POLÍTICA DE TECNOLOGIA DA INFORMAÇÃO

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP

www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

SUMÁRIO

1. OBJETIVO 4
2. ABRANGÊNCIA – APLICABILIDADE 4
3. RESPONSABILIDADES 4
3.1. GESTORES DE PESSOAS E/OU PROCESSOS: 4
3.2. TECNOLOGIA DA INFORMAÇÃO: 5
4. UTILIZAÇÃO DE TECNOLOGIA 5
5. INTERNET E ACESSO À REDE CORPORATIVA 6
6. DIRETRIZES DE SENHAS E ACESSOS 7
7. CONFIGURAÇÃO DE REDE 7
8. UTILIZAÇÃO DA REDE 8
9. BACKUP 10
10. MONITORAMENTO E CONTROLES 11
10.1. CONTROLE DE ACESSOS: 11
10.2. REDIRECIONAMENTOS DE E-MAIL 11
10.3. UTILIZAÇÂO DE E-MAILS 12
11. USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS 13
12. SEGURANÇA DO AMBIENTE DE TI 15
13. INSTALAÇÃO E GERENCIAMENTO DE ANTIVÍRUS 16
14. RECURSOS DE IMPRESSÃO 16
15. INSTALAÇÃO DE SOFTWARE 16
16. POSTO DE TRABALHO 17
17. DIREITOS DE PROPRIEDADE 19
18. PROTEÇÃO DE DADOS PESSOAIS 19
18.1. IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS 19
18.2. RESPEITO DA PRIVACIDADE 20
18.3. SEGURANÇA DOS DADOS 20
18.4. A QUEM COMPETE A PROTEÇÃO DE DADOS 20
19. PENALIDADES 21

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

20. VIGÊNCIAS E VALIDADES 21
21. DEFINICÕES 21
21.1. INFORMAÇÃO 21
21.2. SEGURANÇA DA INFORMAÇÃO 22
21.3. INTEGRIDADE 22
21.4. CONFIDENCIALIDADE 22
21.5. DISPONIBILIDADE 22
21.6. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO 22
21.7. RISCO DE SEGURANÇA DA INFORMAÇÃO 23
22. CONSIDERAÇÕES FINAIS 23

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 - Sala 1501 - Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002- Barueri/SP

POLÍTICA INSTITUCIONAL

1. OBJETIVO

O objetivo dessa política é definir orientações que capacitem a todos os usuários do Instituto Diretrizes, normas de conduta referentes à tecnologia da informação e à segurança da informação, alinhadas às demandas de negócios e às exigências legais para garantir a integridade, confidencialidade e disponibilidade dos ativos da Organização, tais como:

- Integridade
- Confidencialidade
- Disponibilidade

2. ABRANGÊNCIA – APLICABILIDADE

As orientações estabelecidas neste documento devem ser observadas por todos os colaboradores do Instituto Diretrizes, incluindo prestadores de serviços, e são válidas para qualquer forma ou meio de informação.

3. RESPONSABILIDADES

Usuários em geral: Qualquer indivíduo, seja ele um funcionário com contrato CLT ou um prestador de serviços, que desempenhe atividades dentro ou fora do Instituto Diretrizes. Cada colaborador é totalmente responsável por qualquer prejuízo ou dano que possa ocorrer ao Instituto Diretrizes e/ou a terceiros devido ao não cumprimento das diretrizes e normas estabelecidas neste documento.

3.1. GESTORES DE PESSOAS E/OU PROCESSOS:

Devem disseminar as diretrizes aos seus colaboradores, servindo como modelo de comportamento para os mesmos sob sua supervisão. É sua

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

responsabilidade atribuir a eles, durante o processo de contratação e formalização de contratos individuais de trabalho ou de prestação de serviços, a obrigação de seguir a política estabelecida. Além disso, devem garantir que os colaboradores compreendam a importância de cumprir as normas estabelecidas e comprometer-se a manter a confidencialidade e o sigilo, mesmo após o término de seu vínculo com a empresa, em relação a todos os ativos de informação do Instituto Diretrizes. Antes de conceder acesso às informações da unidade, é necessário solicitar a assinatura de um acordo de confidencialidade por parte dos colaboradores temporários e prestadores de serviços que não estejam abrangidos por contratos existentes, especialmente durante a fase de coleta de informações para propostas comerciais.

3.2. TECNOLOGIA DA INFORMAÇÃO:

É responsável por gerenciar, orientar, treinar e documentar informações relacionadas a sistemas legados, ativos inativos e a implementação de novos projetos de tecnologia relacionados à Segurança da Informação no Instituto Diretrizes. A TI também é encarregada de monitorar e controlar o ambiente tecnológico, realizando consultas de monitoramento de atividades em redes (redes de telecomunicações e servidores de arquivos) e produzindo relatórios de auditoria de arquivos, além de manter registros de logs do ERP.

4. UTILIZAÇÃO DE TECNOLOGIA

O Instituto Diretrizes é responsável por disponibilizar equipamentos eletrônicos para auxiliar os colaboradores em suas atividades profissionais, reiterando que é estritamente proibido utilizar esses recursos e meios eletrônicos para finalidades não relacionadas ao trabalho.

Os recursos tecnológicos da empresa, que incluem computadores, correio

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP

www.institutodiretrizes.org.br

eletrônico, acesso à internet, aplicativos e o sistema de comunicação interna, devem ser empregados exclusivamente para fins profissionais, em conformidade com as diretrizes estabelecidas na política de tecnologia da informação.

Sendo assim, toda e qualquer instalação/desinstalação de softwares e aplicativos deve ser solicitada ao departamento de TI via chamado pelo sistema de atendimento do TI.

5. INTERNET E ACESSO À REDE CORPORATIVA

Os sistemas, internet, correio eletrônico e quaisquer outros sistemas similares são de responsabilidade do Instituto Diretrizes e, sob nenhuma circunstância, podem ser utilizados para transmitir (enviar, receber ou divulgar) mensagens discriminatórias ou de assédio, para ações que não tenham natureza profissional, para o encaminhamento de conteúdo obsceno ou imoral, para solicitações comerciais inapropriadas ou qualquer atividade que viole o Programa de Compliance ou o Código de Conduta e Ética do Instituto Diretrizes.

Para acessar os dados armazenados nos servidores do Instituto Diretrizes, cada usuário deve possuir um login e senha previamente registrados pelo departamento de Tecnologia da Informação da matriz. É aconselhável que as senhas sejam trocadas regularmente, a fim de garantir um maior controle e segurança nos acessos.

Cada usuário está autorizado a acessar somente as informações e ambientes previamente designados para sua atividade, e, portanto, só serão concedidos os acessos específicos para cada usuário.

No caso de necessidade de acesso à rede por parte de terceiros, o solicitante deve obter a autorização do gestor imediato do setor relevante, que, por sua vez, deve solicitar a permissão à equipe de TI, fornecendo informações sobre o período de início e término do acesso para fins de monitoramento. Qualquer futura necessidade de acesso deverá ser comunicada à equipe de TI

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP

www.institutodiretrizes.org.br

para desbloqueio.

6. DIRETRIZES DE SENHAS E ACESSOS

Aqueles que possuem acesso aos sistemas de informação do Instituto Diretrizes têm a responsabilidade de tomar as medidas necessárias para evitar qualquer acesso não autorizado a esses sistemas. Os colaboradores devem assegurar a proteção de suas senhas e outros métodos de acesso aos sistemas ou informações da empresa, e jamais devem compartilhar suas senhas ou meios de acesso com terceiros não autorizados.

7. CONFIGURAÇÃO DE REDE

O departamento de Tecnologia da Informação (TI) assume a responsabilidade de oferecer diretrizes referentes à configuração da rede, bem como de adicionar novos funcionários à mesma, definir os níveis de permissão para os colaboradores e gerenciar licenciamentos de software.

Para adicionar ou remover novos colaboradores, segue-se um processo que é iniciado quando o Departamento de Recursos Humanos (RH) solicita à TI a criação de acessos de acordo com as necessidades do usuário, de acordo com o perfil definido pelo gestor.

Além disso, é importante realizar um monitoramento e controle semestral dos arquivos e pastas de rede de cada departamento. Esse monitoramento deve ser conduzido pelo respectivo gestor e tem como objetivo avaliar o conteúdo armazenado.

A divulgação indevida de dados sensíveis e pessoais para departamentos não relacionados é estritamente proibida.

Documentos essenciais para as atividades dos funcionários e colaboradores do departamento devem ser armazenados nos Servidores da Rede.

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 - Sala 1501 - Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002- Barueri/SP

www.institutodiretrizes.org.br

Arquivos que estejam exclusivamente nas máquinas locais não estão sujeitos a backups garantidos e podem ser perdidos em caso de falha do computador, sendo, portanto, de responsabilidade do usuário.

Arquivos pessoais ou não relacionados às operações do Instituto Diretrizes, como fotos, músicas, vídeos, etc., não devem ser copiados ou movidos para os "drives" de rede. A identificação desses tipos de arquivos pode resultar em exclusão permanente sem aviso prévio ao usuário.

O gerenciamento do(s) banco(s) de dados é uma responsabilidade exclusiva do departamento de Tecnologia da Informação, assim como a manutenção, alteração e atualização de equipamentos e programas.

8. UTILIZAÇÃO DA REDE

O ingresso à rede interna deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam minimizados. Assim, é preciso que sejam instauradas algumas regras, listadas a seguir:

- A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade do Instituto Diretrizes, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores;
- O RH ficará responsável por notificar formalmente o setor de Tecnologia da Informação sobre desligamentos de colaboradores, para que os acessos deles sejam revogados;
- O Instituto Diretrizes reserva-se ao direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

- Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade do Instituto Diretrizes, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação;
- É proibida a divulgação e/ou o compartilhamento indevido de informações privadas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet como via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer sanções.
- Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
- Os colaboradores não poderão usar os recursos do Instituto Diretrizes para deliberada ou inadvertidamente propagar qualquer tipo vírus, worms, cavalos de troia, spam, ou programas de controle remoto de outros computadores;
- Não serão permitidos os acessos a softwares peer-to-peer (BitTorrent, µtorrent e afins);
- Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de bypass de firewall;
- Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

realizar auditorias de segurança, quando o setor de Tecnologia da Informação deverá estar devidamente ciente e concedido autorização para tal;

- Os arquivos inerentes ao Instituto Diretrizes, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;
- Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;

9. BACKUP

Um dos procedimentos mais básicos da Segurança da Informação é a implantação de uma Política de Backup (cópia de segurança). Uma organização tem que estar preparada para recuperar (restaurar) todos os seus dados de forma íntegra caso um incidente de perda de dados venha a ocorrer. Assim, estabelecem-se as regras:

- Todo sistema ou informação relevante para a operação das atividades do Instituto Diretrizes, deve possuir cópia dos seus dados de produção para que, em eventual incidente de indisponibilidade de dados, seja possível recuperar ou minimizar os impactos nas operações da instituição;
- Todos os backups devem ser automatizados por sistemas de agendamento para que sejam, preferencialmente, executados fora do horário comercial, períodos de pouco ou nenhum acesso de usuários ou processos aos sistemas de informática;
- Toda infraestrutura de suporte aos processos de backup e restauração deve possuir controles de segurança para prevenção contra acessos não autorizados, bem como mecanismos que assegurem seu correto

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

funcionamento.

- Empresas parceiras e terceiros que utilizam sistemas ou aplicativos são responsáveis por executar seus próprios backups

10. MONITORAMENTO E CONTROLES

10.1. CONTROLE DE ACESSOS:

A gestão de acessos aos sistemas e redes do Instituto Diretrizes é conduzida de forma sistemática. A equipe de TI realiza verificações abrangentes, incluindo:

A inclusão e desativação de colaboradores são comunicadas prontamente pelo departamento de Recursos Humanos da unidade do Instituto Diretrizes por meio da plataforma de atendimento da TI.

Mensalmente, é efetuada uma revisão comparativa dos acessos aos sistemas e redes em relação à lista de colaboradores ativos fornecida pelo RH. Esse processo compara os nomes e a quantidade de usuários registrados e habilitados com a lista de colaboradores ativos fornecida pelo RH.

10.2. REDIRECIONAMENTOS DE E-MAIL

Considerando que os e-mails corporativos são utilizados pelo setor, e não estão vinculados a um usuário específico, qualquer redirecionamento de e-mail deverá ser autorizado pela Diretoria matriz, devendo ser comunicado imediatamente após o desligamento do colaborador, para as devidas trocas de senhas de acesso.

A equipe de TI é encarregada de realizar revisões trimestrais para monitorar os prazos de exclusão dos redirecionamentos.

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP

www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

10.3. UTILIZAÇÂO DE E-MAILS

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

- O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;
- Os e-mails enviados ou recebidos de endereços externos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;
- É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo "corrente", campanhas ou promoções;
- É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;
- É proibido enviar qualquer mensagem por meios eletrônicos que torne o Instituto Diretrizes vulnerável a ações civis ou criminais;
- É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;
- Produzir, transmitir ou divulgar mensagem que:
- Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
- Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl, reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 - Sala 1501 - Dezoito do Forte Empresarial/Alphaville CEP: 06472-002- Barueri/SP
www.institutodiretrizes.org.br

- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

11. USO DE EQUIPAMENTOS PARTICULARES E DISPOSITIVOS MÓVEIS

O objetivo do Instituto Diretrizes é maximizar a agilidade e eficiência da realização das tarefas dos colaboradores, contando com todos os recursos de equipamentos disponíveis, mas não pode deixar de considerar os requisitos de segurança da informação, por isso estabelece algumas regras para o uso de equipamentos de propriedade particular e de dispositivos móveis. Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, seja de propriedade do Instituto Diretrizes ou particular com prévia aprovação e permissão pelo setor de Tecnologia da Informação, como: notebooks, smartphones e pendrives. Todas as regras do tópico "Posto de Trabalho" se enquadram nesta seção, adicionalmente a:

- Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede interna do Instituto Diretrizes, mediante autorização do chefe

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

imediato e preenchimento de Termo de Responsabilidade de Uso de Dispositivo Particular na Rede Corporativa;

- O setor de Tecnologia da Informação deverá verificar as configurações de rede, do aplicativo de antivírus e demais aplicativos instalados para que o acesso à rede interna seja concedido. Aplicativos peer to peer, farejadores de tráfego, softwares que possam gerar carga excessiva na rede, que não estejam de acordo com a legislação vigente ou que possam trazer prejuízos à infraestrutura ou à imagem do Instituto Diretrizes não serão permitidos. Caso o equipamento não obedeça aos requisitos mínimos de segurança, o acesso não será concedido;
- O setor de Tecnologia da Informação tem o direito de, periodicamente, auditar os equipamentos utilizados, visando proteger suas informações bem como garantir que aplicativos ilegais não estejam sendo usados;
- É de responsabilidade do proprietário, a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pelo Instituto Diretrizes;
- É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook;
- Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;
- É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam ao Instituto Diretrizes não podem ser armazenados no disco rígido do notebook ou em dispositivos de armazenamento móvel (ex: pendrive), sem a autorização da área responsável pelos dados. Estes arquivos devem sempre ser armazenados no servidor de compartilhamento destinado para tal;

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

Mesmo nos computadores portáteis fornecidos pelo Instituto Diretrizes, é proibido o armazenamento de informações privadas no disco rígido do equipamento.

12. SEGURANÇA DO AMBIENTE DE TI

As máquinas (servidores) que armazenam sistemas e dados do Instituto Diretrizes estão em área protegida – Data Centers local;

- Todos os sistemas ou equipamentos classificados como críticos devem ser mantidos em áreas seguras;
- A entrada aos Data Centers tem acesso devidamente controlado e monitorado;
- As áreas do Data Centers devem ser protegidas com barreiras de segurança ou mecanismos de acesso, de forma a impedir o acesso não autorizado;
- A porta dos Data Centers deve permanecer fechada, com mecanismo de autenticação individual quando possível;
- O acesso às dependências dos Data Centers com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da equipe de Tecnologia da Informação e mediante supervisão;
- O Data center deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do SHL;
- Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

13. INSTALAÇÃO E GERENCIAMENTO DE ANTIVÍRUS

Todo arquivo em mídia (Pendrives, CD-ROM, DVD, etc) proveniente de propriedade externa, deve ser verificado pelo programa de antivírus. Desta forma, todas as estações de trabalho e notebooks terão o programa de antivírus instalado e atualizado automaticamente.

O usuário não deve cancelar o processo de verificação de vírus quando este for iniciado automaticamente na sua estação de trabalho.

Cabe à TI manter o antivírus sempre atualizado e com a autoproteção ativa nas estações de trabalho do Instituto Diretrizes, a manutenção e controle nos ambientes de servidores hospedados na nuvem são de responsabilidade do fornecedor provedor do serviço de sistema, contratado pelo Instituto Diretrizes.

14. RECURSOS DE IMPRESSÃO

Apenas os usuários que receberam autorização prévia têm permissão para acessar os recursos de impressão. A configuração da impressora na estação de trabalho do usuário será efetuada exclusivamente por técnicos autorizados do departamento de Tecnologia da Informação.

15. INSTALAÇÃO DE SOFTWARE

Para qualquer software, seja ele de código aberto ou com licença, que precise ser instalado por exigência das atividades do setor, é obrigatório obter a autorização do gestor direto e da equipe de Tecnologia da Informação (TI).

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

16. POSTO DE TRABALHO

Os usuários são responsáveis por manter os equipamentos de informática sob sua supervisão em bom estado de conservação, e não devem comer, beber e ou manipular insumos nas proximidades desses equipamentos, que possam afetar a vida útil do equipamento.

É estritamente proibido que os usuários abram as estações de trabalho ou façam modificações na configuração do hardware e dos programas locais instalados. Além disso, é crucial que os usuários bloqueiem seus computadores contra acessos não autorizados sempre que se afastarem de suas estações de trabalho. No caso de identificarem a necessidade de atualizações ou da instalação de aplicativos relacionados às suas funções, devem solicitar assistência à equipe de Tecnologia da Informação.

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

- É de responsabilidade do colaborador do equipamento zelar por ele, mantendo-o em boas condições;
- Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar e retirar a etiqueta de patrimônio;
- É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe de Tecnologia da Informação;
- As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas;
- É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento só poderá ser realizado pela

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

equipe de Tecnologia da Informação;

- É proibida a instalação de softwares que não possuam licença e/ou não sejam homologados pela equipe de Tecnologia da Informação;
- As estações de trabalho devem permanecer bloqueadas (logoff) nos períodos de ausência do colaborador;
- Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
- Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;
- É proibido o uso de estações de trabalho para:
- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
- Burlar quaisquer sistemas de segurança;
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- O setor de Tecnologia da Informação não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição;
- As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP

www.institutodiretrizes.org.br

estação de trabalho é de responsabilidade do funcionário.

17. DIREITOS DE PROPRIEDADE

O Instituto Diretrizes detém a responsabilidade de toda a documentação, procedimentos, instruções de trabalho, processos, fluxos e criações desenvolvidas por funcionários ou fornecedores durante seu período de emprego ou contrato com a organização.

Em situações de término ou rescisão do contrato de prestação de serviços, independentemente do motivo, é obrigatório que o indivíduo devolva todas as informações confidenciais que foram geradas ou manuseadas no decorrer da prestação dos serviços.

18. PROTEÇÃO DE DADOS PESSOAIS

O tratamento de dados pessoais se dará de acordo com as bases legais previstas nas hipóteses dos artigos 7º e 11º, da Lei 13. 709/2018 (Lei Geral de Proteção de Dados), as quais estarão sujeitos os serviços, para propósitos específicos, explícitos, legítimos e informados ao titular dos dados.

18.1. IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS

A proteção de dados pessoais é de extrema importância nos tempos modernos por várias razões, e sua relevância só tem aumentado à medida que a tecnologia e a coleta de dados se tornam cada vez mais presentes em nossa vida cotidiana.

Haja vista que, as pessoas precisam se sentir respeitadas, protegidas e devem confiar na empresa.

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP

www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

18.2. RESPEITO DA PRIVACIDADE

A proteção de dados assegura a privacidades das pessoas, permitindo que elas compartilhem suas informações somente com a empresa e pessoas de sua confiança. Sendo assim, seus dados ficam protegidos.

18.3. SEGURANÇA DOS DADOS

Não compartilhar os dados aleatoriamente é importante para a proteção do detentor das informações. Tendo em vista que, é capaz de evitar fraudes, falsificações de identidade e uma série de crimes que estão cada vez mais comuns usando as informações pessoais que foram coletadas de forma irresponsável.

18.4. A QUEM COMPETE A PROTEÇÃO DE DADOS

Todos profissionais que lidam com dados pessoais e sensíveis se comprometem a cumprir toda legislação aplicável sobre a segurança da informação, privacidade e proteção de dados, inclusive normas setoriais sobre o tema e a que estejam submetidas, sendo dever de todos:

i. cumprir a legislação aplicável, especialmente a LGPD, mantendo um programa de governança em privacidade e proteção de dados, que inclua medidas físicas, técnicas, administrativas e organizacionais de proteção proporcionais à natureza dos Dados Pessoais tratados;

ii. atender eventuais solicitações de autoridades brasileiras, incluindo a ANPD, sempre que figurar como Controlador dos Dados Pessoais na respectiva operação de Tratamento;

iii. não reter quaisquer Dados Pessoais após o atingimento das finalidades para as quais os Dados Pessoais foram coletados,

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 - Sala 1501 - Dezoito do Forte Empresarial/Alphaville CEP: 06472-002- Barueri/SP
www.institutodiretrizes.org.br

devendo eliminá-los após tal condição, autorizada a conservação nas hipóteses previstas na LGPD;

iv. respeitar os direitos dos Titulares previstos na LGPD e, sempre que figurar como Controlador dos Dados Pessoais na respectiva operação de Tratamento, responder às solicitações dos Titulares; e

v. manter atualizado o registro de operações de Tratamento de Dados Pessoais.

19. PENALIDADES

As sanções previstas para esta política estão em conformidade com as orientações estabelecidas no Código de Ética e Conduta Corporativa do Instituto Diretrizes.

20. VIGÊNCIAS E VALIDADES

Este documento não possui um prazo definido e torna-se efetivo após a sua aprovação. Deve ser revisto e atualizado sempre que ocorrerem eventos ou fatos significativos que justifiquem tal revisão.

21. DEFINICÕES

21.1. INFORMAÇÃO

Refere-se à coletânea ou conjunto de dados e conhecimentos resultantes do processamento, manipulação e/ou organização de informações, de modo a representar uma alteração (tanto quantitativa quanto qualitativa) no entendimento do sistema, seja ele humano ou computacional, que a recebe.

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte Empresarial/Alphaville CEP: 06472-002– Barueri/SP

www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

21.2. SEGURANÇA DA INFORMAÇÃO

Engloba um conjunto de medidas e controles cujo propósito é assegurar a preservação dos princípios de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações. Isso contribui para a realização dos objetivos estratégicos da organização.

21.3. INTEGRIDADE

Refere-se à garantia de que a informação permanece inalterada em seu estado original, protegendo-a contra modificações indevidas, sejam elas intencionais ou acidentais, bem como contra possíveis ameaças.

21.4. CONFIDENCIALIDADE

Significa garantir que o acesso às informações seja concedido exclusivamente a pessoas autorizadas, impedindo que informações sensíveis sejam divulgadas a terceiros não autorizados.

21.5. DISPONIBILIDADE

Assegura que os usuários autorizados possam acessar as informações e os ativos correspondentes sempre que necessário, evitando interrupções indevidas ou falhas que possam prejudicar o acesso.

21.6. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Refere-se a um evento resultante da ação de uma ameaça que aproveita uma ou várias vulnerabilidades e que impacta qualquer um dos aspectos da segurança da informação, como confidencialidade, integridade ou disponibilidade.

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

21.7. RISCO DE SEGURANÇA DA INFORMAÇÃO

São os perigos relacionados à possível quebra da confidencialidade, integridade e disponibilidade das informações da empresa, seja em meios físicos ou digitais.

22. CONSIDERAÇÕES FINAIS

Da mesma forma que a ética, a segurança deve ser considerada uma parte essencial da cultura do Instituto Diretrizes.

Qualquer incidente de segurança é entendido como uma ação contrária aos princípios éticos e às normas de conduta estabelecidas pela Instituição. Esta Política de Segurança da Informação estará sempre disponível para consulta a qualquer momento, no Portal de Transparência do Instituto Diretrizes.

É responsabilidade de cada usuário manter-se informado sobre esta Política de Segurança e os procedimentos relacionados, buscando orientação junto ao seu gestor ou à equipe de Tecnologia da Informação (TI) sempre que houver dúvidas em relação à obtenção, uso e descarte de informações.

HISTÓRICO DE DOCUMENTO		
VERSÃO	**DATA**	**DESCRIÇÃO DA ALTERAÇÃO**
1.0	**03/02/2025**	**Novo Template**

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte
Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br

POLÍTICA INSTITUCIONAL

ASSINATURAS	
Assinado por: Thiago Maia Carvalhaes 62ab566d-d57c-4... _____ Thiago Carvalhaes Diretor Administrativo Adjunto **Verificador** *Instituto Diretrizes*	Assinado por: Margareth Mollina 9035639f-d936-4... _____ Margareth Mollina Gerente da Qualidade **Aprovador** *Instituto Diretrizes*

CNPJ:10.946.361/0001-89
Avenida Ipanema, 165 – Sala 1501 – Dezoito do Forte Empresarial/Alphaville CEP: 06472-002– Barueri/SP
www.institutodiretrizes.org.br