DIRECIONAL ENGENHARIA S/A

Companhia Aberta de Capital Autorizado - CVM nº 21.350
CNPJ 16.614.075/0001-00
NIRE 31300025837

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

"Certificamos que o presente documento foi aprovado na Reunião do Conselho de Administração de 08 de novembro de 2021."

SUMÁRIO

1. OBJETIVO

Definir a política para o uso adequado dos serviços e recursos de Gerência de Tecnologia da Informação e proteção das Informações e dados de propriedade da Direcional Engenharia S.A e empresas coligadas e controladas, bem como para proteger os demais dados armazenados pela Companhia, de clientes e terceiros, descrevendo ainda as atividades consideradas violação ao uso dos serviços e recursos, as quais são proibidas.

Definir os princípios e requisitos taxativos para o tratamento de dados, inclusive os pessoais e sensíveis, sob o crivo da Lei nº 13.709/2018 ("LGPD"), para orientar e disciplinar as ações de Gerência de Tecnologia da Informação, visando garantir a criação, armazenamento, tratamento, segurança, integridade, confidencialidade, publicação e disponibilidade dos dados e informações de propriedade da Direcional e dados de terceiros tratados e armazenados.

Estabelecer diretrizes que permitam aos colaboradores, prestadores de serviços e terceiros envolvidos a seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Princípios sobre a preservação das informações da Direcional:

a) Confidencialidade: Garantia de que o acesso seja obtido somente por pessoas autorizadas.

b) Disponibilidade: Garantia da geração da informação através dos dados e fontes da Direcional e que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

c) Integridade: Garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda, transmissão ou publicação, contra alterações indevidas, intencionais ou acidentais.

Para assegurar esses itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.

É fundamental para a proteção e salvaguarda das informações que os usuários adotem a ação de Comportamento Seguro e consistente com o objetivo de proteção das informações, devendo assumir atitudes proativas e engajadas no que diz respeito à proteção das informações.

Campanhas contínuas de conscientização de Segurança da Informação serão utilizadas para monitoração e controle destas diretrizes. A Política de Segurança da Informação da Direcional é aprovada e revisada sob demanda e aprovada pela Diretoria.

2. GLOSSÁRIO

Para melhor aplicação desta política é necessário o conhecimento dos seguintes conceitos e abreviaturas:

Bit Torrent: Software de compartilhamento de arquivos entre usuários em forma de protocolo de rede *peer to peer* que permite ao utilizador realizar downloads de arquivos sem que o arquivo em si precise estar em um servidor.

Canais de Broadcast: Meio usado para transmitir informações ou dados sem distinção de remetentes.

Cloudcomputing: Tecnologia que permite o uso remoto de recursos da computação por meio da conectividade da Internet;

Data Protection Officer: Também conhecido como DPO ou Encarregado, nos termos da Lei nº 13.709/2018 ("LGPD"), é o responsável da empresa para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

E-mail Bombing: Forma de ataque que consiste em enviar um volume muito alto de e-mails para um endereço de e-mail específico tendo como objetivo interromper o serviço de correio eletrônico do destinatário.

Kazaa: Software de compartilhamento de arquivos entre usuários em forma de protocolo de rede peer to peer que permite ao utilizador realizar downloads de arquivos sem que o arquivo em si precise estar em um servidor.

Peer-to-Peer: Arquitetura de redes de computadores onde cada um dos pontos ou nós da rede funcionamos tanto como cliente quanto como servidor, permitindo compartilhamentos de serviços e dados sem a necessidade de um servidor central.

Sniffers: Programas de computador que capturam trafego e analisam da rede.

VPN: Rede de comunicações privada e criptografada construída sobre uma rede de comunicações pública para acesso seguro entre dois pontos.

Worm: Programa malicioso autoreplicante usado para infectar computadores.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Direcional Engenharia S.A para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos seus usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2005, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

4. APLICAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As diretrizes aqui estabelecidas deverão ser seguidas por todos os integrantes da Direcional Engenharia S.A, incluindo empregados, administradores, conselheiros, fornecedores, prestadores de serviços, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a todos os integrantes de que os ambientes, sistemas, computadores, celulares e redes da empresa, bem como qualquer dispositivo conectado à rede da Direcional, poderão ter seu uso e conteúdo monitorados e gravados, sem necessidade de prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada integrante se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor ou da Gerência de Tecnologia da Informação sempre que não estiver absolutamente seguro quanto à aquisição, uso, armazenamento e/ou descarte de informações.

4.1. AUTORIDADE E RESPONSABILIDADE DE APROVAÇÃO

4.1.1. DA GERENCIA E DIRETORIA

a) Analisar e aprovar os instrumentos normativos e operacionais relacionados à adoção desta Política de Segurança da Informação e aos treinamentos necessários para manter a segurança da informação;
b) Avaliar criticamente, periodicamente, esta política e os indicadores de segurança da informação.

4.1.2. DOS INTEGRANTES

a) Entende-se por integrante toda e qualquer pessoa física, contratada CLT (empregados), administradores, conselheiros, fornecedores ou prestadores de serviços por intermédio de pessoa jurídica ou não, que exerçam alguma atividade dentro ou fora da Direcional;

4.1.3. DOS GESTORES

a) Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
b) Aprovar ou solicitar os acessos dos colaboradores aos dados, informações, processos e sistemas da Direcional;
c) Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviço ou de parceria, a responsabilidade do cumprimento desta Política.

4.1.4. DO ENCARREGADO

a) Analisar e aprovar, em conjunto com a Gerência e Diretoria, os instrumentos normativos e operacionais relacionados à adoção desta Política de Segurança da Informação e aos treinamentos necessários para manter a segurança da informação;
b) Avaliar criticamente e periodicamente esta política e os indicadores de segurança da informação.

4.2. DIRETRIZES BÁSICAS QUE REGULAMENTAM O PROCESSO

Toda informação produzida ou recebida pelos integrantes como resultado da atividade profissional exercida no âmbito da Direcional Engenharia S.A é de propriedade exclusiva da Direcional Engenharia S.A. As exceções devem ser explicitadas e formalizadas em instrumento apartado.

Os equipamentos de informática e comunicação, sistemas e informação devem ser utilizados pelos integrantes, para fins exclusivos de realização das atividades profissionais concernentes ao cargo e função que ocupam na estrutura da Direcional Engenharia e empresas coligadas e controladas.

A Direcional, por meio da área de Gerência de Tecnologia da Informação, registrará todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

É dever de todo integrante da Direcional Engenharia S.A:

a) Proteger os ativos e informações que estejam sob sua custódia e por todos os atos executados com sua identificação de acesso (qualquer que seja sua forma, a identificação será pessoal, intransferível e permitirá de maneira clara e indiscutível o seu reconhecimento);
b) Deve ser evitado o uso de qualquer equipamento pessoal para utilização de tarefas coorporativas dentro ou fora da Direcional. A utilização de equipamentos (notebooks, celulares, tablets, etc) pessoais para realização das atividades corporativas, somente será permitida mediante a aprovação do gestor ou do contratante do setor, sendo certo que o tratamento de dados no uso do equipamento será monitorado, sendo ainda passível de auditoria de segurança antes do ingresso à rede ou após o encerramento das atividades do profissional na Direcional. Caso o equipamento auditado não atenda aos requisitos mínimos de segurança da Direcional, o mesmo não terá acesso à rede coorporativa da Direcional.
c) Ao optar pelo uso de equipamentos pessoais, fica a cargo do proprietário do equipamento arcar com o licenciamento de todos os softwares instalados. O proprietário será responsabilizado e deverá arcar com as penalidades prevista na legislação sobre uso de softwares.
d) Fica proibida a instalação de softwares não homologados nos computadores da Direcional. As necessidades de instalação de softwares deverão ser realizadas mediante abertura de chamados no portal CSC.
e) Fica proibida a divulgação de informações, acerca das operações de quaisquer das empresas do Grupo Direcional, fora do ambiente de trabalho;
f) É também obrigação de cada integrante se manter atualizado em relação a esta política e aos seus procedimentos e normas relacionadas, buscando orientação do seu gestor, da área Gerência de Tecnologia da Informação ou do Encarregado sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações;
g) Será de inteira responsabilidade de cada integrante, todo o prejuízo ou dano que vier a sofrer ou causar à Direcional e/ou a terceiros em decorrência de não obediência às diretrizes e normas aqui referenciadas;
h) Para liberação das portas USB dos desktops e notebooks é necessário justificar o uso e a aprovação do gestor do departamento do solicitante e do Encarregado.
i) Os usuários de mídias removíveis são diretamente responsáveis pelos riscos e impactos que o uso de tais dispositivos possa vir a causar nos ativos de informação, pois este tipo de mídia pode conter vírus e softwares maliciosos podendo danificar e corromper dados;
j) O armazenamento de informações corporativas em mídias removíveis é expressamente proibido. As exceções serão analisadas, caso a caso, com os Gestores de Área e Encarregado, cuja liberação ocorrerá por meio de processo de aprovação, mediante a assinatura de termo de responsabilidade, devidamente documentado;
k) Utilizar os equipamentos fornecidos pela Direcional apenas para a realização de suas rotinas de trabalho junto à empresa;
l) Abster-se de utilizar o wireless fornecido pela Direcional para qualquer fim contrário às leis.

4.2.1. GESTÃO DE CONTEÚDO E MÍDIAS REMOVÍVEIS

Fica proibido o armazenamento de arquivos que não estejam relacionados diretamente ao negócio da Direcional, tais como arquivos de filmes, fotos pessoais ou de terceiros, músicas, vídeos, em suas estações de trabalho, nos equipamentos portáteis (notebooks, smartphones, Pen Drives etc.), nos servidores e sistemas da rede da Direcional e nos diretórios compartilhados. Fica concedido o direito aos responsáveis pela Gerência de Tecnologia de Informação da Direcional e do Encarregado, de remover, quando encontrados estes arquivos, sem aviso prévio, e o direito de utilizá-los em procedimentos de Auditoria e prestação de contas à Autoridade Nacional de Proteção de Dados, se necessário.

Todas as informações, documentos e dados técnicos que constituem o capital intelectual da Direcional, independentemente de sua classificação, devem ser salvos nas unidades de rede da Direcional. Entende-se por unidades de rede os repositórios de documentos do file server.

Caso estas informações sejam armazenadas em outros locais não aprovados previamente pela Gerência de Tecnologia de Informação, tais como: disco local do computador, HD externos, pendrive, correio eletrônico, drivers virtuais (One Drive pessoal, DropBox, iCloud, etc.), cópias físicas, dentre outros, as mesmas não terão sua integridade e confidencialidade garantidas. E, em caso de perda, o Integrante que realizou o uso indevido será responsável por todos os danos ou prejuízos causados à Direcional ou a terceiros.

As estações de trabalho não serão objeto de procedimentos de backup. Somente e-mails armazenados na Caixa de Entrada e Subpastas associadas serão copiados. Diariamente o backup é realizado apenas para os servidores de arquivos.

O uso de mídias removíveis na empresa não é estimulado, devendo ser tratado como exceção.

Informações devem ser transmitidas usando as ferramentas corporativas (email, rede de dados, software de mensageria, etc) que proveem a segurança requerida.

Os usuários de mídias removíveis, caso comprovado, serão responsabilizados quando os mesmos causarem dano à direcional, seja por perda/vazamento de informação confidencial e/ou permitir a entrada de vírus ou softwares maliciosos na rede corporativa.

Caso seja necessário transportar arquivos através de mídias removíveis (HD Externo ou PenDrive) é recomendado que os arquivos sejam criptografados e apagados, posteriormente, afim de evitar vazamento de informação sensível.

Os arquivos armazenados na estrutura de troca de arquivos (P:\Público) serão apagados em rotina diária, pela área de Tecnologia da Informação.

As soluções de armazenamento e gestão de conteúdo, fornecidas e providenciadas pela área de Gerência de Tecnologia da Informação e pelo Encarregado, deverão ser prontamente atendidas pelos usuários, não cabendo o direito a outra solução alternativa.

Os usuários são responsáveis pelo destino e armazenamento dos documentos digitalizados

4.2.2. CORREIO ELETRÔNICO / Microsoft Teams (CHAT CORPORATIVO)

O objetivo desta norma é informar aos colaboradores da Direcional Engenharia S/A quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico (e-mail) é para fins corporativos e relacionados às atividades do integrante dentro da instituição, sendo proibida sua utilização para fins pessoais.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Redirecionamento automático de e-mails da Direcional para endereços externos;
- Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a Direcional Engenharia vulnerável a ações civis ou criminais;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pela Direcional;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- Apagar mensagens pertinentes de correio eletrônico quando a Direcional estiver sujeita a algum tipo de investigação;
- Utilizar o e-mail como repositório de documentos.

Produzir, transmitir ou divulgar mensagem que:

- Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da Direcional;
- Contenha ameaças eletrônicas, como: spam, e-mail bombing, vírus de computador;
- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise a obter acesso não autorizado a outro computador, servidor ou rede;
- Vise a interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise a burlar qualquer sistema de segurança;
- Vise a vigiar secretamente ou assediar outro usuário;
- Vise a acessar informações confidenciais sem explícita autorização do proprietário;
- Vise a acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Contenha anexo(s) superior(es) a 15 MB para envio (interno e internet) e 15 MB para recebimento (internet)
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física, mental ou outras situações protegidas;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

4.2.3. ACESSO

Os gestores de cargo gerencial e o Encarregado, no mínimo, serão responsáveis por definir as permissões de acesso às informações de sua área (acesso aos diretórios, sistemas, intranet, etc.), de acordo com o Formulário de Concessão de Acesso disponível na Portal do CSC no endereço (Inicio/Processos/Iniciar Solicitações /Gestão de Chamados de TI).

Caso o gestor e/ou o Encarregado não esteja disponível para autorização dos acessos, o formulário deverá ser enviado pelo superior imediato do gestor.

Diante da necessidade de criação ou exclusão de contas de usuários, sejam eles fixos, temporários ou terceiros, os gestores das áreas deverão enviar a solicitação para a área de Gerência de Tecnologia da Informação. Apenas a área de Gerência de Tecnologia da Informação tem permissão para bloquear ou criar contas de usuários funcionais.

Todos os Integrantes que não efetuarem acessos à rede ou acesso ao e-mail em um período igual ou superior a 30 dias terão suas contas bloqueadas automaticamente; se o fato perdurar por mais 30 dias, as suas contas serão extintas. Diante da ocorrência de uma ausência temporária do Usuário, superior a 40 dias, caberá a ele ou a seu gestor comunicar o fato à área Gerência de Tecnologia da Informação para evitar a extinção da conta.

Fica terminantemente proibido aos usuários tentar burlar os sistemas de segurança instalados pela Direcional, que tem como objetivo garantir a Integridade, Segurança e Confidencialidade da rede e suas informações. A mesma proibição é utilizada para o acesso a sites de internet.

4.2.4. SENHAS

Os dispositivos de identificação e senhas protegem a identidade do integrante, evitando e prevenindo que uma pessoa se faça passar por outra perante a companhia e/ou terceiros.

Fica proibido o compartilhamento de quaisquer senhas ou identificação de uso pessoal com outros Usuários, bem como o armazenamento em locais visíveis a terceiros.
As senhas devem atender os seguintes requisitos e regras de acesso e bloqueio:

a) Tamanho mínimo de senhas: 10 caracteres.
b) Tempo máximo para troca de senhas: 45 dias.
c) Histórico de senhas: não permite utilizar as 6 últimas senhas definidas pelo usuário.
d) Complexidade mínima de senhas:
   - Letras maiúsculas (A até Z) ou letras minúsculas (a até z).
   - Números (0 até 9).
   - Caracteres especiais (exemplo: $, #, %).
e) Bloqueio da conta de usuário após tentativas inválidas de utilização de senha: 03 tentativas.
f) Data de expiração da conta de usuários terceiros: definido de acordo com tempo de contrato ou permanência do terceiro no grupo Direcional com prazo máximo de 90 dias.
g) Bloqueio automático da estação de trabalho: após 15 minutos de inatividade.

4.3. INTERNET

Todas as regras atuais da Direcional visam basicamente ao desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet no âmbito da Direcional Engenharia S/A está sujeita a divulgação e auditoria pela Gerência de Tecnologia de Informação e pelo Encarregado.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento desta Política de Segurança da Informação.

A Gerência de Tecnologia da Informação, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer Integrante, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao Integrante e ao respectivo gestor, quando aplicável. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus integrantes deve ser utilizada com moderação, pautada nos princípios éticos e morais da instituição. A utilização da internet para acesso a sites e utilização de aplicativos que contrariem as leis vigentes é terminantemente proibida, assim como a realização de qualquer download relacionado à práticas ilegais/abusivas/imorais.

Como é do interesse da Direcional que seus integrantes estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários

estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os integrantes que estão devidamente autorizados a falar em nome da Direcional Engenharia para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, seja por documento físico, entre outros.

Apenas os integrantes autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo, redes sociais ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet são expressamente proibidos. Qualquer software não autorizado baixado será excluído pela Gerência de Tecnologia da Informação.

Os integrantes não poderão em hipótese alguma utilizar os recursos da companhia para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

Como regra geral, materiais de cunho sexual não poderão ser baixados da internet, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado à Direcional ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os integrantes não poderão utilizar os recursos da companhia para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer (Kazaa, BitTorrent e afins) e serviços de streaming (rádios on-line, canais de broadcast e afins) não serão permitidos, salvo os Integrantes que o acesso a estes serviços é necessário para a execução das atividades

Não é permitido acesso a sites de proxy.

4.4. CONTROLE DE ACESSO VPN (Acesso remoto ao ambiente computacional da Direcional)

A solicitação de acesso ao VPN deverá ser aberta no Portal CSC e aprovada pelo Gestor do setor e pela Gerência da Tecnologia da Informação. Deve ser informado no chamado, as tarefas do integrante que levam à necessidade do acesso VPN.

Após a aprovação da solicitação aberta no portal CSC, o notebook corporativo do integrante deverá ser encaminhado ao departamento de Tecnologia da Informação para auditoria, instalação do cliente VPN, configurações e orientações de uso para o acesso.

O usuário deve restringir o uso do acesso via VPN para as finalidades relacionadas com os negócios devendo abster-se de usar a funcionalidade para quaisquer outras atividades.

É vetado aos usuários do serviço compartilhar credenciais de acesso via VPN com quem quer que seja, ou de acessar ele próprio o recurso VPN e conceder o uso da sessão a quaisquer outros funcionários.

O acesso VPN implica em riscos para a rede corporativa, uma vez que com ele é possível acessar à mesma, de forma privilegiada, a partir de qualquer ponto da internet, como se o usuário estivesse fisicamente nas instalações das empresas abrangidas neste procedimento. Por isso, deve o Integrante manter-se conectado à rede via acesso VPN apenas pelo tempo necessário à execução da tarefa que requereu o uso do serviço.

Importante! O Integrante nunca deve deixar sessões VPN abertas (logadas). Cada vez que o integrante deixar o seu equipamento conectado via VPN, deve executar logoff ou bloquear seu equipamento.

4.5. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponibilizados aos integrantes são de propriedade da Direcional, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instalados, ativados e atualizados permanentemente. O Integrante, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o Service Desk para que seja analisado.

Arquivos pessoais e/ou não pertinentes ao negócio da Direcional (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede.

Os colaboradores da Direcional e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Tecnologia da Informação.

No uso dos computadores, equipamentos e recursos de informática, os integrantes deverão seguir as seguintes regras:

- Todos os computadores de uso individual deverão ter senha de BIOS para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de Tecnologia da Informação da Direcional Engenharia, que terá acesso a elas para manutenção dos equipamentos.
- Os colaboradores devem informar ao Service Desk qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de Tecnologia da Informação da Direcional ou por terceiros devidamente contratados para o serviço.
- É vedada a movimentação de computadores ou outros equipamentos de informática que não seja realizado por um técnico da Gerência de Tecnologia da Informação da Direcional ou por terceiros devidamente contratados para o serviço.
- É vedada a utilização de modems internos ou externos quando os computadores estiverem conectados na rede da Direcional para impedir a invasão/evasão de informações, programas, vírus.
- O Integrante deverá manter a configuração do equipamento disponibilizado pela Direcional, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.

- Deverão ser protegidos por senha (bloqueados), todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pela Direcional devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da Direcional Engenharia:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para 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.
- Utilizar software pirata, atividade considerada delituosa de acordo com a legislação nacional.

4.6. SOLICITAÇÃO À ÁREA DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO

Toda e qualquer solicitação e/ou comunicação deve ser feita exclusivamente pelo portal do CSC no menu (Inicio/Processos/Iniciar Solicitações /Gestão de Chamados de TI) ou pelo e-mail ti@direcional.com.br.

Após o envio, em casos de comprovada excepcionalidade, a solicitação e/ou comunicação poderá ser feita por telefone ao responsável pelo Service Desk da Direcional.

Situações não previstas nesta política serão deliberadas pelo gerente da Gerência de Tecnologia da Informação em comum acordo com a Diretoria Financeira da Direcional.

4.7. REQUISITOS DE SEGURANÇA DO AMBIENTE FÍSICO

As máquinas (servidores) que armazenam sistemas da Direcional estão em área protegida – Data Centers localizados na Sede e em Computação na nuvem.

A entrada ao Data Center deverá possuir seu acesso devidamente controlado e monitorado.

A entrada nestas áreas ou partes dedicadas, por pessoas não autorizadas (visitantes, prestadores de serviço, terceiros e até mesmo funcionários, sem acesso liberado), que necessitarem ter acesso físico ao local, sempre o farão acompanhados de pessoas autorizadas.

O acesso às dependências da empresa com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, só pode ser feito a partir de autorização da Gerência de Tecnologia da Informação e mediante supervisão. Exceto para eventos e treinamentos organizados pela própria empresa.

As entradas na empresa respeitarão a Norma de Controle de Acesso de Visitantes e Colaboradores da empresa, sendo de responsabilidade da Área de Segurança Corporativa a atualização e verificação de referida normativa, com aprovação do Comitê de Segurança da Informação.

Respeitar áreas de acesso restrito, não executando tentativas de acesso às mesmas, ou utilizando máquinas alheias às permissões de acesso delimitadas a cada categoria de colaboradores.

4.8. DOS DADOS PESSOAIS

4.8.1. O Encarregado da Proteção de Dados - EPD é responsável por:

- Manter a Norma de Tratamento de Dados Pessoais atualizada;
- Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos;
- Receber comunicações da ANPD;
- Adotar providências;
- Orientar os funcionários e os contratados;
- Executar as demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares.

4.8.2. Todos os processos da empresa que tratem dados pessoais deverão obedecer à Norma de Tratamento de Dados Pessoais (Política de Privacidade da Organização).

4.8.3. A Política de Privacidade da Organização é o regramento sobre os seguintes aspectos para a proteção no tratamento de dados pessoais:

- Monitoramento de colaboradores;
- Uso de equipamentos pessoais próprios;
- Uso de Redes Sociais e Aplicativos de Comunicação;
- Uso da rede WiFi;

4.8.4. Todos os sistemas e serviços informatizados devem possuir características de rastreabilidade e auditabilidade por parte do Encarregado, inclusive para verificar quem efetuou pesquisa de determinado dado pessoal, com, no mínimo, usuário, origem, horário e ação.

4.8.5. Cabe essa determinação a todos os contratos terceirizados e sistemas de terceiros.

4.9. DO PLANO DE CONTINUIDADE DE NEGÓCIOS

O PCN – Plano de Continuidade de Negócios é de responsabilidade conjunta e solidária das diretorias, devendo ser estratégico em termos de negócio e operacional em termos de procedimentos e tecnologia.

O PCN deve estar atualizado e prever testes periódicos de recuperação de dados de backup.

5. HISTÓRICO DAS REVISÔES

Revisão	Histórico	Área responsável pela elaboração/revisão	Cargo do aprovador	Data
01	Versão inicial	Tecnologia da Informação	Diretor Presidente	01.01.2020
02	Versão revisada	Tecnologia da Informação	Sup.Seg da informação	09.12.2020