Política de Segurança da Informação

Elaborado por:	Verificado por:	Aprovado por:
Gerente de TI	Diretoria Estatutária e Comitê de Auditoria	Conselho de Administração

SUMÁRIO

1.0 – OBJETIVO:

O objetivo desta política de segurança da informação é estabelecer as normas e diretrizes corporativas que permitam aos Usuários da Priner a atuarem de acordo com padrões de comportamento que garantam a segurança das informações circuladas internamente na Companhia, em conformidade com a Lei nº 13.709, de 14 de agosto de 2018 (“Lei Geral de Proteção de Dados” ou “LGPD”) (“Política” ou “Política de Segurança da Informação”).

2.0 – CONSIDERAÇÕES GERAIS:

A presente Política de Segurança da Informação e suas normas são fornecidas a título de orientação aos Usuários quanto a utilização dos serviços e recursos tecnológicos da Companhia, sendo sua implementação e cumprimento obrigatórios.

As normas e procedimentos específicos de segurança da informação, bem como os controles e processos para seu atendimento, tem como base os seguintes princípios:

i) Princípio da Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, no armazenamento ou na transmissão, contra alterações indevidas, intencionais ou acidentais.

ii) Princípio da Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

iii) Princípio da Disponibilidade: garantia de que apenas Usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

Ficam definidos como serviços e recursos da Companhia sujeitos à presente Política de Segurança da Informação todos os equipamentos utilizados pelos funcionários e Usuários do sistema e de sua rede, tais como: computadores, e-mails e domínios utilizados pela Companhia, “priner.com.br”, “prinerrental.com.br”, “smartcoat.com.br”, “isolafacil.com.br”, “poliend.com.br”, “britoekerche.com.br”, “gmaia.com.br”, “soegeo.com.br”, “tresca.com.br”, “labteste.com.br” e “semarndt.com.br”, *links* de internet e afins.

Em caso de quaisquer dúvidas sobre a presente Política ou com o que é considerado, de alguma forma, violação às normas de segurança da informação, o usuário deverá entrar em contato com o profissional de TI responsável pela sua filial, a fim de obter orientações. Caso a dúvida persista, o usuário deverá contatar o DPO (*Data Protection Officer*).

A Companhia procederá com o bloqueio do acesso ou o cancelamento **imediato** do usuário, caso seja detectada violação às normas referentes a segurança da informação ou o uso do sistema em desconformidade com o estabelecido nesta Política.

O departamento de Gente e Gestão ficará responsável por qualquer advertência a ser realizada junto ao colaborador em razão da violação ou descumprimento das normas de segurança da informação constantes nesta Política ou na legislação aplicável.

As normas para utilização, bem como a descrição das possíveis violações ao sistema da Companhia, encontram-se divididas e apresentadas nesta Política em seis tópicos, da seguinte forma:

i. Utilização da rede;
ii. Utilização dos sistemas corporativos;
iii. Utilização de e-mail, Chat e Chamadas de Vídeo;
iv. Utilização de acesso à internet e compartilhamento de arquivos;
v. Cópia de segurança (*backup*); e
vi. Utilização dos equipamentos.

3.0 – TERMOS E DEFINIÇÕES:

TI: Área de Tecnologia da Informação.

Usuários: Colaboradores, estagiários e funcionários terceirizados da Priner.

DPO (*Data Protection Officer*): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

4.0 – DIRETRIZES:

4.1 – Norma de utilização do sistema:

4.1.1 – Utilização da rede:

Esse tópico visa definir as normas de utilização da rede que engloba desde o login, manutenção de arquivos no servidor e tentativas não autorizadas de acesso.

i. As senhas de login e e-mail são obrigatoriamente complexas. Isso significa que uma senha deve satisfazer os seguintes requisitos:

a) Ter no mínimo 10 caracteres;
b) Não ser igual ou similar ao nome do usuário e/ou login;
c) Não pode ser igual as últimas 10 senhas utilizadas anteriormente,
d) Deve possuir 04 dos seguintes tipos de caracteres:

- Maiúsculos;
- Minúsculos;
- Números;
- Símbolos (@, %, *, etc.).

ii. As senhas têm o tempo máximo de expiração de 90 dias.

iii. Após 05 tentativas erradas de acesso, o login é bloqueado automaticamente.

iv. A conta de usuário (também conhecido como “login”) é pessoal e intransferível, ou seja, não é permitido revelar a senha de seu login para outro colaborador.

Visto que cada colaborador é identificado na rede pelo seu login, acessar o computador com o login de outro usuário poderá ser considerada uma atitude suspeita, tendo em vista que o colaborador está assumindo a identidade de outro usuário na rede.

v. Não é permitida tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta. Isso inclui acesso aos dados não disponíveis para o usuário, conectar-se ao servidor ou conta cujo acesso não seja expressamente autorizado ao usuário ou colocar à prova a segurança de outras redes.

vi. Não é permito o acesso a contas de usuário ausentes, de férias ou em licença. Qualquer necessidade de acesso à informação corporativa contida nas contas destes Usuários deverá ser solicitada através do https://helpdesk.priner.com.br/ e autorizado pelo gerente da área a qual o colaborador está alocado.

vii. A senha da rede WI-FI “SI-GUEST” não deve ser divulgada **para Usuários da corporação, mas apenas visitantes ou fornecedores relacionados à empresa.** A senha da rede “SI-CORP” é de uso **exclusivo para Usuários da corporação.**

viii. Não é permitida tentativas de interferir nos serviços de qualquer outro usuário, servidor ou rede. Isso inclui ataques do tipo "negação de acesso", provocar congestionamento em redes, tentativas deliberadas de sobrecarregar um servidor e tentativas de "quebrar" (invadir) um servidor.

ix. Não é permitido o uso de qualquer tipo de programa ou comando designado a interferir com as sessões dos Usuários.

x. Antes de ausentar-se temporariamente de seu computador, o usuário deverá bloquear sua sessão com as teclas “**Windows Key**” **+** “**L**”. Tal prática evitará o acesso a pessoas não autorizadas.

xi. Material de natureza pornográfica, racista, discurso de ódio e de qualquer natureza preconceituosa não pode ser exposto, armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede, ficando o usuário sujeito as penalidades previstas nesta política e na lei vigente do país.

xii. Existe uma diretiva de segurança para impedir a gravação de arquivos de áudio, vídeo, e-mails, executáveis e scripts nas pastas de rede. Caso o usuário identifique a real necessidade de

gravar alguns dos tipos de arquivos mencionados em sua pasta departamental, será necessário registrar um chamado no canal de comunicação disponibilizado pela Companhia, https://helpdesk.priner.com.br/. Desta forma, sua solicitação será analisada a fim de avaliar e, se for viável, possibilitar a forma mais segura possível de disponibilizar o formato de arquivo desejado.

xiii. A pasta "PÚBLICO", **não** deverá ser utilizada para armazenamento de arquivos que contenham assuntos sigilosos ou de natureza sensível, tais como documentos que contenham informações pessoais de funcionários, Usuários ou clientes. Esta pasta poderá ser limpa a qualquer momento, sem aviso prévio.

xiv. Os acessos às pastas departamentais são administrados através de permissões específicas, de modo a restringir acessos não autorizados. Caso seja necessário acesso a uma pasta de rede a qual o usuário não possua autorização, três condições deverão ser satisfeitas:

- O usuário deverá solicitar acesso ao "dono" da pasta desejada através do portal, https://helpdesk.priner.com.br/

  Entende-se por "dono", o usuário que, **por padrão**, possui direito de acesso a uma pasta. Exemplos: (i) Usuários de "Suprimentos" possuem acesso à pasta "GSUP"; (ii) Usuários de "Contas a Pagar" possuem acesso à pasta "CPAG"; e (iii) Usuários de "Segurança do Trabalho" possuem acesso à pasta "SEGT". Ou, o gestor da área.

xv. Quando um colaborador for desligado da empresa, as seguintes ações deverão ser realizadas pelo responsável do departamento ao qual o colaborador pertencia:

a) Registrar um chamado no canal de comunicação da Companhia, https://helpdesk.priner.com.br/ solicitando **o bloqueio de acessos** (login, e-mail e sistemas RM TOTVS e SoftExpert); e

b) Verificar se há a necessidade de solicitar o redirecionamento de e-mails do ex-colaborador para um funcionário do departamento.

⚠ **É responsabilidade do gestor do departamento** reportar ou designar um funcionário para solicitar o bloqueio de acessos junto à TI.

4.1.2 – Utilização dos sistemas corporativos:

Esse tópico visa definir normas para utilização dos sistemas corporativos como o login e tentativas não autorizadas de acesso.

i. O acesso ao sistema RM TOTVS se dá através de duas etapas de autenticação:

a) O primeiro login é necessário para acessar o ambiente.
b) O segundo login é necessário para acessar o sistema RM.

c) Ambos os logins tratam-se de autenticações distintas, porém necessárias.

ii. Quanto à senha dos respectivos logins, elas deverão seguir os mesmos padrões de complexidade descritos no item 4.1.1 desta Política.

iii. Para acesso ao TOTVS é necessário que o usuário esteja associado a um perfil de acesso. Cada perfil possui opções/áreas específicas. Por exemplo: membros do perfil "A" possuem opções que não estão disponíveis no perfil "B" e vice-versa.

iv. A fim de facilitar a compreensão sobre este assunto, seguem alguns exemplos de perfis atualmente disponíveis:

- "Cadastro de Projeto/Contrato", "Cadastro de Compras", "Cadastro Contrato Suprimento", "Cadastro Estoque", "Estoque QSMS", "DRO", "Operação Faturamento", entre outros.

4.1.3 – Utilização de e-mail, chat e chamadas de vídeo:

Esse tópico visa definir as normas de utilização de e-mail, desde o envio, recebimento e gerenciamento das suas contas, as ferramentas de comunicação interna e externa entre os funcionários (chat) e as chamadas de vídeos.

i. A senha de endereço de e-mail do usuário é **pessoal e intransferível**, ou seja, não é permitido revelar a senha para outros Usuários.

ii. É proibido o assédio ou perturbação de outrem, seja através de linguagem utilizada, frequência ou tamanho das mensagens.

iii. É proibido forjar quaisquer das informações do cabeçalho do remetente.

iv. O usuário é responsável pelos anexos recebidos em seus e-mails, ressaltando-se que mesmo que o remetente seja considerado confiável, é possível que o anexo ou o corpo do e-mail enviado por ele sejam suspeitos, pois o computador de origem pode estar "contaminado" ou a conta de e-mail pode ter sido "sequestrada"; sem conhecimento do remetente. Ao se deparar com um anexo suspeito, o usuário deverá entrar em contato com o profissional de TI responsável pela respectiva filial para obter orientações.

v. O usuário deve ficar alerta a quaisquer e-mails com assuntos iguais ou semelhantes aos que constam abaixo:

a) "Receita Federal - Lote residual disponível";
b) "Segue pix feito em sua conta no valor de R$...";
c) "Comunicado Importante: Clientes 'banco do usuário'...";
d) "Pagamento ainda não confirmado";
e) "Seu nome consta no Serasa. Clique aqui para regularizar sua situação";
f) "Não foi possível localizar o destinatário no endereço de entrega".

Os criminosos virtuais utilizam diversas técnicas criativas para atrair e atiçar a curiosidade dos Usuários, de modo que muitos acabam acessando o *link* informado pelo criminoso e consequentemente baixando códigos maliciosos (*malwares*) em seus respectivos computadores ou levando o usuário, através de *links*, a acessar sites falsos, com o objetivo de roubar dados pessoais e sensíveis, tais como números de documentos e cartões de crédito/débito; login e senha; entre outros.

vi. Caso o usuário desconfie de um e-mail/remetente/anexo, deve contatar imediatamente o profissional de TI da filial.

vii. Embora a rede da Companhia possua ferramentas de segurança necessárias ao seu funcionamento seguro (antivírus, firewall, entre outros.), atualmente não existem recursos de proteção infalíveis. Diante deste cenário, cada colaborador deve manter-se atento e agir com cautela, a fim de evitar a disseminação de malwares e links maliciosos para outros Usuários, ligados ou não à organização.

viii. Por conta da integração com o e-mail, a colaboração e o monitoramento, a solução padrão da organização para chat interno e para chamadas de áudio e vídeo é o Microsoft Teams. O Teams também pode ser usado para conversas via chat com pessoas que estão fora da organização, desde que elas possuam uma conta Microsoft ou Corporativa e o Teams instalado.

ix. O recurso padrão para o agendamento de reuniões online (internas e externas) é o Microsoft Teams.

x. O recurso padrão para armazenamento e troca de arquivos é o Microsoft Sharepoint e o Microsoft One Drive.

xi. Embora, no momento, não haja restrições rigorosas ao uso de aplicativos como WhatsApp, Telegram, Slack, entre outros; NÃO é permitido que os Usuários compartilhem arquivos da organização como documentos, fotos, vídeos, entre outros; sigilosos ou não, para pessoas não autorizadas, sejam eles colaboradores, fornecedores, dentre outros. O acesso a estas ferramentas poderão ser suspenso a qualquer momento sem aviso prévio.

xii. Assim como ocorre com o e-mail, fraudadores utilizam técnicas diversas em aplicativos conhecidos do mercado como WhatsApp e Telegram, a fim de propagar *links* para sites maliciosos para obterem dados pessoais e sensíveis dos Usuários, como números de CPF e cartões de crédito/débito; logins e senhas e códigos gerados por *tokens*. Portanto, o usuário deve suspeitar de qualquer pessoa que esteja solicitando seus dados pessoais e/ou sensíveis por meio desses aplicativos, incluindo pessoas conhecidas e de confiança do usuário. Por exemplo: Talvez você esteja conversando com um golpista que “sequestrou” a conta WhatsApp de um contato seu e está se fazendo passar por ele(a)”.

xiii. Caso o usuário desconfie de uma mensagem, seja ela originada de qualquer ferramenta de colaboração *online* ou *chat*, **inclusive o Teams**, deve contatar imediatamente o profissional de TI de sua filial.

xiv. Não é permitido usar chamadas de vídeo para exibir as instalações das filiais, escritórios e dos canteiros das obras realizadas pela organização, exceto em casos comprovadamente necessários e com a autorização do seu líder imediato.

4.1.4 – Utilização de Acesso à Internet e Compartilhamento de Arquivos:

Esse tópico visa definir as normas para utilização da internet que englobam desde a navegação em sites, *downloads/uploads* de arquivos e compartilhamento de arquivos através de ferramentas de colaboração online como o Microsoft Teams, Onedrive, Sharepoint, entre outros.

i. É proibido utilizar recursos da Companhia para fazer *download* ou distribuição de *software* ou dados não legalizados.

ii. É proibida a divulgação de informações confidenciais da Companhia em redes sociais, aplicativos de mensagens ou similares, não importando se a divulgação foi deliberada ou inadvertida, ficando o usuário sujeito as penalidades previstas nas políticas e procedimentos internos da Companhia e/ou na forma da lei.

iii. Os Usuários que violarem as políticas internas da Companhia, relativas as normas de acesso à internet, poderão ser incluídos **no grupo de acesso restrito**, onde apenas sites específicos poderão ser acessados, sites estes totalmente relacionados aos negócios empresariais. A limitação de acesso ao usuário envolvido deverá será solicitada previamente ao departamento de TI pelo gestor do departamento.

iv. Embora existam mecanismos de controle e monitoramento de acesso à internet, ainda assim é possível que tais recursos falhem em um dado momento. No entanto, independentemente dos recursos envolvidos, cada usuário é responsável pelo que acessa na internet.

v. Não é permitido o *upload* (enviar arquivos) de qualquer *software* licenciado à Companhia, de dados de propriedade da companhia e/ou de seus clientes, sem expressa autorização do DPO (Data Protection Officer).

vi. Caso a área de redes julgue necessário, haverá bloqueio de acesso pelos Usuários à:

a) **Sites** que comprometam o desempenho da rede/internet ou perturbem o bom andamento do trabalho; e

b) **Aplicativos** que comprometam o desempenho da rede/internet ou perturbem o bom andamento do trabalho.

vii. Não é permitida a utilização de *softwares* de *peer-to-peer* (P2P), tais como µTorrent e afins.

viii. Não é permitida a utilização de serviços de *streaming*, tais como Netflix, YouTube, Amazon Prime e similares.

Em casos específicos, alguns Usuários necessitam de acesso a sites como 'YouTube' para baixar vídeos educativos destinados ao treinamento de colaboradores. Para tal, será necessário que o usuário registre um chamado no canal de chamado da Companhia, https://helpdesk.priner.com.br/, para que sua solicitação seja avaliada junto ao departamento de TI e/ou DPO (Data Protection Officer).

ix. As ferramentas padrão para colaboração e guarda de arquivos são exclusivamente o Microsoft Teams, Microsoft OneDrive e Microsoft Sharepoint,

x. É **proibida** a divulgação de informações confidenciais da Companhia e/ou de Usuários através das ferramentas de colaboração *online*, não importando se a divulgação foi deliberada ou inadvertida, ficando o usuário sujeito as penalidades previstas nas políticas e procedimentos internos da Companhia e/ou na forma da lei.

xi. Não é permitido o uso de ferramentas de colaboração *online* de terceiros como Google Drive e Dropbox, por exemplo. Não é permitido compartilhar arquivos a partir de ferramentas de colaboração de terceiros.

4.1.5 – Cópia de segurança (Backup):

Esse tópico visa informar sobre as estratégias de cópia de segurança (*backup*) da Companhia, bem como definir as normas de utilização para a sua cópia e restauração.

i. É obrigatório armazenar os arquivos inerentes à Companhia no Sharepoint para garantir o backup (cópia de segurança) dos mesmos.

Os backups objetivam mitigar "desastres". No entanto, existe um cenário comum no qual o procedimento não surtirá efeito.

Exemplo: Se um arquivo foi criado após o backup de 12:00h e o usuário o excluiu acidentalmente antes do backup das 15:30h, a recuperação do arquivo não será possível, pois o arquivo não passou por nenhum processo de cópia, visto que o arquivo passou a existir após o 12:00h e a "inexistir" antes das 15:30h.

ii. A pasta "PÚBLICO" não é contemplada por nenhuma estratégia de backup e, portanto, **nenhum arquivo vital da Companhia** deve ser armazenado neste diretório.

iii. É vedado o uso de unidade de armazenamento externo, tais como: *Pendrives*, HDs externos e cartões de memória. Sendo obrigatório o uso das ferramentas homologadas para *backup* das informações.

4.1.6 – Utilização dos equipamentos:

Esse tópico visa informar sobre as estratégias de utilização dos equipamentos da companhia, visando o melhor aproveitamento dos recursos.

i. Todos os equipamentos são de propriedade da companhia, tais como *softwares* e licenças, todos disponibilizados para os usuários em perfeitas condições de uso.

ii. O conceito de propriedade setorial não existe. Nenhum equipamento é de "propriedade" de usuário ou área de atuação, cabendo apenas a TI direcionar os recursos adequadamente. Desta forma NÃO é permitida a retenção de qualquer equipamento disponível por parte dos setores.

iii. Qualquer alteração nas características dos equipamentos deverá ser solicitada através https://helpdesk.priner.com.br, seja aumento de capacidade de armazenamento, memória e/ou instalação de software, sendo terminantemente proibida qualquer tipo de movimentação destas por parte dos Usuários.

iv. Todos os equipamentos são entregues mediante a assinatura de "Termo de Responsabilidade e Cautela", no qual são indicadas as melhores práticas para uso dos equipamentos. Qualquer dano por mau uso será de responsabilidade do usuário responsável pelo equipamento, ficando o mesmo responsável por arcar com eventuais despesas para reparo.

v. Para Usuários remotos/Offshore, que recebem os equipamentos através de seus supervisores, é concedido prazo de 30 dias para regularização do Termo de Responsabilidade e Cautela. Em caso de não cumprimento deste prazo, o supervisor será responsável por todos os equipamentos em questão.

4.2 – Classificação da informação:

O gestor de cada área deverá estabelecer critérios relativos ao nível de confidencialidade da informação gerada pela área que ele é responsável e deverá classificá-las como Pública, Confidencial, Restrita ou Interna ("Classificação da Informação").

O processo de Classificação da Informação deve iniciar com a definição do grau de proteção necessário, com base nos quatro níveis de sigilo a seguir definidos:

4.2.1 – Confidencial:

Informação sensível que deve ser mantida em confidencialidade e manuseada apenas por pessoas autorizadas. O vazamento de informações com essa classificação gera impacto para a Companhia e o negócio como um todo.

4.2.2 – Restrita:

Informação cujo acesso e manuseio são apenas para pessoas autorizadas. Caso sejam divulgadas erroneamente, afetam a continuidade de um ou mais processos de negócio da Companhia. O vazamento de informações com essa classificação gera impacto para uma ou mais áreas da empresa.

4.2.3 – Interna:

Informação com baixa sensibilidade, mas que só deve circular internamente, não sendo de acesso ao público.

4.2.4 – Pública:

Informação que pode ser de conhecimento público e não possui qualquer restrição quanto a sua divulgação.

4.3 – Casos omissos:

Antes de efetuar qualquer ação que possa apresentar risco potencial para as informações e sistema da Priner, o usuário deverá consultar a presente Política e a Política de Privacidade e Proteção de Dados Pessoais da Companhia, a fim de certificar-se de que a atividade é lícita e segura. Quaisquer dúvidas sobre segurança da informação ou quanto ao uso do software, deverão ser encaminhados para o responsável pelo departamento de TI da respectiva filial. Caso a dúvida persista, o DPO (Data Protection Officer) deverá ser contatado.

Situações especiais e/ou pedidos de exceção a esta Política deverão ser avaliados pelo Conselho de Administração da Companhia para deliberação.

4.4 – Conformidade:

O usuário deverá estar ciente e seguir as recomendações desta Política, interpretando a classificação atribuída às informações, e assegurando que recebam tratamento adequado.

O mau uso dos recursos de tecnologia caracteriza um incidente de segurança da informação e pode resultar na aplicação de sanções legais e/ou administrativas, variando de acordo com a gravidade e o impacto do incidente para a Priner.

As violações às disposições estabelecidas na presente Política, devidamente apuradas, poderão implicar:

a) Na aplicação das sanções previstas na legislação trabalhista;
b) Na aplicação das sanções previstas na LGPD, sujeita às punições da ANPD;
c) Na aplicação das sanções previstas em contrato aos prestadores de serviço e estagiários; e
d) Na aplicação dos demais procedimentos legais cabíveis.

4.5 – Conclusão:

A Priner conta com recursos para proteger a rede interna e garantir a integridade dos dados e programas utilizados, sempre em harmonia com os interesses da organização. Diante deste cenário, novos recursos poderão ser implementados, políticas poderão ser ajustadas e novas formas de controle, monitoramento e acessos poderão ser alterados, podendo assim gerar mudanças para todos os Usuários.

Este documento informou ao leitor todas as políticas referentes a Segurança da Informação da Priner.

5.0 – REFERÊNCIAS:

- Política de Privacidade e Proteção de Dados Pessoais
- Lei nº 13.709, de 14 de agosto de 2018 (“Lei Geral de Proteção de Dados” ou “LGPD”)
- Termo de Responsabilidade e Cautela

6.0 – PAPÉIS E RESPONSABILIDADES:

A Priner entende que o sistema de segurança da informação somente será eficaz com o comprometimento de todos. Para isso, a presente política traça as principais responsabilidades para todos os Colaboradores e terceirizados:

6.1 – USUÁRIOS:

a) Respeitar esta Política de Segurança da Informação.

b) Respeitar a Política de Privacidade e Proteção de Dados Pessoais da Priner, de forma a garantir a segurança e inviolabilidade dos Dados Pessoais dos colaboradores, funcionários e clientes.

c) Respeitar todas as normas da LGPD.

d) Respeitar os procedimentos de tratamento de Dados Pessoais previsto na Política de Proteção de Dados Pessoais.

e) Garantir adequada proteção e guarda dos recursos computacionais colocados à sua disposição para o trabalho.

f) Garantir o uso exclusivo e intransferível de suas senhas de acesso.

g) Buscar conhecimento necessário para a correta utilização dos recursos de *hardware* e *software* da Companhia.

h) Relatar prontamente à área de TI (Tecnologia da Informação) qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus etc..

i) Assegurar que as informações e dados de propriedade da Companhia, inclusive Dados Pessoais, não sejam disponibilizados a terceiros, a não ser com abertura de chamado e aprovação do gestor.

j) Comprometer-se em não auxiliar terceiro e/ou não provocar invasão dos computadores ou da rede de dados, conforme artigo 154-A do Código Penal Brasileiro.

k) Responder pelo prejuízo ou dano que vier a provocar a Companhia ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

6.2 – RESPONSÁVEIS HIERÁRQUICOS (LÍDERES):

a) Apoiar e zelar pelo cumprimento desta política, servindo como modelo de conduta para os Usuários sob a sua gestão.

b) Autorizar o acesso e definir o perfil do usuário junto ao responsável pelo departamento de TI.

c) Autorizar as mudanças no perfil do usuário junto ao responsável pelo departamento de TI.

d) Educar os Usuários sobre os princípios e procedimentos de segurança da informação da Priner.

e) Notificar imediatamente ao responsável pelo departamento de TI quaisquer vulnerabilidades e ameaças à quebra de segurança.

f) Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação.

g) Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao DPO (*Data Protection Officer*), a ser nomeado pela Companhia.

h) Obter aprovação técnica do DPO (*Data Protection Officer*), conforme Política de Privacidade de Dados Pessoais, antes de solicitar a compra de *hardware*, *software* ou serviços de informática.

i) Adaptar normas, processos, procedimentos e sistemas sob sua responsabilidade para atender a esta Política.

j) Respeitar a Política de Privacidade e Proteção de Dados Pessoais da Priner.

k) Respeitar todas as normas brasileiras da LGPD (Lei Geral de Proteção de Dados).

6.3 – ÁREA DE TI:

a) Configurar os equipamentos e sistemas para cumprir os requerimentos desta política.

b) Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

c) Restringir a existência de pessoas que possam excluir os *logs* e trilhas de auditoria das suas próprias ações.

d) Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação.

e) Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.

f) Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da Priner.

g) Gerenciar o descarte de informações a pedido dos custodiantes.

h) Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário.

i) Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

j) Criar a identidade lógica dos Usuários na empresa.

k) Atribuir contas e senhas identificáveis à pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação.

l) Proteger todos os ativos de informação da empresa contra códigos maliciosos e/ou vírus.

m) Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção.

n) Definir as regras formais para instalação de *software* e *hardware*, exigindo o seu cumprimento dentro da empresa.

o) Realizar inspeções periódicas de configurações técnicas e análise de riscos.

p) Garantir, assim que solicitado, o bloqueio de acesso de Usuários por motivo de desligamento da empresa.

q) Propor as metodologias de desenvolvimento e processos específicos que visem aumentar a segurança da informação.

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

s) Buscar alinhamento com as diretrizes corporativas da Companhia.

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

u) 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 pode ser usada para identificar Usuários e respectivos acessos efetuados, bem como material manipulado.

v) Monitorar o ambiente de TI, a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da Companhia, indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos e assim por diante);

w) Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior), conforme procedimento publicado na matriz de responsabilidade.

x) Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade.

6.4 – DIRETORIA:

a) Implementar as estratégias e diretrizes da Companhia aprovadas pelo Conselho de Administração;

b) Analisar a efetividade desta Política, assim como quaisquer revisões desta, submetendo-a à aprovação do Conselho de Administração;

c) Sempre que julgar necessário, manifestar-se sobre a avaliação da eficácia das políticas.

d) Manifestar-se sobre as sugestões de alteração da estrutura operacional e recomendar ao Conselho de Administração sugestões de aprimoramento, caso entenda necessário.

6.5 – CONTROLES INTERNOS:

a) Realizar a avaliação crítica da política quanto as regras internas e externas.

b) Acompanhar e/ou realizar auditorias internas.

c) Revisar a política em conjunto com a área responsável, quando tiver alteração nos processos e/ou no final do prazo de vigência do documento.

7.0 – ANEXOS:

Não aplicável.

8.0 – APROVAÇÃO E VIGÊNCIA:

Compete exclusivamente ao Conselho de Administração da Priner Serviços Industriais S.A. aprovar quaisquer alterações à presente política.

Esta política entrará em vigor a partir da data de sua aprovação pelo Conselho de Administração e permanecerá em vigor por prazo indeterminado.

9.0 – CONTROLE DE REVISÕES:

REVISÃO	DATA	DESCRIÇÃO DA ALTERAÇÃO
0	26/07/2021	1. Versão Inicial – Elaboração da Política
1	03/11/2022	1. Alteração do modelo da política; 2. Inclusão da classificação do documento; 3. Inclusão dos domínios da Priner Rental, Brito&Kerche e Gmaia; 4. Item 4.1.2: alteração de caracteres mínimos para senha; 5. Inclusão do item 4.1.7; 6. Item 4.1.14: Inclusão da informação sobre exclusão da pasta "PÚBLICO"; 7. Atualização do link do canal de comunicação disponibilizado pela Companhia para abertura de chamados; 8. Inclusão do item 4.5.3; 9. Inclusão do item 4.6 – Utilização dos equipamentos; e 10. Inclusão do item 11.0 – Documentos de referência.
2	07/12/2023	1. Inclusão dos domínios da Soegeo, Tresca, Labteste e Semar. 2. Inclusão dos papéis e responsabilidades da Diretoria e de Controles Internos.