POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

1. OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Principia Educação Tecnologia e Serviços Ltda. ("**Principia**") desenvolveu esta Política de Segurança da Informação para estabelecer as diretrizes e responsabilidades gerais relacionadas ao processo de gestão de informação e segurança no ambiente de tecnologia da Principia.

Esta Política tem vigência indeterminada e se aplica indistintamente a todos os funcionários, independentemente da posição ocupada na Principia, incluindo todos aqueles que integram os quadros de eventuais subsidiárias ("**Colaboradores**"). As regras estabelecidas também são de observância obrigatória para representantes ou prepostos que sejam envolvidos nas relações comerciais da Principia.

Se você tiver dúvidas sobre esta Política, entre em contato pelo e-mail politicas@principia.net

2. DEFINIÇÕES

"Dados Pessoais": significa qualquer informação que, direta ou indiretamente, identifique ou possa identificar uma pessoa natural, como por exemplo, nome, CPF, data de nascimento, dentre outros. Incluem-se neste conceito os Dados Sensíveis e Dados de Crianças e Adolescentes.

"Dados Pessoais Sensíveis": significa qualquer informação que revele, em relação a uma pessoa natural, origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico.

"Dados de Crianças e Adolescentes": significa qualquer informação que, direta ou indiretamente, identifique ou possa identificar uma criança (pessoa até doze anos de idade incompletos) ou adolescente (entre doze e dezoito anos de idade).

"Incidente de Segurança": qualquer evento adverso, confirmado ou sob suspeita, envolvendo Dados Pessoais que possa acarretar risco ou danos às pessoas físicas titulares de dados, como ataques cibernéticos e outros incidentes de violação como infeção por software malicioso (vírus ou outros tipos de malwares, como Trojans – Cavalo de Tróia, Worms e Rootkits), incidentes naturais ou danos físicos (incêndios ou outros desastres, que possam inviabilizar ou comprometer servidores ou outros locais de armazenamento de dados e documentos físicos ou digitais), perda, furto, roubo, dano a dados ou equipamentos, divulgação, cópia, compartilhamento ou uso indevido de cartões de segurança ou login e senha de terceiros ou por terceiros, entre outros.

"Legislação de Proteção de Dados": significa todas as disposições legais que regulem o Tratamento de Dados Pessoais, incluindo a Lei Geral de Proteção de Dados Pessoais ("**LGPD**").

"Tratamento": significa toda e qualquer ação realizada sobre os Dados Pessoais, incluindo a coleta, utilização, processamento, armazenamento, extração e transferência. Esta definição inclui também qualquer Tratamento de Dados Pessoais, físico ou digital.

"Terceiros": qualquer pessoa ou empresa com quem a Principia mantenha relação ou contrato, incluindo fornecedores, prestadores de serviços, agentes e associados, concorrentes, parceiros de negócios e clientes.

"Titular": pessoa natural a quem se referem os Dados Pessoais que são objeto de Tratamento.

3. PRINCÍPIOS

O objetivo desta Política é primordialmente assegurar a proteção de seus ativos de informação contra ameaças, internas ou externas, minimizar eventuais riscos à segurança das informações, reduzir a exposição a perdas ou danos decorrentes de falhas de segurança e garantir que os recursos adequados estarão disponíveis, mantendo um programa de segurança efetivo e conscientizando seus Colaboradores a respeito.

Os processos de segurança de dados e da informação da Principia devem assegurar a:

- **Integridade**: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais;
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário; e
- **Confidencialidade**: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas da Principia.

4. RESPONSABILIDADES

4.1. RESPONSABILIDADE DOS COLABORADORES

Todos os Colaboradores têm a obrigação de proteger a segurança e a integridade das informações e equipamentos de informática, sendo proibido o uso de dados da Principia ou de Terceiros para propósitos incoerentes com as necessidades do negócio ou para fins que possam violar qualquer lei, regulamento, norma, ou contrato estabelecido pela Principia.

Todos os Colaboradores da Principia têm o dever de conhecer esta Política de Segurança da Informação e são responsáveis por garantir sua aplicação no âmbito de suas atividades, com a finalidade de prevenir a ocorrência de violações legais, éticas ou de outras condutas que possam comprometer a integridade e reputação da Principia.

Os Colaboradores também são responsáveis por buscar esclarecimentos junto às respectivas lideranças sobre dúvidas em relação à legislação, a esta Política de Segurança da Informação e demais políticas da Principia.

Todos os Colaboradores e Terceiros que tiverem acesso aos sistemas e equipamentos disponibilizados pela Principia comprometem-se a:

- Não transmitir quaisquer dados, incluindo Dados Pessoais, ou informações da Principia ou Terceiros que estejam em sua posse, ou ainda, que tenham a habilidade de acessar, para pessoas não autorizadas, seja de maneira verbal, escrita, impressa ou digital;
- Utilizar somente softwares originais e devidamente licenciados, bem como dispositivos e meios de comunicação previamente autorizados e recomendados pela Principia;
- Não usar informações da Principia ou Terceiros, Dados Pessoais ou quaisquer dos recursos e equipamentos da Principia para fins pessoais ou diversos daqueles necessários ao desempenho da função contratada;
- Zelar pela segurança de seu login e senha de acesso individual aos ambientes de sistemas da Principia, ficando proibida a transmissão ou uso compartilhado;
- Observar e cumprir com o disposto nesta Política e demais políticas relacionadas da Principia;
- Zelar por todo e qualquer Dado Pessoal e informação armazenada na rede corporativa contra alteração, destruição, transmissão, divulgação, cópia e acessos não autorizados;
- Guardar sigilo das informações e Dados Pessoais, mantendo-os em caráter restrito;
- Respeitar a propriedade intelectual da Principia ou de Terceiros, não copiando, modificando, usando ou divulgando em todo ou em parte, sem a permissão expressa, por escrito, do detentor de tais direitos;
- Zelar pelos equipamentos que utiliza, não sendo permitido qualquer, remoção, desconexão de partes, substituição ou qualquer alteração nas características físicas ou técnicas dos equipamentos integrantes da rede;
- Utilizar computadores, sistemas de telefonia, redes e outros serviços de informática (como sistema ERP) apenas e exclusivamente para fins profissionais, ficando vedado sua utilização para fins particulares ou para beneficiar outras empresas que não tenham relação com a Principia, salvo se autorizado por escrito pela Principia;
- Não tomar atitude ou ação que possa direta ou indiretamente indisponibilizar os recursos da rede;
- Não executar programas que tenham como finalidade a decodificação de senhas, o monitoramento desautorizado da rede ou leitura de dados, propagação de vírus de computador, a destruição parcial ou total de arquivos ou a indisponibilidade de serviços;
- Não executar programas, instalar equipamentos ou executar ações que possam facilitar o acesso à rede de pessoas não autorizadas;
- Utilizar quaisquer recursos, sejam eles microcomputadores, impressoras, ou outros equipamentos periféricos não autorizados pela Principia;

- Não utilizar os equipamentos e dispositivos da Principia para fazer download ou distribuição de software ou dados "piratas" (sem licença/autorização de uso);
- Não utilizar os recursos da Principia para deliberadamente propagar qualquer tipo de vírus, worms, cavalos de tróia, malwares ou programas de controle de outros computadores;
- Não realizar cópia de arquivos para quaisquer tipos de mídia (pen-drives, CD's, DVD's etc.), salvo se autorizado pela Principia;
- Não efetuar qualquer tipo de acesso ou alteração não autorizada a dados, Dados Pessoais e informações dos recursos computacionais pertencentes à Principia;
- Não violar os sistemas de segurança dos recursos computacionais, no que tange à identificação de usuários, senhas de acesso, fechaduras automáticas, sistemas de alarme e demais mecanismos de segurança e restrição de acesso;
- Não fazer o uso de qualquer tipo de software de acesso remoto, salvo quando expressamente autorizado pela Principia ou na prestação de suporte a distância, sendo terminantemente proibido aos usuários fazer o uso de qualquer solução nesse sentido;
- Informar imediatamente ao superior imediato ou ao e-mail seguranca@principia.net sobre a ocorrência ou suspeita de quaisquer falhas, Incidentes de Segurança ou condutas inadequadas ou ilícitas, brechas de segurança ou desvios das regras estabelecidas nesta Política, bem como sobre a ocorrência de qualquer violação à presente Política praticada em atividades relacionadas ao trabalho, dentro ou fora das dependências da Principia, para que sejam tomadas as medidas cabíveis.

A Principia exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, doloso, negligente ou imprudente dos recursos e serviços disponibilizados aos seus Colaboradores ou Terceiros, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

4.2. RESPONSABILIDADE DA LIDERANÇA

Faz parte da responsabilidade da liderança da Principia garantir que sua conduta esteja em consonância com os parâmetros da presente Política, servindo como exemplo de atuação para os Colaboradores da Principia e Terceiros.

A liderança é responsável por divulgar e conscientizar os Colaboradores sobre a importância e a necessidade do cumprimento das disposições desta Política de Segurança da Informação.

5. ACESSO ÀS INSTALAÇÕES FÍSICAS, SISTEMAS E RECURSOS DE REDE

Todo Colaborador deve ter identificação única, pessoal e intransferível, qualificando-o como responsável por qualquer atividade desenvolvida sob esta identificação. O Colaborador assume a responsabilidade quanto ao sigilo de seu login e senha pessoal. Os dispositivos de identificação como crachás e login e senhas de acesso a sistemas protegem a identidade do Colaborador, evitando e prevenindo que uma pessoa se faça passar por outra.

Por segurança, as senhas de rede e de aplicações devem seguir um padrão de segurança com senhas fortes, com critérios definidos pelo time de tecnologia da Principia. Também é recomendável que não se utilize informações pessoais fáceis de serem obtidas como, o nome, o número de telefone ou data de nascimento como senha.

Colaboradores e Terceiros autorizados são responsáveis pela correta utilização e por eventuais usos inadequados dos direitos de acesso que lhes são atribuídos. Os direitos de acesso são intransferíveis.

Os acessos aos sistemas de informação, base de dados e demais recursos de tecnologia devem ser concedidos somente pela Principia. Além disso, a concessão de acesso a dados, Dados Pessoais, informações e sistemas deve se basear na necessidade comprovada para o desempenho da função.

A Principia poderá a qualquer momento efetuar o bloqueio de acesso de Colaboradores ou Terceiros autorizados em caso da ocorrência ou suspeita de ocorrência de Incidente de Segurança, realização de investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da Principia.

Cabe à área de Recursos Humanos informar pelo e-mail seguranca@principia.net, de maneira imediata a contratação, mudança de cargo, função, suspensão ou o desligamento de Colaboradores para que as providencias de criação, ajustes no perfil ou cancelamento dos acessos concedidos sejam tomadas.

Cabe ao Colaborador responsável pelo contato com o Terceiro, avisar diretamente à Principia pelo e-mail seguranca@principia.net, quando do início, suspensão ou encerramento do contrato de prestação de serviços, para que proceda com a devida criação ou cancelamento dos acessos aos sistemas.

6. INSTALAÇÃO DE SOFTWARE

Os computadores serão configurados exclusivamente com softwares licenciados e necessários para a execução das atividades da Principia. Qualquer necessidade específica deverá ser previamente solicitada à Principia, pelo e-mail rh@principia.net, que fará análise da necessidade e acionará a área ou profissional responsável. Em nenhum caso será permitida a utilização de softwares sem a devida licença de uso.

É considerada falta grave instalar no computador qualquer software sem as devidas licenças corporativas, por se tratar de atividade ilegal, assim como os não autorizados, pelos riscos de segurança causados aos sistemas como um todo.

7. USO DO E-MAIL CORPORATIVO

O e-mail corporativo é uma ferramenta disponibilizada para que o Colaborador possa desenvolver suas atividades profissionais, o que requer cuidados para garantir a segurança da informação.

O Colaborador é responsável pela correta utilização do e-mail corporativo, ficando proibida as seguintes práticas:

- Enviar mensagens de correio eletrônico cujo conteúdo seja confidencial a pessoas não autorizados a receber tais mensagens;
- Divulgar informações não autorizadas, como por exemplo, fotos, imagens de tela, dados de sistemas, documentos e afins, sem autorização expressa e formal da Principia;
- Enviar mensagens com conteúdo ilegal, pornográfico, obsceno, de caráter racista, político-partidário, calunioso, difamatório, discriminatório, infame, ofensivo, violento e/ou ameaçador;
- Divulgar material protegido por ou que contenha qualquer informação protegida por propriedade intelectual sem a permissão da Principia ou do detentor dos direitos;
- Enviar e-mails não solicitados (SPAM);
- Falsificar qualquer informação da mensagem original que está sendo enviada;
- Abrir ou executar arquivos anexados enviados por remetentes desconhecidos ou suspeitos, com as extensões .bat, .exe, .src, .lnk, .com e .dmg. Em caso de dúvida sobre a legitimidade do e-mail, entre em contato com o líder da sua área para verificação antes de qualquer ação;
- Utilizar o e-mail profissional para fins e/ou assuntos pessoais. Por exemplo, os endereços de e-mail da Principia não devem ser utilizados em lojas virtuais ou em cadastros de lojas ou promoções de qualquer natureza.

A utilização do e-mail pessoal não é recomendada nos computadores e celulares disponibilizados, bem como utilizando a rede da Principia. Caso seja necessária a utilização, todos os itens dessa Política devem ser respeitados.

O e-mail corporativo e as informações nele contidas são de propriedade da Principia e, como tal, poderão ser auditados sem prévio aviso. A Principia também poderá realizar o monitoramento contínuo da rede e dos e-mails, visando evitar a perda de informações da Principia.

A Principia poderá restringir a entrada de arquivos suspeitos como prevenção contra vírus de computador.

8. USO DA INTERNET

O uso da Internet se limita a pesquisas e necessidades específicas do trabalho do Colaborador. Acessos não relacionados com a prática profissional não são recomendados. Ainda, apenas páginas da internet alinhadas com as necessidades da Principia serão liberadas para acesso.

O uso e acesso à Internet é proibido para os seguintes casos:

- Acessar sites suspeitos, não confiáveis ou que não adotem protocolo de segurança;
- Acessar sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados e a tentativa do acesso será monitorada;

- Divulgar e compartilhar dados ou informações da Principia ou de Terceiros em listas de discussão (fóruns), sites ou comunidades de relacionamento, salas de bate-papo, chat, comunicadores instantâneos ou qualquer outra Rede Social ou tecnologia correlata que venha surgir na Internet;
- Usar a Internet para copiar ou distribuir quaisquer materiais, incluindo software, que viole direitos de propriedade intelectual da Principia ou Terceiros ou fazer o download ou distribuição de software ou dados pirateados ou qualquer atividade considerada ilegal;
- Usar ferramentas de torrent e de troca de informação e conteúdo on-line em redes P2P (Peer-to-peer);
- Usar nos computadores corporativos ferramentas de mensagens instantâneas não autorizadas pela Principia;
- Utilizar serviços de vídeos em tempo real não autorizados pela Principia;e
- O uso de redes de internet Wi-Fi públicas ou que exijam o acesso de dados para a conexão.

A utilização da Internet não é recomendada para fins pessoais nos computadores e celulares disponibilizados, bem como utilizando a rede da Principia. Caso seja necessária a utilização, todos os itens dessa Política de Segurança da Informação devem ser respeitados.

9. EQUIPAMENTOS MÓVEIS

A Principia poderá disponibilizar, a depender da função, equipamentos eletrônicos móveis, como smartphones e notebooks. É responsabilidade do Colaborador e do Terceiro autorizado manter esses equipamentos em condições seguras, evitando danos ou furtos.

O equipamento disponibilizado será para uso profissional, ou seja, apenas para os negócios relacionados à Principia. Desta maneira, não está autorizado o uso de equipamentos pessoais, instalar aplicativos ou configurar recursos e serviços não autorizados pela Principia, pois podem trazer riscos para o ambiente computacional e informações de negócio.

Todo Colaborador ou Terceiro que utiliza um ou mais equipamentos disponibilizados pela Principia está sujeito às seguintes regras:

- A sessão de trabalho deve ser encerrada no final do expediente, com desligamento do equipamento;
- É obrigatório manter todos os arquivos originais salvos nos sistemas da Principia, sendo proibido que esses sejam mantidos em unidades de armazenamento locais ou móveis (exemplo: drive "C", pen drive, HD externos, área de trabalho dos computadores, CD, etc.).;
- O usuário deverá, obrigatoriamente, utilizar bloqueio automático e senhas de acesso para seus dispositivos móveis;

- Havendo necessidade de transporte do equipamento, mantenha o dispositivo sempre com você e não deixe o dispositivo em local visível, mantendo atenção a locais de grande fluxo de pessoas, como saguões de hotéis, aeroportos, aviões, táxi e etc.;
- Ao se conectar em sua residência, o Colaborador deve garantir que seu roteador esteja com a senha de administrador diferente da fornecida pelo fabricante. Além disso, deve o Colaborador verificar com o fornecedor da rede Wi-Fi a aplicação de configurações de segurança como, por exemplo: habilitação do protocolo WPA2; e
- É responsabilidade do usuário, no caso de furto ou roubo de um dispositivo móvel fornecido pela Principia, notificar imediatamente seu gestor direto ou ao e-mail rh@principia.net.

A Principia, na qualidade de proprietária ou possuidora dos dispositivos móveis, reserva-se o direito de inspecioná-los a qualquer tempo, sem prévio aviso.

10. EQUIPAMENTOS PARTICULARES

O uso de equipamentos particulares nas dependências da Principia deve seguir as seguintes regras:

- É proibida a utilização de equipamentos portáteis (como notebooks, ultrabooks, tablets etc.) contendo informações comerciais da Principia, sem autorização e/ou ciência do superior imediato;
- O uso de smartphones é permitido, desde que sejam conectados na rede Wi-Fi própria autorizada da Principia, configurada pela área responsável;
- É vedada a utilização do e-mail corporativo nos equipamentos particulares, exceto para situações com autorização e/ou ciência do superior imediato; e
- Nenhum equipamento eletrônico particular ou serviços de armazenamento de arquivos pessoal na Nuvem (como DropBox, Google Drive) devem ser utilizados para fins de trabalho, exceto quando autorizado pela Principia. Casos específicos (solicitações de exceções) e necessidades eventuais serão tratadas caso a caso pela Principia, em conjunto com um superior responsável.

11. SEGURANÇA EM IMPRESSOS E MESA LIMPA

Documentos enviados para impressão devem ser retirados imediatamente caso a impressora não possua o recurso de impressão por crachá.

Documentos confidenciais ou que contenham Dados Pessoais ou informações da Principia ou de Terceiros não devem ficar expostos com fácil acesso quando não estiverem sendo utilizados, como por exemplo, sobre as mesas ou estantes, e deverão ser triturados antes de serem descartados.

12. CANAL DE DENÚNCIAS

As violações às diretrizes dessa Política de Segurança da Informação devem ser levadas ao conhecimento da liderança da Principia. O anonimato do Colaborador e a confidencialidade

do relato serão garantidos pela Principia. Não serão toleradas retaliações ou punições contra Colaboradores que efetuarem de boa-fé denúncias ou reclamações.

As denúncias podem ser realizadas pelo e-mail: etica@principia.net.

Internamente, a Principia poderá apurar denúncias diretamente ou contratar consultoria especializada para apuração. Caso a denúncia envolva membros da liderança, as apurações serão realizadas por consultoria externa especializada.

13. CONSIDERAÇÕES FINAIS

Esta Política de Segurança da Informação contempla princípios que norteiam a atitude profissional e deve ser respeitada por todos os que, de alguma forma, estejam vinculados à Principia.

O descumprimento de qualquer item desta Política, bem como a omissão de informações relevantes, sujeitará os Colaboradores a ações disciplinares. É dever de todos os Colaboradores levar ao conhecimento da Principia quaisquer desvios de conduta que contrariem as determinações constantes nessa Política de Segurança da Informação.

Esta Política Anticorrupção foi aprovada pela Diretoria da Principia em 04 de abril de 2023.