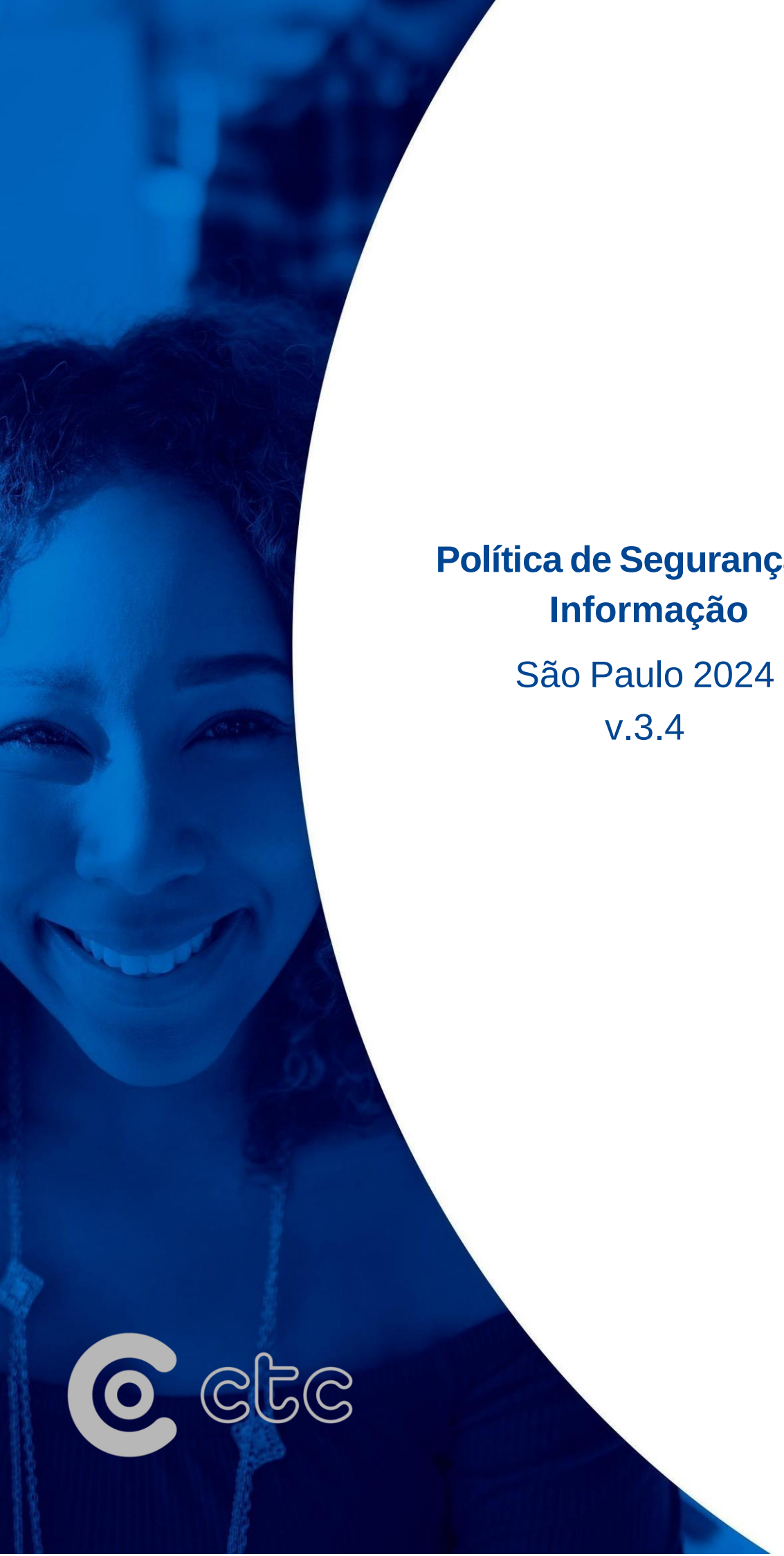

Política de Segurança da Informação

São Paulo 2024

v.3.4

Sumário

1. Distribuição e Vigência

Com fito de estabelecer as diretrizes de Segurança da Informação, a A **CONNECTCOM TELEINFORMATICA COMERCIO E SEVICOS LTDA**., denominada neste instrumento como *"CTC Tech"*, devidamente inscrita no CNPJ sob o nº 00.308.141/0001-76, implementou a presente POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI, cujo as diretrizes deverão ser rigidamente observadas para fins de manutenção de boas práticas, para a proteção de ativos e prevenção de sinistros. Ademais, destaca-se que as diretrizes aqui descritas devem ser adotadas, cumpridas e aplicadas em todas as áreas da instituição.

A CTC Tech reserva-se ao direito de alterar a presente versão da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO a qualquer momento, . Sem prejuízo da revisão anual a ser realizada, considerando o mês de publicação.

2. Objetivo

A CTC Tech estabelece a presente POLÍTICA DE SEGURANÇA DA INFORMAÇÃO fim de garantir a aplicação dos princípios e diretrizes de proteção de informações e da propriedade intelectual da organização, colaboradores, terceirizados, e clientes.

3. Público-Alvo

Esta política destina-se a todos os colaboradores, prestadores de serviço, empregados terceirizados, membros do corpo diretivo e demais empresas relacionadas à da CTC Tech. Para os fins do disposto no presente instrumento, o termo "*colaboradores"* abrange todos os funcionários, menores aprendizes, estagiários, consultores e administradores e membros do corpo diretivo da CTC Tech.

4. Escopo

O presente instrumento não se limita apenas as diretrizes contidas no mesmo, mas também conta em sua estrutura com normas complementares distribuídas e criadas em outros documentos aprovados.

A Política Geral de Segurança da Informação, assim como as demais normas e políticas complementares, se aplica a todos os usuários que possuem acesso à informação, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a CTC Tech abrangendo para todos os fins aos, ex-funcionários, ex - prestadores de serviço e demais colaboradores que possuem ou possuíram acesso às informações da CTC Tech, incluindo, mas não se limitando ao uso de recursos computacionais e tecnológicos compreendidos na infraestrutura da CTC Tech, não importando o regime jurídico ao qual estejam submetidos.

5. Regras

Todas as POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO deverão estar disponíveis em local de fácil acesso aos colaboradores e protegida contra alterações.

As POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO serão revisadas

anualmente e aprovada pelo Comitê de SI da CTC Tech.

6. Segurança da Informação

6.1. Princípios de Segurança da Informação

Nosso compromisso com o tratamento adequado das informações da CTC Tech, de seus colaboradores e clientes está fundamentado nos seguintes princípios:

6.1.1 Confidencialidade: Garantia de que o acesso à informação seja obtido somente por pessoas autorizadas e quando de fato necessário;

6.1.2 Disponibilidade: Garantia de que as pessoas autorizadas tenham acesso à informação sempre que necessário;

6.1.3 Integridade: Garantia de oferecer a exatidão e a completude da informação e dos métodos de seu processamento, bem como da transparência no trato com os públicos envolvidos.

6.1.4 Conformidade: Garantia de que o cumprimento dos requisitos, obrigações empresariais referentes à informação com as partes interessadas (colaboradores, clientes) e com aspectos legais e regulatórios relacionados a CTC Tech

6.1.5 Necessidade: O tratamento de dados pessoais realizado pela CTC Tech será limitado ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento;

6.1.6 Finalidade: a CTC Tech realizará o tratamento de dados pessoais apenas para propósitos legítimos, específicos, explícitos e informados ao titular de dados pessoais, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

6.1.7 Não Discriminação: a CTC Tech garantirá a impossibilidade de realização do tratamento de dados pessoais para fins discriminatórios ilícitos ou abusivos;

6.1.8 Responsabilização e Prestação de Contas: a CTC Tech se compromete a demonstrar a adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais, e a eficácia dessas medidas.

6.2. Diretrizes de Segurança da Informação

A Segurança da Informação da CTC Tech estabelece os principais controles, denominados diretrizes:

6.2.1 As informações da CTC Tech dos seus clientes e colaboradores deverão ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

6.2.2 A informação deverá ser utilizada de forma transparente e apenas para a finalidade e necessidade para a qual foi coletada.

O acesso às informações e recursos só deverá ser feito se devidamente autorizado pelo titular dos dados ou responsável previamente designado.

6.2.3 A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

6.2.4 A concessão de acessos deve obedecer ao critério de menor privilégio, no qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.

6.2.5 Os riscos de acesso às informações da CTC Tech deverão ser reportados ao comitê de segurança da informação através do email comite.seguranca@ctctech.com.br

6.2.6 As responsabilidades quanto à Segurança da Informação devem ser amplamente divulgadas aos colaboradores, que devem entender e assegurar a observância das diretrizes.

6.2.7 Os projetos de implementação e/ou implantações de novos sistemas operacionais e/ou softwares devem ser informados ao Comitê de Segurança da Informação, para análise e aderência as diretrizes e regras da presente Política de Segurança da Informação.

6.2.8 As normas e boas práticas de Segurança da Informação, bem como orientações de como deve ser utilizado o ambiente tecnológico não se esgotam ao presente instrumento, sobretudo em razão da constante evolução tecnológica, todos são responsáveis em notificar qualquer problema de segurança, sendo que a presente POLÍTICA DE SEGURANÇA DA INFORMAÇÃO será revisada periodicamente conforme a necessidade do negócio, visando garantir a segurança da informação.

6.3 Processo de Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, a CTC Tech adota os seguintes processos.

6.3.1 Gestão de Ativos: Os ativos devem ser identificados de forma individual, inventariados no sistema GLPI do departamento de Tecnologia da Informação (TI), protegidos contra acessos indevidos, acompanhado de documentação assinada digitalmente pelo colaborador no momento da entrega do equipamento e planos de manutenção de atualizações.

6.3.2 Classificação da Informação: As informações deverão ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

6.3.3 Gestão de Acessos: As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da CTC Tech. Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o colaborador ou prestador de serviço, para que seja responsabilizado por suas ações, de acordo com normas internas da CTC Tech. (Norma de Gestão de Acesso)

6.3.4 Gestão de Riscos: Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação (SW e HW) da CTC Tech, para que sejam recomendadas as proteções adequadas. Os cenários de riscos de segurança da informação são levantados e analisados pelo comitê de SI onde será encaminhado para a equipe responsável e retornar com solução definitiva ao risco.

6.3.5 Tratamento de Incidentes de Segurança da Informação: Os incidentes de Segurança da Informação da CTC Tech devem ser reportados ao Comitê de SI, o qual deve reportar a ANPD (Autoridade Nacional de Proteção de Dados) no caso de incidentes envolvendo vazamento de dados pessoais (casos graves), respeitando os processos de solicitação/incidente estabelecidos previamente.

6.3.6 Gestão de Crise:

Incidentes de segurança da informação serão tratados como uma crise, conforme os princípios definidos pelo comitê de SI:

- ✓ coleta de evidências, tão rápido quanto possível, logo após a ocorrência;
- ✓ escalação, conforme requerido;
- ✓ casos de vazamento de dados pessoais, deverão ser comunicados a ANPD
- ✓ garantia de que todas as atividades de respostas envolvidas são adequadamente registradas para análise futura;
- ✓ comunicação da existência de incidente de segurança da informação ou qualquer detalhe relevante para pessoas internas ou externas, clientes envolvidos ou organizações que precisam tomar conhecimento;
- ✓ tratamento das fragilidades de segurança da informação encontradas que causem ou contribuam para o incidente;
- ✓ uma vez que o incidente for formalmente tratado e solucionado, é necessário encerrar o incidente e registrar a solução na base de conhecimento.

6.3.7 Conscientização em Segurança da Informação: A CTC Tech promove a disseminação dos princípios e diretrizes de Segurança da Informação por meio de programas de conscientização, com o objetivo de fortalecer a cultura organizacional através de treinamentos aplicados na jornada de onboarding empresarial, devidamente disponibilizado na plataforma oficial de desenvolvimento LMS NEXT, disponíveis a todos os colaboradores e terceiros de forma obrigatória..

6.3.8 Serão aplicados treinamentos de conscientização a respeito das boas práticas de uso dos equipamentos, e sobre como manter a segurança do ambiente mesmo em ambiente de teletrabalho (Home-Ofice); que por sua vez, serão disponibilizados por vídeos, comunicações internas e publicações nas redes sociais da CTC Tech.

6.3.9 Governança com as Áreas de Negócio e Tecnologia: As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade e disponibilidade das informações.

6.3.10 Segurança Física do Ambiente de TI: O processo de Segurança Física visa estabelecer controles de acesso somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas.

6.3.10.1 A entrada ao Centro de Processamento de Dados (CPD) tem acesso devidamente controlado e monitorado por cameras de segurança.

6.3.10.2 A porta do CPD deverá permanecer fechada com mecanismo de autenticação individual.

6.3.10.3 O acesso ao CPD sem as devidas identificações poderá é permitido apenas em situações de emergência, quando a segurança física do CPD for comprometida, por incêndios, inundações, abalo da estrutura predial ou outros eventos catastróficos naturais, ou ainda, quando o sistema de autenticação não estiver funcionando.

6.3.10.4 Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno, ou inflamável. A entrada ou retirada de quaisquer equipamentos do CPD somente poderá ser concedida com o preenchimento da solicitação de liberação pelo colaborador solicitante com a respectiva autorização pelo Gestor de Segurança da Informação.

6.3.10.5 A entrada de *pen-drives,* HD interno/externo, HD HotSwap ou qualquer dispositivo similar, só serão liberados mediante autorização previa dos responsáveis do Gestor de Segurança da Informação.

6.4 Avaliação Independente da Auditoria

A efetividade das políticas de Segurança da Informação é verificada por meio de avaliações periódicas de auditoria.

7. LGPD

A CTC Tech, em observância a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709, de 14/08/2018, instituiu o compromisso de zelar pelos dados pessoais de seus colaboradores e de terceiros conforme estipulado nas cláusulas a seguir:

7.1 Privacidade: Assegurar o direito à privacidade e à proteção de dados pessoais dos colaboradores e de terceiros, por meio de práticas transparentes e seguras, garantindo direitos e liberdades fundamentais.

7.2 Transparência: Estabelecer regras claras sobre tratamento de dados pessoais da empresa.

7.3 Desenvolvimento: Fomentar o desenvolvimento econômico e tecnológico.

7.4 Padronização: Estabelecer regras únicas e harmônicas sobre tratamento de dados pessoais, independentemente do setor,

facilitando as relações e reduzindo custos decorrentes de incompatibilidades sistêmicas de tratamentos feitos por agentes diversos.

7.5 Proteção: Fortalecer a segurança das relações jurídicas e a confiança do titular no tratamento de dados pessoais.

8. Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios ediretrizes de Segurança da Informação da CTC Tech em todo o seu ciclo de vida: Geração, Manuseio, Armazenamento e Descarte.

9. Propriedade Intelectual

Quaisquer informações e propriedade intelectual que pertençam a CTC Tech, ou por ela disponibilizadas, não devem ser utilizadas para fins particulares, tão pouco repassadas a outrem, ainda que tenham sido obtidas, inferidas, incluídas ou desenvolvidas pelo próprio colaborador em seu ambiente de trabalho.

10. Uso dos equipamentos e estações de trabalho

As estações de trabalho, *notebooks* e celulares devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas das medidas de segurança abaixo especificadas deverão ser tomadas, quais sejam:

10.1 É de responsabilidade do colaborador zelar pelo equipamento disponível, mantendo-o em boas condições;

10.2 É proibido a abertura de computadores ou instrumentos tecnológicos para qualquer tipo de reparo pelos colaboradores. Caso seja necessário, o reparo deverá ser feito pela equipe de TI;

10.3 É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais. Este procedimento somente poderá ser realizado pela equipe de TI solicitados via chamado.

10.4 As estações de trabalho deverão permanecer bloqueadas (*logoff*) nos períodos de ausência do colaborador;

10.5 Os documentos e arquivos relativos à atividade desempenhada pelo colaborador, deverão obrigatoriamente ser armazenados em local próprio dentro do servidor da rede ou one drive, os quais possuem rotinas de backup e controle de acesso adequado, nunca no disco local da máquina;

10.6 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.

10.7 O departamento de Tecnologia da Informação (TI) da CTC Tech não se responsabiliza por manutenção e instalação de softwares em máquinas pessoais que não sejam os da instituição.

10.8 As estações de trabalho possuem nomes, os quais permitem que sejam identificadas na rede e no inventário do departamento de Tecnologia da Informação. Desta forma, tudo que for executado e instalado nas estações de trabalho ou qualquer outro dispositivo é de responsabilidade do colaborador.

11. Políticas de Senhas

A senha é a forma mais convencional de identificação e acesso do usuário, é um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra. O uso de dispositivos e/ou senhas de identificação de outra pessoa que não seja o usuário titular constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

11.1 À senha é de total responsabilidade do colaborador ou terceiro, sendo expressamente proibida a sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada em caso de suspeita de divulgação;

11.2 As senhas não devem ser anotadas e deixadas próximo ao computador, debaixo do teclado, colada no monitor, etc., mesmo em ambiente de teletrabalho (*Home-Office*).

11.3 No momento da criação da senha disponibilizada pela equipe de TI, o colaborador será forçado a trocar a senha no instante do primeiro login, sendo obrigatória a troca à cada **90 dias**.

11.4 Está desabilitada em nosso *Active Directory*, a função de armazenamento de senha com criptografia reversível, para dificultar a quebra.

11.5 As senhas devem seguir os seguintes pré-requisitos:Mínimo de oito caracteres;

Existência de caracteres dos seguintes grupos: letras maiúsculas,

letras minúsculas, números e caracteres especiais; Exemplo:(Senha3876W@)

11.5.1 Não devem ser baseadas em informações pessoais de fácil dedução (aniversário, nome do cônjuge, etc.).

11.5.2 É definido o limite de até 10 senhas memorizadas e utilizadas anteriormente.

11.5.3 Limite de bloqueio de conta, limitado até 5 tentativas de login, com contador de tempo de até 3 min, para minimizar incidentes de ataques de força bruta.

11.6 Os acessos de colaboradores devem ser imediatamente revogados mediante envio de e-mail ou abertura de chamados no GLPI do TI(RH), nas seguintes situações:

11.6.1 Desligamento do colaborador.

11.6.2 Período de recesso.

11.6.3 Afastamento.

12. E-mail

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.

13.1. O e-mail corporativo é destinado para fins profissionais, relacionados àsatividades dos colaboradores;

13.2. Os e-mails enviados ou recebidos poderão ser monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;

13.3. É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;

13.4. É proibido abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;

13.5. É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

13.6. Produzir, transmitir ou divulgar mensagem que:

13.6.1. Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;

13.6.2. 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;

13.6.3. Vise obter acesso não autorizado a outro computador, servidor ou rede;

13.6.4. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

13.6.5. Vise burlar qualquer sistema de segurança;

13.6.6. Vise vigiar secretamente ou assediar outro usuário;

13.6.7. Vise acessar informações confidenciais sem explícita autorização do proprietário;

13.6.8. Tenha conteúdo considerado impróprio, obsceno ou ilegal;

13.6.9. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo,violento, ameaçador, pornográfico entre outros;

13.6.10. Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos;

13.7. O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

13.7.1. Não contrariar as normas estabelecidas pelo presente instrumento;

13.7.2. Não interferir,negativamente, nas atividades profissionais individuais ou coletivas.

14. Antivírus e Firewall

A rede da CTC Tech é protegida pelo firewall, sistema responsável pela a filtragem de pacotes, controle de aplicação, análise de pacotes com logs para gerenciamento, juntamente com o antivírus no auxílio a proteção dos equipamentos. Haverá o bloqueio de sites de conteúdo impróprio, download de torrents, sites não oficiais de softwares e drivers de equipamentos, streamers de vídeos (considerados como sites improdutivos), e recursos de armazenamento de arquivos em nuvens não homologados pela CTC Tech.

15. Office 365

O Office 365 é uma das principais plataformas de trabalho e colaboração de equipes da empresa, com disponibilidade de diversos recursos de comunicação, como por exemplo, chat de mensagens, organizador de tarefas, ligações e videoconferências. Contudo é importante frisar que, com tantas facilidades de comunicação, surge a necessidade de normatização ante a exposição na web, para a correta utilização deste recurso.

15.1. É proibida a utilização dos recursos oferecidos do Office 365 para uso pessoal ou por terceiros que não façam parte da corporação, como;

15.1.1. Uso da ferramenta Microsoft Teams para envio de mensagens e ligações de vídeos chamadas que não sejam pelo proprietário da licença.

15.1.2. Instalar a suíte da Microsoft 365 em máquinas de terceiros ou de uso particular.

15.1.3. Utilizar o Onedrive Corporativo para salvar qualquer arquivo que não seja de utilidade da CTC Tech ou pertinente às suas atividades empresariais.

16. Papéis e Responsabilidades

16.1 A presente Política de Segurança da Informação baseia-se nas recomendações propostas pelas normas da ABNT NBR ISO/IEC 27002:2005 eNBR ISO/IEC 27001:2005, reconhecidas mundialmente por serem normas de boas práticas para a gestão da segurança da informação; bem como a BS 7799, do Bristsh Standard Institute, que compreendem as melhores práticas para o Gerenciamento de Segurança da Informação, segundo princípios éticos e legais.

16.2 A Política de Segurança da Informação tem por finalidade garantir a proteção de dados e a segurança dos seus ativos, atribuindo as responsabilidades, conscientizando e, se necessário, punindo, de maneira a mitigar riscos e garantir a segurança dos dados de evetuais ataques cibernéticos ou físicos.

16.3 As políticas, estratégias e processos corporativos de Segurança da Informação são elaboradas e supervisionadas pela Segurança da Informação e Comite de SI.

16.3.1 Gestor da Informação

O Gestor da Informação será o profissional responsável por:

- ✓ Realizar o gerenciamento das informações geradas e/ou de responsabilidade da sua área, durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte.

- ✓ Classificar e identificar as informações geradas ou que sejam de responsabilidade da sua área, tendo em vista quais informações são públicas, confidenciais ou de uso interno.

- ✓ Revisar e autorizar os acessos à informação e sistemas sob sua responsabilidade.

16.3.2 Gerência de Tecnologia da Informação

- ✓ A Gerência de Tecnologia da Informação deverá manter as topologias da arquitetura de rede da CTC Tech e reportar as suas atualizações. As respetivas topologias deverão ser documentadas, atualizadas e disponibilizadas para equipe técnica, possibilitando a continuidade de negócio da CTC Tech.

- ✓ Todas as arquiteturas de rede deverão atender aos requisitos de disponibilidade e capacidade de modo que atendam ao negócio.

16.3.3 Comitê de Segurança da Informação

São também atribuições do Comitê de Segurança da Informação

- ✓ A coordenação da comunicação e divulgação institucional desta política para recomendar medidas cabíveis para reduzir os riscos de segurança da informação, coordenar treinamentos periódicos e processos de conscientização que se fizerem necessários. Para tanto, poderá contar com a colaboração de equipes internas e externas, desde que estas sejam formalmente aprovadas e contratadas para este fim. Elevar níveis de maturidade dos processos, gerando planos de melhoria contínua para a Segurança da Informação.

- ✓ O comitê de Segurança da Informação poderá definir, a qualquer momento, novas diretrizes, ferramentas, políticas e ações para melhorar a segurança da informação, sendo que toda alteração definida será divulgada internamente.

16.3.4 Declaração de Responsabilidade

- ✓ Os Colaboradores, Prestadores de Serviços diretamente contratados pela CTC Tech devem aderir formalmente a um termo de responsabilidade, a fim de comprometerem-se a agir de acordo com a presente Política de Segurança da Informação. Os contratos firmados com a CTC Tech deverão possuir cláusulas que assegurem a confidencialidade das informações.

16.3.5 Medidas Disciplinares

- ✓ As violações desta política estão sujeitas às sanções disciplinares, previstas nas normas internas da CTC Tech, e demais normas legais vigentes.

17 Revisões e Política e Aprovações

17.1 O presente instrumento será revisado com periodicidade anual ou conforme o entendimento do Comitê de Segurança da Informação.

17.2 A Política de Segurança da Informação será aprovada pelo Comitê deSegurança da Informação.

18 Histórico de Revisões

Histórico de Revisões Ação	Versão	Nome Responsável	Descrição	Data
Revisão e alteração	3.2	Tarcisio Paciulo Castilho	Manter a política e incluir ordem título capitulo são 5, 6, 7, 16 e 17	17/11/2021
Revisão e alteração	3.4	Samuel Oliveira Sandes	Revisão da política com alteração de termos, remoção e adição de novos capítulos: 3, 4, 5, 6, 8, 9, 10, 11, 12, 14 e 16	01/04/2024

19 Aprovação

A presente política foi aprovada e entra em vigor a partir de:

Ação	Versão	Aprovador	Status	Data
Aprovado	3.3	Jackson Marinho	OK	26/01/2022
Aguardando Aprovação	3.4	Marcelo Silva Marcelo de Marchi	OK	26/06/2024