sped Fiscal, TI e Triagem.

8.6.3 Deverá o CP reunir-se formalmente pelo menos uma vez a cada 4 meses. Reuniões adicionais devem ser realizadas sempre que for necessário deliberar sobre algum incidente grave ou relevante a PLUMAS.

8.6.4 As atribuições do CP são:

8.6.4.1 Garantir que os processos de cada setor ou departamento estão sendo aplicados e seguidos por todos os colaboradores.

8.6.4.2 Garantir que as diretrizes de Segurança da Informação, internas, relacionado a LGPD e outras Normas estejam em conformidade, sendo aplicadas e seguidas por todos.

8.6.4.3 Avaliar os incidentes de segurança da informação e propor ações corretivas. Informar ao DPO por e-mail todo e qualquer incidente.

8.6.4.4 Definir as medidas cabíveis nos casos de descumprimento da PSI, processos e/ou Normas de Segurança da Informação.

8.6.4.5 Propor alterações nas versões da PSI e a inclusão, eliminação ou a mudança de processos ou normas.

8.6.4.6 Propor investimentos relacionados a segurança da informação com o objetivo de reduzir os riscos.

9. DIRETRIZES

9.1 Toda informação acessada ou gerada pelos colaboradores, seja utilizando parcialmente ou integralmente, os recursos da PLUMAS, é exclusivamente de propriedade da PLUMAS.

9.2 É proibido o compartilhamento de informações sem autorização, bem como tudo aquilo que não esteja previamente autorizado por essa PSI ou por quaisquer outros documentos normativos internos.

9.3 Devem ser prevenidas todas as possibilidades de vazamento de informações da PLUMAS.

9.4 Toda informação deve ser classificada e a divulgação dela deverá ser feita por meio das áreas especificas, seguindo suas atribuições e com autorização do Gestor da área e, somente com quem tem permissão de acessar a informação.

9.5 A classificação deve ser feita quanto a confidencialidade e identificadas de forma a serem adequadamente armazenadas, copiadas, transmitidas, manuseadas, descartadas ou destruídas.

9.6 Os colaboradores devem acessar os recursos da empresa seguindo os princípios de segurança e os processos definidos sem afetar ou causar danos a outrem.

9.7 O eventual descumprimento desta PSI deve ser comunicado imediatamente ao Gestor da área para aplicar as medidas disciplinares cabíveis.

9.8 Os controles internos devem ser constantemente reavaliados e aprimorados, principalmente em relação ao risco de Segurança das Informações, com procedimentos apropriados nos processos de cada área.

9.9 Todos os processos internos e informações devem estar mapeados e documentados. Precisam ser revisados periodicamente e aplicados, visando elevar o nível de maturidade de segurança da PLUMAS.

9.10 As medidas de proteção aos recursos devem ser aplicadas de forma compatível com o risco e com o valor da informação para os negócios da PLUMAS.

9.11 Todos os ativos de informação devem ser identificados, classificados e permanentemente atualizados pelo responsável pela informação.

9.12 Deve haver um processo definido que visa conscientizar os colaboradores sobre a necessidade da segurança da informação e os aspectos previstos nesta PSI, pois todos os colaboradores devem estar devidamente capacitados quanto a correta e eficiente utilização dos recursos, de acordo com as normas em vigor.

9.13 Um plano de continuidade do negócio com o objetivo de manter funcionando a empresa com todos os processos e serviços críticos, na ocorrência de desastres, atentados e falhas, deve ser mantido atualizado e documentado.

9.14 Os procedimentos de backup e recuperação devem ser documentados, mantidos atualizados e regularmente testados, para garantir a disponibilidade das informações.

9.15 No caso de permissões de acessos a recursos, sejam eles físicos ou lógicos, precisa ser observado o princípio do menor privilégio, ou seja, conceder acessos somente os estritamente necessários ao desempenho das atividades autorizadas.

9.16 Os colaboradores devem ter acesso físico e logico, liberado somente aos recursos e informações necessários e indispensáveis ao desemprenho de suas atividades e em conformidade com os interesses da PLUMAS.

9.17 O acesso às áreas restritas deve ser resguardado, por meio do uso de dispositivos de controle de acesso e utilização de câmeras de monitoramento.

9.18 As câmeras de monitoramento devem gravar as imagens para posterior análise do pessoal responsável ou através de solicitação formal dos gestores.

9.19 O acesso de visitantes, prestadores de serviço e clientes às dependências da PLUMAS deve ser registrado através de controle de acesso de visitantes.

9.20 As imagens devem ser armazenadas de maneira segura e protegida.

9.21 Os registros (informações, arquivos, documentos, imagens) devem ser protegidos e armazenados de forma segura, com o período de armazenamento definido pela área específica, através de comunicação formal e aprovada pelo Gestor.

9.22 Todos os computadores, servidores, sistemas e demais ativos, devem ser monitorados, verificando sua normalidade, assim como detectar situações anômalas em questão de segurança.

9.23 Os horários dos computadores e servidores devem estar sincronizados para permitir o rastreamento de eventos.

9.24 Mídias e informações que não forem mais necessárias devem ser eliminadas de forma segura. Documentos físicos devem ser descartados de forma correta, utilizando as processadoras de papeis de cada setor, obrigatoriamente.

9.25 Uma política de mesa e tela limpa deve ser implementada para reduzir os riscos de acesso não autorizados ou danos a documentos/papeis, mídia e sistemas.

9.26 A comunicação interna e externa deve ser clara e objetiva, contemplando todas as partes interessadas, mas sem expor informações confidenciais e/ou estratégicas. Somente deve ser feito por mecanismos corporativos.

9.27 Acordos de confidencialidade devem ser firmados para garantir a confidencialidade das informações da PLUMAS.

9.28 Controle de Acesso

9.28.1 Todas as contas de acesso aos ativos de informações da PLUMAS deverão ser revogadas ou suspensas quando não mais necessárias.

9.28.2 Todo acesso às informações e aos ambientes lógicos da PLUMAS deve ser controlado, garantindo acesso apenas aos colaboradores autorizados pelo respectivo proprietário da informação, da seguinte forma:

9.28.2.1 **Controle de Acesso Lógico:** Permite que sistemas de TI verifiquem a identidade dos usuários que tentam utilizar os serviços. Acesso de acordo com cada setor ou departamento. Acesso a informações somente as que tem necessidade de acesso.

9.28.2.2 **Controle de Acesso Físico:** Por questões de segurança, é obrigatório o uso de Token de acesso para áreas restritas ou por meio de senha disponibilizada por pessoa autorizada.

9.28.3 As senhas de qualquer ativo ou sistema é pessoal e intransferível, e é de responsabilidade de cada usuário em caso de incidentes. O compartilhamento é proibido em quaisquer circunstâncias.

9.28.4 Em casos de desligamento de funcionários, os acessos são removidos e as informações serão disponibilizadas por meio de solicitação formal autorizada pelo Gestor do setor ou departamento. É proibido o uso de um ativo ou login de acesso de outro colaborador na ausência dele, exceto pela mesma autorização do Gestor, mencionada anteriormente.

9.29 Uso de E-mail

9.29.1 O e-mail é um recurso de comunicação corporativa da PLUMAS. As regras de acesso e utilização de e-mail devem atender a todas as orientações desta PSI e demais normas internas.

9.29.2 O uso é destinado apenas para fins corporativos e relacionados às atividades do colaborador dentro da empresa. A utilização desse serviço para fins pessoais é proibida.

9.29.3 É **PROIBIDO** aos colaboradores o uso do e-mail das seguintes maneiras:

9.29.3.1 Enviar mensagens em nome de outro colaborador ou usando o e-mail de outra pessoa sem autorização.

9.29.3.2 Enviar mensagens que torne seu remetente ou o domínio da PLUMAS vulneráveis a ações civis ou criminais.

9.29.3.3 Divulgar informações não autorizadas ou imagens de sistemas, documentos e afins sem autorização expressa e forma concedida pelo proprietário desse ativo de informação.

9.29.3.4 Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar punições previstas.

9.29.3.5 Produzir, transmitir ou divulgar mensagens que contenha qualquer ato ou forneça orientação que conflite com os interesses da PLUMAS.

9.29.3.6 Produzir, transmitir ou divulgar mensagens que contenha ameaças eletrônicas, como: Spam, mail bombing, vírus, phishing, entre outros.

9.29.3.7 Produzir, transmitir ou divulgar mensagens que contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf), contendo certificados digitais (.pfx, .cer, .crc) ou qualquer outra extensão que seja um risco a segurança.

9.29.3.8 Produzir, transmitir ou divulgar mensagens que vise obter acesso não autorizado a outro computador, servidor ou rede, ou que interrompa um serviço por meio de métodos ilícitos e não autorizados.

9.29.3.9 Produzir, transmitir ou divulgar mensagens que vise burlar qualquer sistema de segurança, vigiar secretamente ou assediar outro usuário, acessar informações confidenciais ou acessar indevidamente informações que causem prejuízo a qualquer pessoa.

9.29.3.10 Produzir, transmitir ou divulgar mensagens que inclua imagens criptografadas ou de qualquer forma mascaradas ou que tenham conteúdo considerado improprio, obsceno ou ilegal.

9.29.3.11 Produzir, transmitir ou divulgar mensagens que contenham anexo(s) superior(es) a 15 MB para envio (interno ou externo) e 15 MB para recebimento (internet).

9.29.3.12 Produzir, transmitir ou divulgar mensagens que seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico, com perseguição preconceituosa baseada em sexo, raça, incapacidade física, mental ou outras situações protegidas por lei.

9.29.3.13 Produzir, transmitir ou divulgar mensagens que tenha fins políticos, com propagandas políticas, propagandas diversas, vendas ou materiais protegidos por direitos autorais sem permissão do detentor dos direitos.

9.29.3.14 Usar como chat de conversas.

9.29.4 As mensagens de e-mail sempre deverão conter assinatura com as seguintes informações: Nome do colaborador, Departamento, E-mail, Telefone, Ramal e Nome da empresa.

9.30 Acesso à Internet

9.30.1 Todas as regras de acesso a internet visam um comportamento mínimo esperado de ética e profissionalismo, e é regido por normas internas.

9.30.2 No ambiente corporativo a internet é monitorada e sujeito a auditorias. Por isso, em total conformidade com as leis do país, a PLUMAS se reserva ao direito de monitorar e registrar todos os acessos a ela.

9.30.3 O acesso à internet contém bloqueios a certos sites, sendo liberado apenas os sites e acessos que são necessários para a realização das atividades relacionadas a PLUMAS e suas obrigações legais de prestação de serviços. Caso seja necessário a liberação de algum site que esteja bloqueado, essa solicitação deve ser feita formalmente por meio de normas e processos internos definidos.

9.30.4 O acesso a sites para fins pessoais não é permitido. Mesmo que o site esteja disponível para acesso, o acesso sem autorização está sujeito as penalidades previstas nas normas internas da PLUMAS.

9.30.5 Uso, instalação, cópia ou distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software baixado não autorizado será excluído pelo TI.

9.30.6 Os colaboradores não poderão em hipótese alguma utilizar os recursos da PLUMAS para fazer download ou distribuição de softwares pirateados, atividade ilícita de acordo com as leis nacionais.

9.30.7 As permissões de acesso à internet são definidas por nível hierárquico e/ou por setor ou departamento.

9.30.8 Como regra geral, materiais de cunho sexual não poderão ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso interno ou externo.

9.30.9 Não são permitidos acessos a softwares peer-to-peer (Kazaa, BitTorrent e afins), serviços de comunicação instantânea (Skype, Whatsapp Web, Telegram e afins), sites de proxy e serviços de streaming (Rádios Oline, Youtube e afins) serão permitidos a grupos ou usuários específicos.

9.31 Uso de Redes Sociais

9.31.1 O uso de redes sociais (Instagram, Facebook e afins) pelos recursos da PLUMAS é proibido. Esses conteúdos são bloqueados por padrão. Mesmo que o site esteja

disponível para acesso, o acesso sem autorização está sujeito as penalidades previstas nas normas internas da PLUMAS.

9.32 Uso de dispositivos móveis

9.32.1 A descrição de Dispositivos Móveis entende-se por qualquer equipamento eletrônico como: Notebooks, Smartphones, Tablets, pen-drives e demais equipamentos com atribuições de mobilidade.

9.32.2 O uso de dispositivos móveis é proibido internamente durante o horário de expediente, podendo ser usado apenas nos horários de descanso (Almoço, Café e outros intervalos que o contrato de trabalho tenha definido) ou com aprovação do Gestor do setor ou departamento, com base nos artigos 2º e 444 da CLT que dá ao dono do negócio (empresa), que assume o risco da atividade econômica e tem o poder de dirigir e disciplinar as atividades de seus empregados.

9.32.3 O uso do dispositivo móvel sem consentimento ou de forma indevida pode configurar ato de indisciplina, podendo acarretar ao empregado punições como advertência, suspensão e inclusive a dispensa por justa causa. Somente é liberado o uso durante o período de descanso, mesmo nas dependências da empresa.

9.32.4 No caso de Smartphones, deverão permanecer guardados juntamente com seus pertences pessoais, não poderão ser conectados em nenhum equipamento de TI e em casos emergenciais ou necessários, poderão solicitar uso ao Gestor do setor ou departamento que poderá liberar o uso do Smartphone ou até mesmo da linha fixa da empresa .

9.32.5 O uso de Notebooks e Tablets particulares são proibidos internamente durante o horário de expediente, podendo ser usado apenas nos horários de descanso (Almoço, Café e outros intervalos que o contrato de trabalho tenha definido) ou com aprovação do Gestor do setor ou departamento.

9.32.6 O uso de Pen-drives pessoais é proibido e não podem ser conectados em nenhum equipamento de TI de propriedade da PLUMAS. O não cumprimento dessa regra poderá acarretar medidas disciplinares cabíveis.

9.32.7 Somente será permitido o uso de dispositivos móveis disponibilizados pela PLUMAS a seus colaboradores, ou seja, apenas para uso corporativo e sob autorização do Gestor do setor ou departamento.

9.33 Uso de Computadores

9.33.1 Os equipamentos disponíveis aos colaboradores são de propriedade da PLUMAS, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações do setor de TI e desta PSI.

9.33.2 É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento ou autorização de um técnico do TI da PLUMAS. Ações contraria a essa regra, o colaborador será unicamente responsável.

9.33.3 O usuário, em caso de suspeita de vírus ou problemas na funcionalidade dos equipamentos, deverá acionar o departamento de TI responsável mediante abertura de chamado técnico na Freshdesk.

9.33.4 Arquivos pessoais e/ou não pertinentes ao negócio da PLUMAS (Fotos, Vídeos, Músicas etc.) não devem ser copiados/movidos para os equipamentos ou pastas na rede PLUMAS. Caso identificado a existência desses arquivos, serão excluídos definitivamente sem comunicação prévia.

9.33.5 Documentos imprescindíveis para as atividades da PLUMAS e seus Clientes deverão ser salvos na Rede. Tais arquivos, se gravados apenas localmente nos computadores (C:/), não terão garantia de backup e poderão ser perdidos, sendo, portanto, da responsabilidade do usuário.

9.33.6 No uso de computadores, equipamentos e recursos de TI, deve-se seguir algumas regras descritas abaixo:

9.33.6.1 Cada computador é de uso individual, configurado com um login e senha para cada colaborador, sendo esse login pessoal e intransferível. É responsabilidade do colaborador a privacidade e proteção de seu login.

9.33.6.2 Deverão ser protegidos por senha (bloqueados) todos os computadores quando não estiverem sendo utilizados. O sistema bloqueia automaticamente após 240 segundos (4 minutos) de inatividade.

9.33.6.3 Caso perceba alguma anormalidade em seu computador, deve ser informado imediatamente ao departamento de TI da Plumas, sendo feito formalmente por meio da Freshdesk.

9.33.6.4 É proibido a abertura ou o manuseio de computadores e outros equipamentos de TI para reparos que não seja por um técnico do departamento de TI da PLUMAS.

9.33.6.5 É EXPRESSAMENTE PROIBIDO o consumo de alimentos e bebidas na mesa de trabalho e próximo de equipamentos de TI.

9.33.6.6 O colaborador deverá manter a configuração do equipamento disponibilizado pela PLUMAS, seguindo os controles de segurança informados nessa PSI e sendo responsável por ele.

9.33.6.7 Todos os equipamentos de TI são de propriedade da PLUMAS, podendo ser repassados a outro usuário, removidos e alterados a qualquer momento segundo a necessidade.

9.33.7 Acrescentamos abaixo algumas situações em que é PROIBIDO no uso de computadores e recursos de TI:

9.33.7.1 Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.

9.33.7.2 Burlar quaisquer sistemas de segurança.

9.33.7.3 Acessar informações confidenciais sem explícita autorização para isso.

9.33.7.4 Usar qualquer tipo de recurso de TI para cometer ou ser cúmplice de atos ilícitos, de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular.

9.33.7.5 Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

9.33.7.6 Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

10. PENALIDADES

10.1 O não cumprimento ou violação, por qualquer colaborador, às regras previstas nesta PSI poderá resultar na aplicação das seguintes sanções, com base na CLT:

10.1.1 Advertência Verbal: Tem por objetivo alertar o colaborador de que sua conduta não esteve em consonância com as regras desta PSI. (Será realizada em particular, acompanhado do Gestor da área ou departamento ao qual pertence).

10.1.2 Advertência Escrita: Devem ser realizadas, notadamente, por escrito e em duas vias assinadas (uma a ser entregue ao empregado e outra a ser arquivada pelo empregador). Do mesmo modo que a advertência verbal, deve indicar, de maneira objetiva, o motivo pelo qual o empregado está sendo advertido, ou seja, qual a conduta realizada pelo empregado ensejou a aplicação da advertência.

10.1.3 Suspensão: Trata-se de sanção mais enérgica face a uma falta cometida pelo empregado.

10.1.4 Demissão por Justa Causa: A dispensa com justa causa é o resultado da ineficácia das medidas de advertência ou suspensão anteriormente aplicadas ao empregado. É a penalidade máxima imposta ao trabalhador que, embora tenha recebido medidas corretivas, não demonstrou mudança de comportamento no ambiente de trabalho. Indispensável dizer, portanto, que a justa causa como medida disciplinar é a última medida a ser implementada.

10.2 O colaborador poderá responder disciplinarmente e/ou civilmente pelo prejuízo que vier ocasionar a PLUMAS, podendo culminar com seu desligamento e eventuais processos criminais, se aplicáveis.

11. DISPOSIÇÕES FINAIS

Da mesma forma que a ética, a segurança da informação deve ser entendida como parte fundamental da cultura interna da PLUMAS. Ou seja, qualquer incidente de segurança seria o mesmo que agir contra a ética e os bons costumes da organização.

12. APROVAÇÃO

Esta Política foi aprovada em reunião realizada pelo Comitê Gestor em 05/11/2021, através de Ata Nº 02/2021, e vigora a partir de sua assinatura.

Comitê Gestor - Plumas

COMITÊ GESTOR

FIM DA PSI