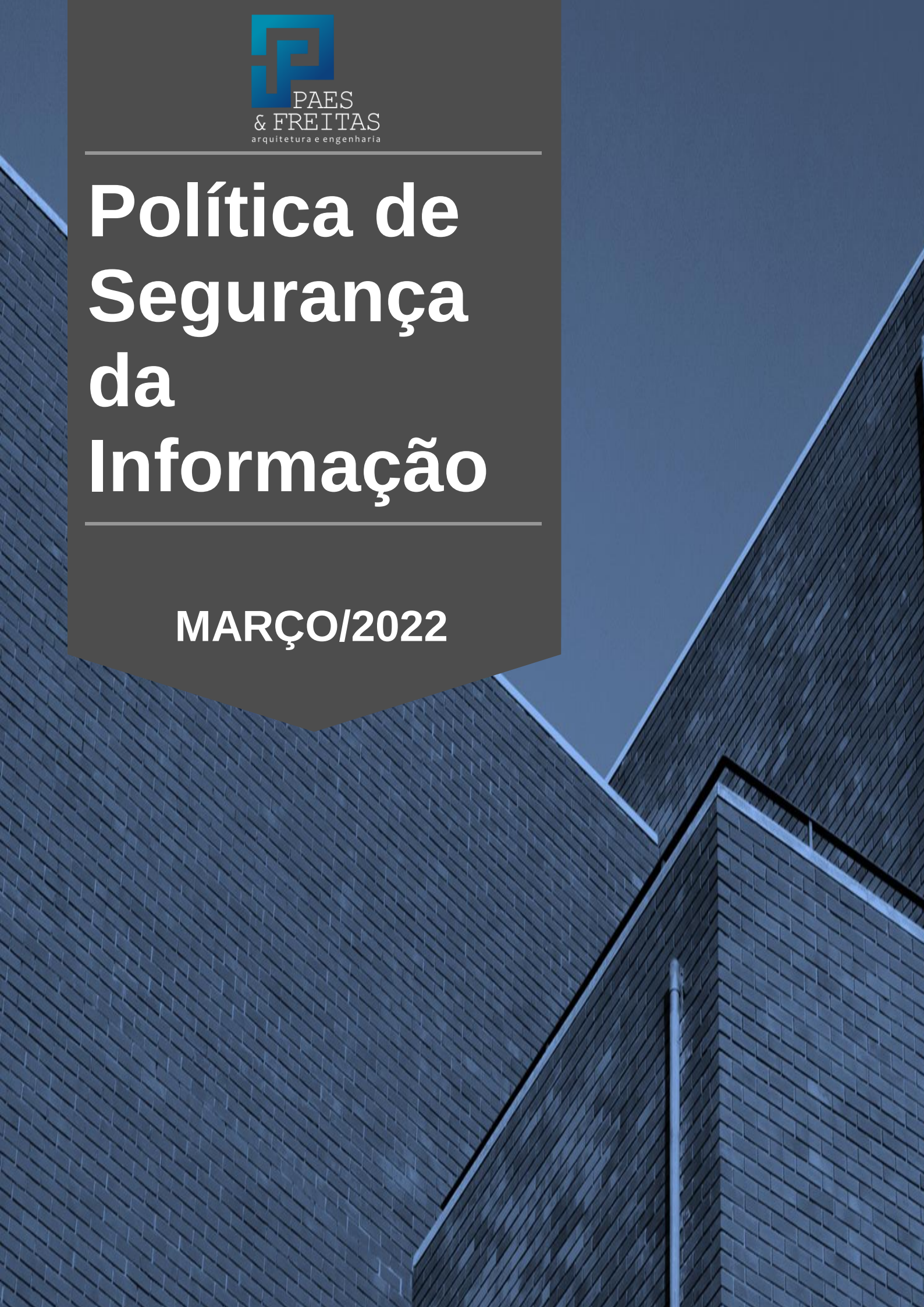
PAES
& FREITAS
arquitetura e engenharia

Política de Segurança da Informação

MARÇO/2022



Política de Segurança da Informação (PSI)

1. Introdução

Com o advento da Lei Geral de Proteção de Dados (LGPD), o Paes e Freitas investiu na segurança para proporcionar uma experiência segura e transparente de tratamento de dados para clientes, prestadores de serviço, fornecedores e colaboradores. A política de segurança da informação formaliza um guia de melhores práticas para reafirmar e padronizar a segurança da informação dentro da instituição.

2. Propósito

Este documento apresenta e institui um conjunto de instruções formais para normatizar e sistematizar a segurança da informação do Paes e Freitas e confirma, a responsabilidade e compromisso da empresa com o tratamento de dados pessoais e outros tipos de informação de sua propriedade e/ou guarda.

3. Abrangência da Política de Segurança da Informação

A PSI deve ser seguida por todos, incluindo, mas não se limitando a: colaboradores, prestadores de serviços temporários, prestadores de serviço, terceirizados, executivos, acionistas, auditores, consultores, fornecedores e parceiros de negócio que estejam a serviço do Paes e Freitas em qualquer etapa do processo.

4. Papéis e responsabilidade de Segurança da Informação

Papel	Responsabilidades
Encarregado da Proteção de Dados (DPO)	Prestar esclarecimentos para os titulares de dados acerca da política de privacidade de dados e os direitos previstos na Lei Geral de Proteção de Dados (LGPD). Prestar esclarecimentos para a Autoridade Nacional de Proteção de Dados (ANPD), quando solicitado. Adequar e auditar as melhores práticas necessárias para a conformidade com a Lei Geral de Proteção de Dados (LGPD). Monitorar a tabela de temporalidade de documentos e o descarte das informações. Orientar e esclarecer sobre melhores práticas de segurança da informação no âmbito do Paes e Freitas.
Membro do Comitê de Proteção de Dados	Assessorar o Encarregado da proteção de dados (DPO) sobre decisões que possam impactar a confidencialidade, disponibilidade e integridade de dados.
Colaborador	Ler, assimilar e praticar a PSI durante o período integral de trabalho e/ou durante a prestação de serviços em nome do Paes e Freitas. Acionar o Encarregado da proteção de dados no caso de dúvidas sobre a segurança das informações e proteção de dados pessoais. Acionar o setor de tecnologia da informação no caso de suspeitas de ameaças no ambiente tecnológico. Não divulgar informações e dados pessoais do Paes e Freitas e/ou informações que estejam provisoriamente sobre sua posse.
Prestadores de serviços temporários, prestadores de	Ler, assimilar e praticar a PSI durante o período integral de trabalho e/ou durante a prestação de serviços em nome do Paes e Freitas.

serviços e terceirizados	Acionar o Encarregado da proteção de dados no caso de dúvidas sobre a segurança das informações e proteção de dados pessoais. Acionar o setor de tecnologia da informação no caso de suspeitas de ameaças no ambiente tecnológico. Não divulgar informações e dados pessoais do Paes e Freitas e/ou informações que estejam provisoriamente sobre sua posse.
Fornecedores e parceiros de negócio	Ler, assimilar e praticar a PSI durante o período integral de trabalho e/ou durante a prestação de serviços em nome do Paes e Freitas. Acionar o Encarregado da proteção de dados no caso de dúvidas sobre a segurança das informações e proteção de dados pessoais. Não divulgar informações e dados pessoais do Paes e Freitas e/ou informações coletadas durante a prestação de serviços em nome do Paes e Freitas.
Consultores e auditores	Ler, assimilar e praticar a PSI durante o período integral de trabalho e/ou durante a prestação de serviços em nome do Paes e Freitas. Acionar o Encarregado da proteção de dados no caso de dúvidas sobre a segurança das informações e proteção de dados pessoais. Não divulgar informações e dados pessoais do Paes e Freitas e/ou informações coletadas durante a prestação de serviços em nome do Paes e Freitas.

5. Termos e definições

- TI: Tecnologia da Informação
- *Software*: É a parte lógica, o conjunto de instruções e dados processados nos servidores ecomputadores. Toda interação dos usuários de computadores é realizada através de *softwares*.
- *Backup*: É a cópia de dados de um dispositivo de armazenamento a outro para que possa serrestaurado em caso da perda dos dados originais.
- Mídias Removíveis: Dispositivos que permitem a leitura e gravação de dados tais como: CD,DVD, *Pen Drive*, cartão de memória entre outros.

- *USB:* É um tipo de conexão em computadores que permite a de uma mídia removível ouperiféricos (teclado, mouse, etc.)
- *Dado pessoal:* Informação relativa a uma pessoa, identificada ou identificável. Também constituem dados pessoais o conjunto de informações distintas que podem levar à identificação de uma determinada pessoa.
- VPN (*Virtual Private Network*): Modalidade de acesso remoto à rede corporativa estando o computador fisicamente fora das instalações da companhia. Comumente é utilizado por funcionários em trânsito.
- *Softwares* de Mensageria: São softwares que permitem a troca de mensagens (textos, imagens, sons, arquivos, etc) entre mais de um usuário através da rede corporativa (exemplo: Microsoft Office Communicator, Yahoo Messenger, Gtalk, Skype, etc).
- *Firewall:* É um dispositivo utilizado em redes de computadores para segmentar e controlar os acessos entre redes internar e/ou externas.
- *Log*: É o termo técnico para descrever o registro das transações que ocorrem quando um software é utilizado.
- *Phishing:* Que vem do inglês e corresponde a “pescaria”, tem o objetivo de “pescar” informações e dados pessoais importantes através de mensagens falsas. Com isso, os criminosos podem conseguir nomes de usuários, senhas e dados pessoais de um site qualquer, como também são capazes obter dados de contas bancárias e cartões de crédito.

6. Diretrizes de Segurança da Informação

As diretrizes de segurança das informações, expõem o posicionamento do Paes e Freitas acerca de melhores práticas de segurança que devem ser seguidas por todos.

Uso de senhas

- A troca de senhas para acesso aos computadores deverá ser alterada a cada 45 dias;
- Não registre as senhas em locais de fácil acesso e/ou em locais que possam ser acessados por outras pessoas;

- As senhas terão um tempo de vida útil pré-determinado pelo sistema de informação, devendo o mesmo ser respeitado;
- A senha de usuário é INTRANSFERÍVEL e não deve ser compartilhada nem mesmo com o setor de tecnologia da informação;
- Caso desconfie que sua senha não está mais segura, sinta-se à vontade para alterá-la, mesmo antes do prazo de validade pré-determinado;
- Os sistemas de informação do Paes e Freitas registram logs de atividade de usuário e, portanto, auditorias sobre a utilização das senhas para realização de ações poderão ser realizadas pelo setor de tecnologia da informação;
- A senha de sistemas da informação é de inteira responsabilidade do próprio usuário.

Comunicação no ambiente digital

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com, principalmente se não tiver comprovação de que solicitou o e-mail. Na dúvida, acione o setor de tecnologia da informação;
- Desconfie de e-mails ou mensagens instântaneas com assuntos estranhos ao seu conhecimento;
- Não reenvie e-mails dos quais não tenha certeza sobre a origem segura;
- O e-mail corporativo deve ser usado exclusivamente para fins profissionais e que tenham relevância para o Paes e Freitas;
- Antes de enviar um mensagem, verifique se todos os destinatários precisam receber a informação;
- Utilize apenas as ferramentas de comunicação homologadas pelo setor de tecnologia da informação do Paes e Freitas;
- As comunicações realizadas através das ferramentas de comunicação deverão acontecer apenas dentro do horário de jornada prevista ou através da autorização direta do gestor da área;
- Evite trafegar documentos sigilosos e que possuam dados pessoais e/ou dados pessoais sensíveis através do e-mail. Ao invés disso, prefira trafegar documentos através da solução oficial de compartilhamento de documentos em nuvem do Paes e Freitas;
- As ferramentas de comunicação do Paes e Freitas são monitoradas e as mensagens trocadas poderão ser auditadas.

Acesso à Internet

- O uso da internet é monitorado e poderá ser auditado pela equipe de tecnologia do Paes e Freitas e o usuário poderá vir a prestar contas de seu uso para o comitê de proteção de dados e o Encarregado da Proteção de Dados (DPO);
- A internet deve ser utilizada para fins profissionais e de interesse do Paes e Freitas;
- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados é proibido;
- É proibido o download de softwares e conteúdos protegidos pela lei de propriedade intelectual;
- Não utilize ferramentas de compartilhamento Peer-2-Peer (P2P) (kazaa, Morpheus, Torrent e afins).

Documentos físicos, impressão e descarte

- Verifique se é realmente imprescindível a necessidade de impressão do documento;
- No caso da utilização de impressora compartilhada, se dirija até a impressora imediatamente após autorizar a impressão;
- Documentos que, possuam qualquer tipo de dados pessoais, como nomes, telefones, e-mails e afins, não poderão ser utilizados como rascunho;
- Caso seja necessário descartar documentos que contenham dados pessoais, rasgue-os de forma que seja impossível identificar os dados que estavam ali contidos;
- Caso alguma documentação física precise ser transportada por um prestador de serviço terceirizado, assegure-se de lacrar a documentação e registrar um número de protocolo;
- Toda a informação física precisa ser etiquetada, contendo informações do conteúdo da documentação e tempo de retenção. Após o tempo de retenção, acione o Encarregado da Proteção de Dados (DPO) para acompanhar o descarte da documentação;
- Caso seja necessário levar a documentação para a sua residência, solicite a autorização do Encarregado da Proteção de Dados (DPO).

Política da Mesa e Tela Limpa

- Jamais deixe documentos, principalmente aqueles que contenham dados pessoais, visíveis sobre a sua mesa;
- Após a utilização a documentação, guarde-a imediatamente em um local seguro;
- Após a utilização a estação de trabalho, certifique-se de realizar o procedimento de “logoff” (desconectar o usuário conectado);
- Caso precise se ausentar da frente do seu computador, faça o bloqueio da tela. Mesmo quando em regime de trabalho remoto (Home Office);

Uso de estação de trabalho e cópia de segurança (Backup)

- Todas as estações de trabalho (computadores, dispositivos e afins) são monitoradas pelo setor de tecnologia da informação e poderão ser auditadas a qualquer momento;
- A estação de trabalho deve ser utilizada exclusivamente para fins profissionais e de interesse do Paes e Freitas;
- O reparo e manutenção das estações de trabalho somente poderão ser realizadas pelo setor de tecnologia da informação;
- Não instale nenhum tipo de software/hardware sem autorização do setor de tecnologia da informação. A instalação ou remoção de softwares devem ser acompanhadas;
- Não armazene arquivos MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria na estação de trabalho ou no servidor de arquivos da empresa;
- Todos os dados relativos à empresa devem ser mantidos na solução oficial do Paes e Freitas de armazenamento de arquivos, onde existe um sistema de backup diário e confiável. O setor de tecnologia da informação e o DPO não se responsabilizam por arquivos armazenados na estação de trabalho;
- Informações salvas em estações de trabalho de prestadores de serviços, fornecedores, prestadores de serviços temporários, consultores, auditores e afins, são de responsabilidade dos mesmos, bem como em relação à integridade, confidencialidade e disponibilidade da informação;

Política Social

- Não comente sobre as rotinas de trabalho no Paes e Freitas para terceiros e/ou em locais públicos;
- Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa;
- Somente aceite ajuda técnica de um membro do setor de tecnologia da informação, previamente apresentado e identificado;
- Nunca execute procedimentos técnicos cujas instruções não tenham sido cedidas pelo setor de tecnologia da informação;
- Relate o setor de tecnologia da informação pedidos externos ou internos que venham a discordar dos tópicos anteriores.

Vírus, códigos maliciosos e dispositivos removíveis

- Mantenha o software de antivírus da sua estação de trabalho atualizado. Caso perceba mensagens de alerta do seu software de antivírus, como ameaças ou necessidade de atualização, acione o setor de tecnologia da informação imediatamente;
- O uso de dispositivos removíveis como: smartphones conectados na estação de trabalho, CDs, DVDs, Blu-ray's, pendrives ou qualquer tipo de mídia é probidio, exceto, nos casos extraordinários previamente autorizados pelo Encarregado da Proteção de Dados (DPO);
- Informe atitudes suspeitas em seu sistema para o setor de tecnologia da informação, para que possíveis códigos maliciosos possam ser identificados no menor espaço de tempo possível;
- Suspeite de softwares recém-instalados na sua estação de trabalho sem o seu consentimento. Caso isto ocorra, acione imediatamente o setor de tecnologia da informação.

Trabalho remoto

- Durante o período de trabalho fora das dependências do Paes e Freitas, cuide da estação de trabalho e não permita que estranhos tenham acesso;

- Mesmo em trabalho remoto, a estação de trabalho deverá ser utilizada exclusivamente para fins profissionais e de interesse do Paes e Freitas;
- A utilização da estação de trabalho do Paes e Freitas para prática de cyber crimes, é passível de penalidades, inclusive, na esfera judicial.

Uso de dispositivos móveis (Smartphones, tablets e correlatos)

- Todas as informações trafegadas nos dispositivos móveis do Paes e Freitas são monitoradas pelo setor de tecnologia da informação e poderão ser auditadas, incluindo os horários e dias e utilização por parte do colaborador e/ou prestadores de serviços e terceirizados;
- É permanentemente proibido realizar a captura de imagens, ainda que em formato de printscreen (captura de tela) dos sistemas operacionais internos da empresa;
- Não é permitido utilizar o celular de uso pessoal para registrar, por texto, áudio, vídeo ou foto, quaisquer informações empresariais ou confidenciais;
- Não é permitido usar o celular para gravar conversas sem que todos os envolvidos na conversa tenham autorizado previamente a gravação;
- Não é permitido o celular para atividades que infrinjam quaisquer leis ou normativas aplicáveis à pessoa física ou à empresa;
- É proibido utilizar o celular para disseminar informações pessoais relacionadas a empresa, ou dados referentes ao setor ao qual o remetente do conteúdo esteja incluído;
- É proibido usar de linguagem imprópria, ou ter comportamentos considerados nocivos à imagem da empresa enquanto estiver em ligação ou envio de áudio no horário de trabalho, principalmente na presença de clientes, parceiros e colaboradores.

Lei Geral de Proteção de Dados

- Todo e qualquer dado pessoal coletado deve ser utilizado exclusivamente para a finalidade informada no momento da coleta;
- Não faça o compartilhamento de dados pessoais (nome, telefone, e-mail, etc.) sem consultar o Encarregado da Proteção de Dados (DPO);

- ❖ Não registre dados pessoais em dispositivos particulares, sempre utilize os equipamentos e armazenamento providos pelo Paes e Freitas;
- ❖ Caso receba algum questionamento sobre o cumprimento da Lei Geral de Proteção de Dados (LGPD), redirecione o questionamento para o Encarregado da Proteção de Dados (DPO);

7. Processo Disciplinar

O não cumprimento das diretrizes da Política de Segurança da Informação, acarretará em advertência verbal, reciclagem obrigatória em segurança da informação, advertência emitida pelo DPO (Encarregado da Proteção de Dados) e formalizada pelo setor de Recursos Humanos do Paes e Freitas, suspensão com desconto em folha de pagamento ou até mesmo o desligamento do colaborador ou rescisão contratual com fornecedores e prestadores de serviço, de acordo com a gravidade da ocorrência.

Tais penalidades não excluem a possibilidade de direito de regresso, através de ação judicial em desfavor do funcionário.

8. Casos omissos e exceções

Os casos omissos e exceções à Política de Segurança da Informação, serão tratados formalmente, através de um processo administrativo interno, liderado pelo Encarregado da Proteção de Dados (DPO) e registrado em ata.

9. Dados de contato

Abaixo seguem todos os contatos dos membros do comitê de proteção de dados e Encarregado da proteção de dados do Paes e Freitas.

Nome	Papel	E-mail
Isa Paes	DPO – Encarregada da Proteção de Dados	isa@paesefreitas.com.br

Cynthia Freitas	Representante do comitê de proteção de dados	cynthia@paesefreitas.com.br

Aracaju, ___ de _____ de _____.

_____

Assinatura da parte interessada

☐ Colaborador ☐ Prestador de Serviço ☐ Fornecedor