csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

Sistema de Gestão

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

SG-PO-001

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

1. Propósitos e princípios da Política de Segurança da Informação - PSI

Implementar as melhores práticas de segurança e privacidade da informação, tendo por finalidade atribuir responsabilidades, definir direitos, deveres, expectativas de acesso e uso, penalidades e promover uma cultura educativa organizacional de proteção dos dados e da informação da **CSP Tech**, de clientes, fornecedores e de parceiros.

Estabelecer as diretrizes para criação, transmissão, processamento, utilização, armazenamento, recuperação e descarte de informações a fim de preservar as informações quanto aos seguintes princípios:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, exata e completa;
- **Confidencialidade:** garantia de que o acesso à informação esteja disponível somente para pessoas, entidades ou processos autorizados;
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.
- **Autenticidade:** garantia da veracidade da autoria da informação;
- **Legalidade:** garantia de que a informação foi produzida em conformidade com a lei.

2. Referência

- NBR ISO IEC 27001: 2022;
- NBR ISO IEC 27002: 2022.

3. Procedimentos e planos para implementação da PSI

- SG-PL-006 Plano de Disponibilidade e Capacidade dos Serviços de Tecnologia da Informação
- SG-PL-002 Plano de Continuidade de Negócio
- SG-PR-004 Procedimento Gestão de Risco
- SG-PR-001 Procedimento Gestão da Informação Documentada
- SG-PR-014 Procedimento Gestão de Mudança
- SG-PR-006 Procedimento Gestão de Ativo e Configuração
- SG-PR-008 Procedimento Gestão de Incidente
- SG-PR-013 Procedimento Gestão de Evento
- SG-PR-009 Procedimento Gestão de Provedor Externo
- SG-PR-005 Procedimento Gestão de Acesso
- SG-PR-028 Procedimento Gestão de Privacidade
- SG-PR-012 Procedimento Administração de Sistema
- SG-PR-015 Procedimento Administração de Rede
- SG-PR-016 Procedimento Gestão de Vulnerabilidade Técnica
- SG-PR-010 Procedimento Administração de Facilities
- SG-PR-007 Procedimento de Desenvolvimento Seguro

4. Responsabilidades

4.1 Colaborador

4.1.1 É da responsabilidade de cada colaborador (pessoa física, independente do tipo de regime de trabalho), o prejuízo ou dano que vier a sofrer ou causar à **CSP Tech** ou a terceiros em decorrência da não obediência às diretrizes desta PSI.

4.1.2 Notificar os incidentes de segurança e privacidade da informação observados na **CSP Tech** via canal de denúncia oficial da empresa.

4.1.3 Notificar as fragilidades ou ainda, suspeitas de fragilidades de segurança e privacidade da informação observadas na **CSP Tech** ao comitê de segurança da informação.

4.2 Gestor

4.2.1 Incentivar e monitorar o cumprimento da PSI pelos colaboradores sob sua gestão.

4.2.2 Garantir a adaptação dos processos, procedimentos e sistemas sob sua responsabilidade para atender à PSI.

4.2.3 Segregar as funções dos colaboradores sob sua gestão a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e de evitar conflitos de interesses.

4.2.4 Definir os direitos e níveis de acesso dos colaboradores sob sua gestão.

4.2.5 Realizar análise crítica periódica das permissões de acesso em conjunto com Governança.

4.2.6 Definir os níveis de segurança e privacidade para as informações pertinentes ao seu processo e promover a rotulagem conforme política de classificação e tratamento da informação do item 7.

4.2.7 Identificar os riscos associados aos ativos da informação pertinentes ao seu processo e realizar a análise crítica periódica dos riscos associados aos ativos da informação.

4.2.8 Garantir que as informações pertinentes ao seu processo estejam protegidas contra perda ou dano por meio de backup.

4.3 Contratos

4.3.1 Atribuir aos clientes e aos provedores externos, na fase de formalização dos contratos de prestação de serviços, a responsabilidade pelo cumprimento de diretrizes aplicáveis desta PSI, conforme apropriado.

4.3.2 Atribuir aos colaboradores, na fase de formalização dos contratos individuais de trabalho, a responsabilidade com a segurança e privacidade da informação.

4.4 Comitê de Segurança e Privacidade da Informação

4.4.1 O Comitê de Segurança e Privacidade da Informação é multidisciplinar, necessariamente composto por representantes da área de Governança, Gestão de Pessoas, da Tecnologia da Informação e do Encarregado pela Proteção de Dados Pessoais.

4.4.2 Este comitê constitui um grupo de trabalho para tratar de questões, propor soluções, metodologias e processos específicos de segurança e privacidade da informação. Neste contexto, é responsável por analisar criticamente anualmente a PSI.

4.4.3 É responsável pela análise das infrações cometidas pelos colaboradores frente a esta PSI, com consequência de incidente, devendo examinar a gravidade e riscos sob o enfoque técnico e legal de cada infração cometida, resultando na recomendação de processo disciplinar para apuração dos fatos e aplicação das ações disciplinares cabíveis, para eventual e futuro encaminhamento às autoridades policiais ou judiciais, quando necessário.

4.4.4 Este Comitê poderá ser contatado a qualquer momento pelos colaboradores para esclarecer dúvidas, obter orientações, expressar opiniões, reportar situações de violação a esta PSI ou outros eventos de segurança e privacidade da informação, por meio da conta corporativa de e-mail csi@csptech.com.br.

4.5 Gestão de Pessoas

4.5.1 Garantir que, na fase de integração organizacional, os colaboradores participem das conscientizações sobre segurança e privacidade da informação e recebam esta PSI.

4.5.2 Na fase de integração organizacional, solicitar a assinatura do Termo de Ciência da Política de Segurança da Informação.

4.5.3 Garantir que os colaboradores participem das conscientizações periódicas sobre segurança e privacidade da informação disponibilizadas pela **CSP Tech**.

4.5.4 Solicitar os acessos e os recursos básicos para os novos colaboradores.

4.5.5 Aplicar sanções previstas nesta PSI quando for o caso.

4.6 Tecnologia da Informação

4.6.1 Segregar as funções administrativas e operacionais dos sistemas a fim de restringir ao mínimo necessário os privilégios de cada indivíduo e reduzir a existência de colaboradores que possam excluir os logs e trilhas de auditoria das suas próprias ações.

4.6.2 Monitorar e auditar o ambiente tecnológico, através da implantação de sistemas de monitoramento de servidores, correio eletrônico, conexões com a internet, dispositivos móveis, wireless e outros componentes da rede ou da nuvem.

4.6.3 Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança e privacidade da informação estabelecidos nesta PSI.

4.6.4 Promover treinamentos e conscientizações sobre segurança e privacidade da informação para a **CSP Tech**.

4.6.5 Manter os contatos de autoridades relevantes para a **CSP Tech** na Lista de Contatos das Autoridades Relevantes.

4.6.6 Manter os contatos de grupos de segurança e privacidade da informação na Lista de Contatos com Grupos de Conhecimento em SI.

5. POLÍTICA DE CONTROLE DE ACESSO

5.1 É de responsabilidade do colaborador, quaisquer acessos realizados com os dispositivos de identificação fornecidos pela **CSP Tech** pois estes são únicos, pessoais e intransferíveis.

5.2 Todos os dispositivos de identificação fornecidos pela **CSP Tech**, como o número de registro do colaborador, o crachá, o adesivo identificador, token, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm que estar associados a uma pessoa física e atrelados aos seus documentos oficiais reconhecidos pela legislação brasileira.

5.3 Os visitantes e prestadores de serviço terceirizados devem ser identificados distintamente dos funcionários tanto no acesso físico quanto no acesso lógico.

5.4 Deverá constar nos contratos da **CSP Tech** com colaboradores e com fornecedores, um Acordo de Responsabilidade com a Segurança da Informação, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação da **CSP Tech** ou dos seus clientes.

5.5 O acesso à informação e às funções dos sistemas de aplicação devem ser restringidos por meio de perfil de acesso dos colaboradores de forma a limitar quais dados e quais funções dos sistemas de aplicação poderão ser acessados por determinado colaborador e qual o nível de permissão.

5.6 O perfil de acesso deve estar baseado na premissa de menor privilégio do colaborador.

5.7 Os direitos de acesso devem ser revisados periodicamente.

5.8 A concessão, alteração e remoção de acesso deverão ser feitas pela **CSP Tech** mediante solicitação e autorização formal.

5.9 Os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

5.10 Os registros dos eventos (logs) significativos sobre o uso e a gestão de identidades dos usuários devem ser retidos.

- O Procedimento Gestão de Acesso apresenta o processo que viabiliza esta política.

6. POLÍTICA DE SENHA

6.1 Ao realizar o primeiro acesso ao ambiente de rede local, o colaborador deverá trocar imediatamente as suas senhas conforme as orientações apresentadas a seguir:

6.1.1 Todas as senhas de acesso devem ter, no mínimo, 8 caracteres.

6.1.2 As senhas não devem conter dados pessoais como nomes e sobrenomes, sequências identificáveis, datas comemorativas, números de documentos, placas de carros, números de telefones e similares.

6.1.3 A senha deve respeitar os 4 critérios de complexidade abaixo:

6.1.3.1 Uma ou mais letras minúsculas;

6.1.3.2 Pelo menos 1 letra maiúscula;

6.1.3.3 Pelo menos 1 caractere numérico;

6.1.3.4 Pelo menos 1 caractere especial (! @, #, $, %, %, &, ,*).

6.2 Devido à impossibilidade de adoção da complexidade de senha especificada no item 6.1.3 no celular corporativo, deve-se no mínimo:

6.2.1 Evitar sequências identificáveis, datas especiais, números de documentos, placas de carros, números de telefones e similares;

6.2.2 Ativar bloqueio de tela inicial e utilizar recurso de biometria e reconhecimento facial nos aplicativos que possuam este recurso.

A senha de acesso expirará automaticamente em 6 meses, sendo o colaborador notificado pelo sistema a partir de 15 dias antes do prazo máximo para alteração da referida senha.

6.3 Quando da renovação da senha, não serão aceitas as últimas 10 senhas já registradas.

6.4 Em caso de digitação errônea por 5 vezes consecutivas da senha de acesso, a conta será bloqueada.

6.5 O colaborador deve utilizar a autenticação de duplo fator em todos os sistemas que possuem este recurso.

6.6 O colaborador não deve utilizar a mesma senha em serviços e sistemas distintos.

6.7 As senhas não devem ser expostas, compartilhadas ou reveladas a outras pessoas.

6.8 Em caso de descoberta da senha por terceiros, o colaborador deverá trocar a senha, tão logo o fato seja percebido.

6.9 A alteração ou recuperação de senha de acesso aos sistemas poderá ser feita a qualquer tempo pelo próprio colaborador.

- O Procedimento Administração de Rede apresenta o processo que viabiliza esta política.

7. POLÍTICA DE CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

7.1 A definição do grau de sensibilidade para a informação deve possibilitar a determinação das salvaguardas mínimas para proteger tais informações.

7.2 O grau de sensibilidade da informação deve ser analisado quanto ao impacto na Confidencialidade, Integridade, Disponibilidade, Autenticidade e Legalidade (CIDAL) da informação.

7.3 A classificação da informação, ou seja, a definição do grau de sensibilidade de cada informação é de responsabilidade do gestor da Unidade Organizacional onde a informação teve origem.

7.4 A rotulagem da informação é de responsabilidade do dono do processo onde a informação tem origem.

7.5 As informações documentadas devem ser identificadas, armazenadas, transmitidas e descartadas de acordo com um processo formal.

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

7.6 Ativos tecnológicos deverão ter controles aplicados para a proteção da informação que armazena, processa e manuseia, com o tratamento apropriado à sensibilidade e criticidade operacional, conforme classificada.

7.7 Os outros ativos, que não sejam as informações, devem ser classificados em conformidade com o mais alto grau de sensibilidade da informação que ele trata.

7.8 A informação eletrônica, física ou verbal deve ser tratada conforme esta política.

7.9 Classificação da informação quanto ao sigilo:

Classificação	**PÚBLICA**	**INTERNA**	**CONFIDENCIAL**	**CONFIDENCIAL – CSP TECH**	**RESTRITO**
Impacto quanto à perda de Confidencialidade	Inexistente	Baixo	Médio	Médio	Alto
Definição	Pode ser divulgada a qualquer pessoa sem que haja implicações à **CSP Tech.** O conhecimento desta informação pelo público não expõe a CSP Tech a prejuízo financeiro, constrangimento, tampouco compromete a segurança dos ativos.	Pode ser divulgada para todos os colaboradores da **CSP Tech.** No entanto, o conhecimento desta informação, por pessoas não autorizadas, não afeta a estratégia e não causa grave prejuízo financeiro.	Para documentos que precisam ser compartilhados com pessoas de fora da empresa, mas que possui dados pessoais, como nome e e-mail. Não tem criptografia restritiva, ou seja, o destinatário externo consegue abrir normalmente.	Documentos com Informações confidenciais do dia a dia da empresa. Qualquer colaborador da CSP Tech consegue abrir, mas ninguém de fora.	Informações com o mais alto grau de proteção. Apenas pessoas com permissão específica conseguem acessar — nem todos os colaboradores têm acesso.

- O Procedimento Gestão da Informação Documentada apresenta o processo que viabiliza esta política.

8. POLÍTICA PARA SEGURANÇA FÍSICA E DO AMBIENTE

8.1 Perímetro de segurança física

8.1.1 Deve haver vigilância, portaria ou recepção e catracas com sistemas baseados em cartão de acesso ou biometria na entrada ao local do escritório (sítio).

8.1.2 O local do escritório (sítio) deve possuir câmeras de segurança aos seus arredores, monitoradas por Sistema de Monitoramento por Circuito Fechado de Televisão (CFTV).

8.1.3 A entrada principal ao escritório da **CSP Tech** deve possuir porta protegida com tranca segura.

- O Procedimento Administração de Facilities apresenta o processo que viabiliza as diretrizes do item 8.1.

8.2 Controles de entrada física

8.2.1 A **CSP Tech** deve possuir recepção para controlar o acesso físico.

8.2.2 A **CSP Tech** deve implementar o sistema de controle de entrada física no escritório com identidade autenticada por meio de sistemas baseados em cartão de acesso ou biometria.

8.2.3 Os visitantes que não são identificados/autenticados por meio de sistemas baseados em cartão de acesso ou biometria, deverão ser identificados e suas entradas e saídas registradas em planilha específica.

8.2.4 O acesso físico dos visitantes ao escritório deverá ser feito, imprescindivelmente, acompanhado por um colaborador da **CSP Tech**.

8.2.5 Os colaboradores devem possuir identificação visível ao transitar pelo escritório por meio do crachá ou do adesivo identificador.

8.2.6 Os direitos de acesso a áreas de acesso restrito devem ser revistos e atualizados periodicamente.

8.2.7 Uma trilha de auditoria eletrônica deve ser mantida e monitorada quanto aos acessos físicos às dependências físicas da **CSP Tech**.

- O Procedimento Gestão de Acesso apresenta o processo que viabiliza as diretrizes do item 8.2.

8.3 **Segurança em escritórios, salas e instalações**

8.3.1 As subdivisões e salas do escritório que possuem informações com algum grau de sensibilidade definido devem ser protegidas de forma a evitar o acesso às informações, por pessoas não autorizadas.

8.3.2 A **CSP Tech** adota a cultura 'portas abertas' e devido essa característica, as políticas de mesa limpa, tela limpa e controle de acesso lógico devem ser estritamente implementadas para minimizar o risco de acesso não autorizado às informações, pois o acesso físico é restringido apenas no perímetro, na entrada e em salas críticas.

8.3.3 As salas críticas (de acesso restrito) devem ser protegidas por sistemas baseados em cartão de acesso ou biometria.

8.3.4 Devem ser implementadas proteções para o acesso a áreas de carga e descarga de equipamentos e outros materiais, como por exemplo, o isolamento desta área das demais áreas do site, bem como supervisão e inspeção do material recebido ou expedido.

8.3.5 O escritório deve possuir câmeras de segurança, monitoradas por Sistema de Monitoramento por Circuito Fechado de Televisão (CFTV).

- O Procedimento Gestão de Acesso, bem como o Procedimento Administração de Facilities apresentam o processo que viabiliza as diretrizes do item 8.3.

8.4 **Proteção física contra ameaças externas e do meio ambiente**

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

8.4.1 Os sites devem conter, no mínimo, proteções físicas implementadas contra: fogo, inundação, sobrecarga elétrica, explosão e manifestações civis, conforme apropriado.

- O Procedimento Administração de Facilities, bem como o Procedimento Gestão de Continuidade de Negócio apresentam o processo que viabiliza as diretrizes do item 8.4.

8.5 **Proteção dos equipamentos e cabeamento**

8.5.1 Os equipamentos devem ser acondicionados em local apropriado de forma a minimizar danos causados por poeira, efeitos químicos, interferência ou radiação eletromagnética e vandalismo.

8.5.2 Os locais que possuem equipamentos devem ter a temperatura e umidade do ar monitoradas para evitar que ambas afetem negativamente os equipamentos.

8.5.3 A remoção, movimentação e a instalação de equipamentos (com exceção de dispositivos móveis) só podem ser feitas pela equipe de Infraestrutura.

8.5.4 A manutenção dos equipamentos deve ser realizada apoiada em bases de conhecimento e especificações do fabricante para garantir a integridade e disponibilidade dos mesmos. Os equipamentos que passarem por manutenção devem ser inspecionados para garantir que não estão em mau funcionamento antes de entrar em operação.

8.5.5 Os equipamentos da **CSP Tech** que operam fora do escritório, devem possuir medidas de segurança e privacidade implementadas para minimizar os riscos inerentes ao ambiente externo.

8.5.6 Os equipamentos devem ser inspecionados pela equipe de Infraestrutura antes da reutilização ou descarte para averiguar quanto à existência de informação sensível armazenada. Caso o equipamento inspecionado em questão contenha informação sensível, a mesma deve ser sobrescrita de forma segura antes da reutilização ou descarte.

8.5.7 Para os equipamentos que não estão sendo monitorados pela **CSP Tech**, devem ser implementadas medidas de segurança e privacidade como a conscientização e a responsabilização dos usuários destes equipamentos quanto à proteção da informação existente nos mesmos.

8.5.8 No Data Center, os equipamentos devem ser protegidos contra indisponibilidades causadas devido à falta ou interrupções no suprimento de serviços como energia elétrica, água, gás, esgoto, calefação/ventilação e ar-condicionado por meio de redundância.

8.5.9 O cabeamento de energia e o de telecomunicações devem ser protegidos contra interferência através da separação dos cabos de energia e de comunicações e da utilização de blindagem eletromagnética, conforme apropriado.

8.5.10 O cabeamento de energia e o de telecomunicações devem ser protegidos contra danos através da passagem correta do cabeamento em eletrocalhas.

8.5.11 Nos cabos e nos equipamentos devem ser utilizadas marcações identificáveis a fim de minimizar erros no manuseio.

8.5.12 As salas de cabos, painéis de conexões e pontos terminais devem ser protegidos contra acesso não autorizado.

- O Procedimento Gestão de Ativo, bem como o Plano de Disponibilidade e Capacidade dos Serviços de Tecnologia da Informação apresentam o processo que viabiliza as diretrizes do item 8.5.

9. POLÍTICA PARA USO ACEITÁVEL DOS ATIVOS

9.1 A **CSP Tech** disponibiliza equipamentos para seus colaboradores exclusivamente para o desempenho de suas atividades profissionais, portanto, o uso inadequado desses equipamentos e para fins que não sejam os delineados pela **CSP Tech**, é proibido.

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

9.2 O colaborador deve zelar pelo bom uso dos recursos de informática a ele disponibilizados pela **CSP Tech** não removendo, alterando ou acrescentando, qualquer tipo de componente interno de hardware ou software, sem autorização.

9.3 O uso das mídias removíveis deve ser bloqueado por padrão e liberado conforme necessidade. É imprescindível, o uso de criptografia ao armazenar em mídia removível autorizada, informação com mais alto grau de sensibilidade.

9.4 Todos os dispositivos de armazenamento de dados portáteis autorizados (DVD, CD, pendrive) devem ser submetidos a uma rotina de verificação quanto à existência de vírus, antes de serem utilizados no ambiente da **CSP Tech** (em 'dispositivo de propriedade da CSP Tech' ou BYOD, em 'rede local' ou em 'serviço em nuvem da CSP Tech').

9.5 É vedado o armazenamento, no ambiente da **CSP Tech**, de material obsceno, ilegal ou não ético, fato que ensejará a apuração de responsabilidade.

9.6 Arquivos particulares ou não pertinentes ao negócio da **CSP Tech** não devem ser copiados/movidos para o ambiente da **CSP Tech**.

9.7 Informações relacionadas aos concorrentes, propostas comerciais, protótipos e projetos da concorrência não devem ser armazenados no ambiente da **CSP Tech**.

9.8 É vedado ao colaborador, copiar total ou parcialmente, normas, livros, artigos, relatórios ou outros documentos, além do permitido pela lei de direitos autorais e as licenças aplicáveis.

9.9 É vedado ao colaborador, duplicar, converter para outro formato ou extrair de gravações comerciais externas (vídeo, áudio), além do permitido pela lei de direitos autorais e as licenças aplicáveis.

9.10 A **CSP Tech** deve assegurar que está em conformidade com os termos de uso dos softwares homologados.

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

9.11 Documentos necessários para as atividades da **CSP Tech** devem ser armazenados na rede. Tais documentos, se armazenados apenas localmente nos computadores, não possuem garantia de backup, podendo, o colaborador ser responsabilizado pela perda definitiva de documentos em decorrência deste ato.

9.12 O colaborador não deve executar comando ou programa que possa sobrecarregar os serviços tecnológicos da CSP Tech ou dos clientes sem a prévia solicitação e autorização da equipe de Infraestrutura e do cliente, quando for o caso.

9.13 O colaborador não deve consumir alimentos e bebidas próximo aos recursos tecnológicos e aos documentos físicos corporativos, podendo ser responsabilizado por danos causados em decorrência deste ato.

9.14 O colaborador deve manter a configuração do equipamento disponibilizado pela **CSP Tech**, o qual possui os controles de segurança e privacidade da informação definidos pela **CSP Tech**.

9.15 É vedada a conexão de quaisquer equipamentos que não sejam homologados pela **CSP Tech**, em sua rede corporativa, podendo essa conexão ser realizada em rede específica disponibilizada pela **CSP Tech**.

9.16 Na utilização de equipamentos de propriedade da **CSP Tech**, o colaborador deverá tomar os seguintes cuidados:

9.16.1 Encerrar sessões ativas quando não forem mais necessárias e desligar o equipamento ao final do expediente;

9.16.2 Sempre que tiver incidentes relacionados aos equipamentos, o colaborador deverá comunicar a equipe de Infraestrutura por meio de um processo formal;

9.16.3 O uso das impressoras do escritório deve ser feito, exclusivamente, para impressão de informações que sejam de interesse da **CSP Tech;**

9.16.4 O colaborador deve retirar imediatamente da impressora os documentos que tenha solicitado a impressão, caso contenham informações sensíveis.

9.17 A **CSP Tech** tem propriedade legal sobre todas as informações produzidas em seu ambiente, reservando-se o direito de manter, a seu critério, histórico de acessos e transações realizadas através das conexões Internet ou Intranet, quando considerado necessário, por motivos de segurança ou para fins de auditoria.

9.18 Os ativos da **CSP Tech** devem ser inventariados.

9.19 Os ativos de tecnologia da informação devem ter uma linha de base de configuração, incluindo configurações de segurança da informação.

- O Procedimento Administração de Rede, o Procedimento Gestão de Ativo, bem como o Procedimento Gestão de Incidente apresentam os processos que viabilizam esta política.

10. POLÍTICA PARA MESA E TELA LIMPAS

10.1 As mesas de trabalho devem estar limpas de papéis e mídias de armazenamento removíveis que contenham informações sensíveis.

10.2 Os papéis e mídias contendo informações sensíveis devem ser guardados em mobília segura, imediatamente após o uso.

10.3 As áreas de trabalho dos computadores devem estar limpas de arquivos que contenham informações sensíveis. Estes arquivos devem estar armazenados apropriadamente na rede.

10.4 Sempre que não for utilizar o computador ou tiver que se ausentar da sala, o colaborador deverá efetuar procedimento de desconexão - logoff ou o bloqueio do computador.

10.5 O sistema operacional deve fazer o bloqueio automático de tela a partir de 15 minutos de inatividade.

- O Procedimento Administração de Rede apresenta o processo que viabiliza a política de tela limpa.

11. POLÍTICA PARA TRANSFERÊNCIA DE INFORMAÇÕES

11.1 Os requisitos para confidencialidade da informação devem estar descritos em um Acordo de Responsabilidade com a Segurança da Informação e devem ser analisados criticamente quando houver mudança que afete estes requisitos.

11.2 O colaborador deve verificar o destinatário antes do compartilhamento das informações, a fim de evitar o compartilhamento com pessoas não autorizadas.

11.3 O transporte dentro ou fora das dependências da **CSP Tech** de documentos físicos (em papel) e de mídias removíveis que contenham conteúdo sensível deve ser realizado em envelope lacrado opaco e a **CSP Tech** deve assegurar a identificação dos entregadores e recebedores.

11.4 Os colaboradores devem ser extremamente cautelosos na utilização de quaisquer meios de comunicação, ficando proibida qualquer troca de informações com o meio exterior sobre informações com mais alto grau de sensibilidade, sem autorização, justificativa e criptografia.

11.5 É vedada a disseminação para o meio externo à CSP Tech, sem autorização, justificativa e criptografia, de informações que contenham referência a:

11.5.1 Documentação dos sistemas (código fonte, diagramas, playbooks, documentação de tabelas etc.);

11.5.2 Diagramas, checklists operacionais, projetos, papers técnicos ou da empresa;

11.5.3 Decisões sobre aquisições, fusões, incorporações;

11.5.4 Patentes, pesquisas, desenvolvimento de software e de soluções.

11.6 **E-mail**

11.6.1 O correio eletrônico corporativo fornecido pela **CSP Tech** deve ser utilizado em função das atividades da **CSP Tech**.

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

11.6.2 A tecnologia utilizada pela **CSP Tech** para correio eletrônico deve garantir a autenticidade do remetente, bem como bloquear anexos de conteúdo mal-intencionado.

11.6.3 É expressamente proibido:

11.6.3.1 O envio de material obsceno, ilegal, não ético, propagandas, mensagem do tipo "corrente", discriminatórias, preconceituosas ou ofensivas no que se refere à nacionalidade, raça, orientação sexual, religião ou opinião política;

11.6.3.2 O envio simultâneo de mensagens para todos os colaboradores e clientes da **CSP Tech**, salvo para comunicações previamente autorizadas por Gestão de Gente;

11.6.3.3 A inserção ou disseminação de arquivos que contenham vírus ou qualquer espécie de programas nocivos;

11.6.3.4 O envio de grande quantidade de mensagens de e-mail que prejudique a capacidade técnica;

11.6.3.5 Divulgar conteúdo que viole quaisquer direitos autorais, patentes, marcas registradas, marcas de serviço, nomes comerciais, segredos comerciais ou outros direitos de propriedade intelectual;

11.6.3.6 Participar de listas de discussão que possa abordar assuntos alheios às áreas fins da empresa e de suas gerências;

11.6.3.7 Utilizar e-mail corporativo para inscrição em sites alheios à **CSP Tech**, sem autorização.

11.6.3.8 Anunciar quaisquer produtos ou serviços, bem como promover qualquer marca, setor, empresa ou outras formas de autopromoção;

11.6.3.9 Forjar quaisquer das informações do cabeçalho do remetente.

11.6.4 As mensagens de correio eletrônico devem incluir assinatura padronizada com as seguintes informações:

11.6.4.1 Nome Completo

11.6.4.2 Área/Setor

11.6.4.3 Cargo

11.6.4.4 Telefone

11.6.4.5 Logo da empresa.

11.6.5 Os anexos das mensagens de correio eletrônico, com informações sensíveis, devem ser protegidos por meio de criptografia.

11.6.6 No caso de transferência de arquivos, em que o servidor de e-mail não a suporte, a mesma deverá ser feita via OneDrive da CSPTECH.

- O Procedimento Administração de Rede apresenta o processo que viabiliza esta política.

12. POLÍTICA PARA USO DE DISPOSITIVOS MÓVEIS E TRABALHO REMOTO

12.1 O colaborador, no caso de perda, furto ou roubo de um dispositivo móvel, deve notificar imediatamente para a equipe de Infraestrutura, e no caso de furto ou roubo, procurar a ajuda das autoridades policiais, registrando um boletim de ocorrência.

12.2 Diante da notificação de perda, furto ou roubo de um dispositivo móvel, a Infraestrutura deverá comunicar o Comitê de Segurança da Informação. A Infraestrutura deverá imediatamente desvincular o e-mail do dispositivo móvel roubado/furtado/perdido, se necessário inativar a conta do Microsoft 365 do usuário e nos sistemas da **CSP Tech** que o usuário tiver acesso. Em paralelo, deverá executar o rastreamento para tentar localizá-lo e auxiliar o colaborador na troca de todas as senhas, além de reforçar o monitoramento quanto a acesso indevido aos sistemas críticos da CSP Tech durante e pós incidente.

12.3 O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracteriza a assunção de todos os riscos da sua má utilização, sendo responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar à **CSP Tech** ou a terceiros em decorrência deste ato.

12.4 É vedada a conexão dos dispositivos móveis de propriedade da **CSP Tech** em redes wifi públicas.

12.5 No teletrabalho, o colaborador deverá configurar o serviço de rede sem fio de sua rede doméstica em conformidade com os requisitos e restrições da **CSP Tech**.

12.6 O colaborador deve checar e instalar as atualizações do celular corporativo constantemente.

12.7 O colaborador não deve fazer downloads de aplicativos de terceiros de fontes desconhecidas no celular corporativo, mas apenas de fontes confiáveis, como App Store e Google Play.

12.8 O colaborador que deseje utilizar dispositivos móveis particulares ou adquirir acessórios e conectá-los ao ambiente da **CSP Tech**, deverá submeter previamente tais equipamentos ao processo de homologação com a equipe de Infraestrutura e atender a política para uso corporativo de dispositivos pessoais.

12.9 O acesso remoto à rede ou à nuvem da **CSP Tech** somente é permitido via Virtual Private Network (VPN) mediante processo formal para concessão do acesso.

- O Procedimento Administração de Rede apresenta o processo que viabiliza esta política.

13. POLÍTICA PARA USO E INSTALAÇÃO DE SOFTWARE

13.1 É vedado o uso de software não licenciado no ambiente da **CSP Tech** e pela **CSP Tech** no ambiente da **CSP Tech**.

13.2 A aquisição de software não constante na relação dos homologados deverá ser solicitada por meio de processo formal.

13.3 Softwares do tipo “jogos eletrônicos” não podem ser instalados, armazenados ou usados nos computadores de propriedade da **CSP Tech**, resguardado os computadores destinados para finalidade de lazer, se houver.

13.4 Não é permitido o download de software, programas ou executáveis da Internet ou de quaisquer outros meios para os computadores de propriedade da **CSP Tech** sem o devido processo formal, evitando assim, qualquer contaminação por malware que pode comprometer os sistemas e informações da **CSP Tech** ou problemas com a legislação de direitos autorais.

13.5 Os softwares fornecidos por entidades externas, sem ônus para a **CSP Tech** e acompanhado da autorização do detentor legal dos direitos autorais, deverão ser submetidos a Infraestrutura para homologação.

13.6 A **CSP Tech** deve implementar controles que impeçam ou detectem o uso de software não homologado em seu ambiente.

- O Procedimento Administração de Sistema apresenta o processo que viabiliza esta política.

14. POLÍTICA DE BACKUP

14.1 A **CSP Tech** deve adotar soluções de Backup e Disaster Recovery para proteger os seus dados contra perda.

14.2 A estratégia de backup deve categorizar as informações de acordo com a natureza dos dados:

14.2.1 Arquivo;

14.2.2 E-mail;

14.2.3 Banco de Dados;

14.2.4 Aplicação;

14.2.5 Máquina Virtual.

14.3 O backup deve ser protegido por criptografia.

14.4 A **CSP Tech** deve garantir que os serviços em nuvem sejam protegidos por backup.

14.5 A **CSP Tech** deve garantir que testes periódicos de restauração são programados e realizados, com o intuito de atestar a integridade do backup, averiguar os processos de backup e estabelecer melhorias tanto em backups realizados pela **CSP Tech** quanto naqueles realizados pelos prestadores de serviços em nuvem.

14.6 Devem ser definidas e respeitadas as janelas para execução do backup a fim de não causar impacto no funcionamento normal do serviço.

14.7 Deve ser definida a retenção de backup para cada tipo de informação conforme requisitos de negócio, legais e regulamentares.

14.8 As necessidades especiais de backup devem ser solicitadas à Infraestrutura por meio de um processo formal.

14.9 O esquema de realização de backups deve ser documentado no procedimento de Backup e Restore e pode ser constituído por:

14.9.1 Backup Completo;

14.9.2 Backup Incremental;

14.9.3 Backup Diferencial;

14.9.4 Snapshot de Banco de Dados e de Máquina Virtual.

- O Procedimento Administração de Rede apresenta o processo que viabiliza esta política.

15. POLÍTICA PARA PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

15.1 A **CSP Tech** deve adotar soluções de proteção contra malware, com medidas de detecção e de prevenção.

15.2 Os computadores da **CSP Tech** devem ter software antivírus instalado, ativado e atualizado sistematicamente.

15.3 As soluções de proteção contra malware devem executar varreduras periódicas, análise de comportamento nos computadores, nas mídias removíveis de armazenamento, anexo de e-mails e análise de dados recebidos do meio externo.

15.4 As soluções de proteção também devem detectar sites suspeitos e maliciosos, bloqueando o acesso ao esse domínio.

15.5 Os colaboradores são responsáveis pela não interrupção das soluções de proteção contra malware em seus computadores.

15.6 Os colaboradores, ao identificarem ou suspeitarem de malware, devem solicitar análise ao departamento de Infraestrutura por meio de abertura de chamado.

15.7 O departamento de Infraestrutura tem a responsabilidade de seguir os processos e utilizar ferramentas para detecção, proteção, remoção e reparo de malware.

- O Procedimento Administração de Rede apresenta o processo que viabiliza esta política.

16. POLÍTICA PARA CONTROLES CRIPTOGRÁFICOS E GERENCIAMENTO DE CHAVES

16.1 O uso de criptografia na **CSP Tech** é mandatório para informações classificadas com mais alto grau de sensibilidade, conforme a política de classificação e tratamento da informação do item 7, tanto em seu armazenamento como em sua transmissão.

16.2 A **CSP Tech** deve utilizar somente algoritmos de criptografia padronizados e extensivamente revisados.

16.3 O gerenciamento das chaves criptográficas públicas e privadas da **CSP Tech** deve ser feito por uma Autoridade Certificadora (CA) confiável.

16.4 A **CSP Tech** deve implementar um processo seguro para gerar, armazenar, arquivar, recuperar, distribuir, retirar e destruir chaves criptográficas, bem como para lidar com chaves comprometidas.

- O Procedimento Administração de Rede apresenta o processo que viabiliza esta política.

17. POLÍTICA PARA DESENVOLVIMENTO DE SOFTWARE

17.1 Os princípios de segurança para o desenvolvimento de software na **CSP Tech** estão baseados no conceito de Security by Design.

17.2 Os requisitos mínimos de segurança e privacidade da informação para software desenvolvidos internamente ou externamente devem ser estabelecidos pela **CSP Tech**.

17.3 O desenvolvimento de software deve ser realizado mediante um processo formal e utilizando uma metodologia autorizada pela **CSP Tech**.

17.4 A **CSP Tech** deve garantir ambientes seguros e separados para desenvolvimento, teste e produção, e deve considerar a segurança e privacidade para cenários de reuso de código.

17.5 A **CSP Tech** deve garantir que o ambiente de desenvolvimento possua repositório e controle de versão seguros de software.

17.6 O desenvolvimento de software deve ser orientado a evitar, encontrar e corrigir vulnerabilidades.

17.7 A **CSP Tech** deve utilizar em seu ambiente de desenvolvimento, técnica de revisão por pares ou afins. As equipes de desenvolvedores devem ser continuamente capacitadas para o desenvolvimento seguro.

- O Procedimento Administração de Sistema, bem como Procedimento Gestão de Mudança e Procedimento de Desenvolvimento Seguro, apresentam o processo que viabiliza esta política.

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

18. POLÍTICA PARA AQUISIÇÃO DE SOFTWARE

18.1 Os requisitos de segurança e privacidade da informação para aquisição de software devem ser estabelecidos pela **CSP Tech**.

18.2 Para aquisição de software, a política para relacionamento com provedores externos do item 20 deve ser respeitada.

18.3 A aquisição de software feita pela **CSP Tech** deverá ser submetida à avaliação e autorização da Infraestrutura como condição imprescindível para a compra.

- O Procedimento Administração de Sistema apresenta o processo que viabiliza esta política.

19. POLÍTICA PARA SEGURANÇA EM REDE CORPORATIVA E AMBIENTE EM NUVEM

19.1 A navegação em sites de categoria restringida pela **CSP Tech** conforme abaixo, é expressamente proibida tanto a partir da rede corporativa quanto a partir de equipamentos de propriedade da **CSP Tech**:

19.1.1 Propaganda político partidária;

19.1.2 Conteúdo ofensivo, difamatório, ilegal, discriminatório e similares;

19.1.3 Transferência de arquivos de programa ou executáveis a partir da internet;

19.1.4 Pornográfico e de caráter sexual;

19.1.5 Crackers;

19.1.6 Ferramentas de proxy;

19.1.7 Violência e agressividade;

19.1.8 Violação de direito autoral;

19.1.9 Terrorismo e disseminação de violência a partir de crença ou posição política;

19.1.10 Práticas de comercialização, divulgação ou posicionamento sobre drogas;

19.1.11 Pedofilia;

19.1.12 Sites que possuem função de upload;

19.1.13 Sites maliciosos conhecidos ou suspeitos;

19.1.14 Servidores de comando e controle.

19.2 Periodicamente, varreduras automatizadas de portas dos sistemas devem ser realizadas para verificar se portas não autorizadas estão abertas.

19.3 Os ativos de tecnologia da informação devem ser identificados através de uma ferramenta de descoberta ativa.

- O Procedimento Administração de Rede apresenta o processo que viabiliza esta política.

20. POLÍTICA PARA RELACIONAMENTO COM PROVEDORES EXTERNOS

20.1 Os requisitos de segurança e privacidade da informação devem ser acordados com o provedor externo em Acordo de Responsabilidade com a Segurança da Informação. Para os contratos de adesão, a **CSP Tech** deve avaliar as cláusulas e certificar-se que seus requisitos de segurança e privacidade da informação estão contemplados.

20.2 O Acordo de Responsabilidade com a Segurança da Informação firmado com o provedor externo deve contemplar as diretrizes desta PSI que sejam aplicáveis ao prestador de serviço, a fim de mitigar os riscos associados com o acesso destes terceiros aos ativos da **CSP Tech.**

20.3 Para os serviços terceirizados de tecnologia da informação, este Acordo de Responsabilidade com a Segurança da Informação deve ser estendido por toda a cadeia de suprimento do provedor externo.

- O Procedimento Gestão de Provedor Externo apresenta o processo que viabiliza esta política.

21. POLÍTICA PARA PROTEÇÃO DE INFORMAÇÃO PESSOAL

21.1 A **CSP Tech** deve garantir que exista uma Política de Privacidade em seus portais institucionais e que o propósito do tratamento dos dados pessoais seja lícito.

21.2 A **CSP Tech** deve assegurar que os processos e os sistemas estejam habilitados para viabilizar um tratamento de dados pessoais limitado ao que é necessário ao propósito através do princípio de Privacy by Design.

21.3 A **CSP Tech**, enquanto controladora de dados pessoais, deve acordar com seu operador de dados pessoais, sobre consentimento, finalidade, notificação de divulgação do dado pessoal, compartilhamento do dado pessoal com subcontratados, violação de dados pessoais, devolução, transferência e sobre o descarte de dado pessoal.

21.4 A **CSP Tech**, enquanto operadora de dados pessoais, deve exigir de seus controladores, que forneçam as condições necessárias para seu cumprimento de obrigações de operador perante a Lei Geral de Proteção de Dados (LGPD).

- O Procedimento Gestão de Privacidade apresenta o processo que viabiliza esta política.

22. POLÍTICA PARA CONTINUIDADE DO NEGÓCIO E DA SEGURANÇA DA INFORMAÇÃO

22.1 A **CSP Tech** deve assegurar que existam planos de contingência/redundância, planos de resposta e planos de recuperação para situações de desastre.

- O Plano Gestão de Continuidade de Negócio apresenta o processo que viabiliza esta política.

23. POLÍTICA PARA A CONFORMIDADE COM REQUISITOS NORMATIVOS, LEGISLATIVOS, REGULAMENTARES E CONTRATUAIS

23.1 Os requisitos normativos, legislativos, regulamentares e contratuais aplicáveis à **CSP Tech** devem ser identificados e continuamente monitorados quanto às mudanças quanto à conformidade.

24. POLÍTICA PARA USO DE SERVIÇOS EM NUVEM (PaaS, IaaS ou SaaS)

24.1 A **CSP Tech** deve estabelecer critérios de segurança e privacidade da informação para a seleção de provedor de serviços em nuvem.

24.2 Para aquisição de provedor de serviço em nuvem, a política para relacionamento com provedores externos do item 20 deve ser respeitada.

24.3 A **CSP Tech** deve realizar avaliação de risco de segurança e privacidade da informação para identificar e tratar os riscos associados ao uso do serviço em nuvem, bem como compreender a responsabilidade compartilhada e o esforço colaborativo pela segurança e privacidade da informação junto ao provedor de serviços em nuvem.

24.4 A **CSP Tech** deve se informar sobre como obter garantia da eficácia dos controles de segurança e privacidade da informação implementados pelo provedor de serviços em nuvem.

24.5 A **CSP Tech** deve se informar sobre como alterar ou parar o uso dos serviços em nuvem.

24.6 A **CSP Tech** deve avaliar o método utilizado pelo provedor de serviços em nuvem para fornecer, retornar e excluir as informações da **CSP Tech.**

24.7 A **CSP Tech** deve requerer do provedor de serviços em nuvem, suporte em caso de incidentes de segurança e privacidade da informação no ambiente dos serviços em nuvem.

24.8 A **CSP Tech** deve verificar se e como o backup será assegurado pelo provedor de serviços em nuvem, bem como deve verificar se e como a proteção contra malwares será assegurada pelo provedor de serviços em nuvem.

24.9 A **CSP Tech** deve verificar se e como o gerenciamento de logs, a gestão de vulnerabilidades técnicas e a gestão de acessos serão assegurados pelo provedor de serviços em nuvem.

24.10 Nos casos em que os serviços em nuvem são contratados pelos fornecedores da **CSP Tech**, a **CSP Tech** deve requerer destes fornecedores que os requisitos de segurança e privacidade da informação sejam atendidos também pelo provedor de serviços em nuvem.

25. POLÍTICA PARA GESTÃO DE EVENTOS (LOGS)

25.1 Os registros dos eventos (logs) das atividades dos usuários dos sistemas, eventos de falhas e de comportamentos atípicos ou anormais dos sistemas devem ser produzidos, mantidos e analisados periodicamente.

25.2 Os registros dos eventos (logs) devem ser agregados a um sistema central de gerenciamento de logs para análise e revisão.

25.3 Os ativos de tecnologia da informação devem ser sincronizados a partir de fontes de tempo confiáveis para que os registros dos eventos (logs) contenham informação de data/hora consistente.

25.4 Os registros dos eventos (logs) devem ser protegidos contra acesso não autorizado e adulteração.

- O Procedimento Gestão de Evento apresenta o processo que viabiliza esta política.

26. POLÍTICA PARA GESTÃO DE INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

26.1 A **CSP Tech** deve estabelecer critérios para classificar eventos de segurança da informação em incidentes de segurança da informação.

26.2 A **CSP Tech** deve estabelecer um processo de gestão de incidentes de segurança da informação que forneça capacidade de documentação, detecção, triagem, priorização, comunicação com as partes interessadas, resposta aos incidentes de segurança da informação e identificação de lições aprendidas.

26.3 O plano de resposta ao incidente deve incluir a contenção, erradicação e recuperação, coleta de evidências, escalonamento, se necessário, registro das atividades de resposta, análise forense, se necessário e a análise pós-incidente da causa-raiz.

- O Procedimento Gestão de Incidente de Segurança da Informação apresenta o processo que viabiliza esta política.

27. POLÍTICA PARA GESTÃO DE RISCOS

27.1 A **CSP Tech** deve conduzir um processo contínuo de avaliação e tratamento de riscos de segurança e privacidade da informação.

27.2 Os riscos de segurança e privacidade da informação devem ser identificados, analisados quanto à probabilidade e ao impacto, classificados quanto à significância do risco e avaliados quanto à tolerância ao risco.

- O Procedimento Gestão de Risco apresenta o processo que viabiliza esta política.

28. POLÍTICA PARA USO DE MÍDIAS SOCIAIS CORPORATIVAS

28.1 A **CSP Tech** deve conscientizar continuamente os colaboradores quanto à menção à **CSP Tech** em suas mídias sociais pessoais e quanto à interação com as mídias sociais corporativas.

28.2 O colaborador deve relatar imediatamente ao Marketing quando tiver conhecimento sobre postagem que possa trazer repercussão negativa à **CSP Tech**.

28.3 O processo para gestão das mídias sociais corporativas deve estabelecer um plano de resposta para situações de crise decorrente de incidentes de segurança ou privacidade da informação nas mídias sociais corporativas.

28.4 A **CSP Tech** deve analisar os recursos de segurança e privacidade da informação dos aplicativos gerenciadores de seus perfis sociais e controlar o uso destes aplicativos.

28.5 A **CSP Tech** deve adotar o recurso de conta verificada nas mídias sociais corporativas.

28.6 O social media da **CSP Tech** deve configurar as mídias sociais corporativas com os recursos de segurança e privacidade disponíveis na plataforma da mídia social corporativa.

28.7 O social media da **CSP Tech** deve seguir as seguintes diretrizes:

28.7.1 Habilitar a notificação de login e a verificação em duas etapas;

28.7.2 Não armazenar as senhas das mídias sociais corporativas no navegador;

28.7.3 Não acessar as mídias sociais corporativas em computadores públicos;

28.7.4 Acessar o site da mídia social corporativa usando conexão segura (https);

28.7.5 Não utilizar a mesma senha das mídias sociais corporativas em outros sites;

28.7.6 Proteger direitos autorais e de propriedade antes de postar, compartilhar ou distribuir materiais nas mídias sociais corporativas;

28.7.7 Não postar opiniões pessoais ou textos nas mídias sociais corporativas de forma que aparentam ou sugiram ser a opinião da **CSP Tech**;

28.7.8 Ter controle sobre quais aplicativos tem acesso às mídias sociais corporativas;

28.7.9 Efetuar logout da mídia social corporativa no computador, quando não estiver utilizando;

28.7.10 Se o perfil não for ser utilizado temporariamente ou definitivamente, desativá-lo;

28.7.11 Não clicar em links suspeitos (links reduzidos) ou em arquivos que foram enviados pelas mídias sociais corporativas;

28.7.12 Não compartilhar dados sensíveis nos chats das mídias sociais corporativas.

29. POLÍTICA PARA USO CORPORATIVO DE DISPOSITIVOS PESSOAIS

29.1 O colaborador pode utilizar seus dispositivos pessoais (smartphone, tablet, computador) para execução das atividades corporativas da **CSP Tech**, desde que em conformidade com o disposto nessa política, também conhecida como Política de Bring Your Own Device (BYOD).

29.2 Todos os colaboradores que optarem por utilizar seus dispositivos pessoais deverão cumprir integralmente as disposições previstas na Política BYOD, bem como as demais políticas de Segurança da Informação da CSP Tech.

29.3 Em caso de conflito entre esta Política e a Política BYOD, prevalecerão as regras específicas previstas na Política BYOD.

30. Tratamento das Exceções

30.1 As exceções a Política de Segurança da Informação devem ser explicitadas, autorizadas e formalizadas em procedimentos ou em Acordo de Responsabilidade com a Segurança da Informação.

31. Processo Disciplinar

31.1 O colaborador tem por obrigação cumprir a Política de Segurança da Informação. Desta forma, o não cumprimento será considerado uma infração.

31.2 Por meio do Comitê de Segurança da Informação, a **CSP Tech** exercerá seu poder para determinar sanções aos infratores. A infração será classificada em 3 níveis:

31.2.1 Incidente leve: quando há perda de um dos critérios CIDAL de informação classificada como corporativa;

31.2.2 Incidente médio: quando há perda de um dos critérios CIDAL de informação classificada como confidencial;

31.2.3 Incidente grave: quando há perda de um dos critérios CIDAL de informação classificada com mais alto grau de sensibilidade. Ou quando denigra a imagem da **CSP Tech**. São considerados ainda incidentes graves, as tentativas deliberadas de acesso não autorizado a dados com mais alto grau de sensibilidade, bem como atividades ilícitas vinculadas a ações de "corrupção", "fraude", "conluio", "má-fé contratual", "terrorismo", "pedofilia" e "comercialização de drogas".

31.3 Diante da constatação de um incidente já devidamente classificado, as seguintes sanções serão aplicadas aos colaboradores sob regime de trabalho CLT:

31.3.1 Advertência Verbal: Aplicada diante da constatação de incidente leve.

31.3.2 Advertência Escrita: Aplicada diante da constatação de incidente médio ou grave.

31.3.3 Demissão: Aplicada diante da constatação de incidente grave. Aos colaboradores enquadrados no regime de trabalho CLT, a pena de demissão por justa causa será aplicada nas hipóteses previstas no artigo 482 e parágrafo único da Consolidação das Leis do Trabalho - DECRETO-LEI N.º 5.452, de 1º de maio de 1943.

31.4 Diante da constatação de um incidente já devidamente classificado, no caso de colaboradores terceirizados, será solicitado à empresa prestadora da respectiva mão de obra, o afastamento temporário ou definitivo do colaborador terceirizado, conforme a falta cometida podendo em último caso, a **CSP Tech** solicitar a rescisão do contrato de prestação de serviço.

31.5 A aplicação destas sanções não isenta o colaborador de sofrer outras penalidades previstas em contratos, ou mesmo de sofrer processos penais por crimes de condescendência criminosa, de violação de sigilo funcional entre outros, estabelecidos no código penal.

31.6 Diante da omissão ou inércia daquele que tiver ciência ou que desconfie da ocorrência de incidente relacionado à segurança ou privacidade da informação, este poderá ser responsabilizado na medida de sua omissão.

Versão	Data da Revisão	Histórico	Editado por
1.0	02/04/2023	Elaboração do Documento	Infraestrutura
2.0	05/08/2025	Inclusão do Termo de Ciência	Governança e Jurídico
3.0	29/08/2025	Nova PSI	Governança e Infraestrutura
4.0	19/01/2026	Alteração dos procedimentos vinculados à política	Governança e Infraestrutura

TERMO DE CIÊNCIA E ACEITE DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Declaro ter ciência e pleno conhecimento da Política de Segurança da Informação (PSI) da CSP Tech.

Declaro que compreendo e aceito integralmente os termos e condições estabelecidos na PSI, incluindo, mas não se limitando a confidencialidade, integridade, disponibilidade, controle de acesso, etc.

Estou ciente de minhas responsabilidades e obrigações em relação à segurança da informação, incluindo a proteção dos dados e sistemas da organização, e

csptech.com.br
+55 21 2263 7660
+55 11 97376 1007

concordo em cumprir todas as diretrizes, normas e procedimentos definidos na PSI.

Estou ciente de que o não cumprimento da PSI será considerado ato de indisciplina para os fins do artigo 482, alínea ‘h” da CLT, passível, portanto, de demissão por justa causa, além de sanções civis e penais, conforme previsto em lei e nas normas internas da organização.

Estou ciente de que minhas atividades no ambiente computacional corporativo podem ser monitoradas e auditadas, e que não devo criar expectativa de privacidade em relação a essas atividades.

Por fim, comprometo-me a reportar imediatamente qualquer incidente ou suspeita de violação da PSI através do canal oficial de denúncias da CSP Tech: https://csptech.clickcompliance.com/reporting-channel .

Rio de Janeiro/RJ, (dia de mês de ano).

Nome:
_____

Assinatura:
_____