1 OBJETIVO

Esta política tem por objetivo estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da CST MEDICINA DO TRABALHO adotar padrões de comportamento seguro, adequados às metas e necessidades da CST.

Além disso, fornece diretrizes e práticas que permitam atingir de forma segura, a estratégia e requisitos de negócio, regulamentações, legislações, contratos, riscos e ameaças atuais e futuras projetadas para a segurança da informação.

2 DEFINIÇÕES

a) **Confidencialidade**: A informação deve estar disponível e somente ser divulgada a indivíduos, entidades ou processos autorizados;

b) **Integridade**: Salvaguarda da exatidão da informação e dos métodos de processamento;

c) **Disponibilidade:** As pessoas autorizadas devem obter acesso à informação e aos ativos correspondentes sempre que necessário;

d) **Autenticidade:** É a propriedade que algo ou alguém é o que alega ser;

e) **Conformidade:** Processo de garantia do cumprimento de um requisito, podendo ser obrigações empresariais com as partes interessadas (investidores, empregados, credores, etc.) e com aspectos legais e regulatórios relacionados à administração das empresas, dentro de princípios éticos e de conduta estabelecidos pela Alta Administração da CST MEDICINA DO TRABALHO;

f) **Informação:** É a reunião ou conjunto de dados e conhecimentos resultante do processamento, manipulação e/ou organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (humano ou máquina) que a recebe;

g) Ativo de informação: Um ativo de informação é um recurso corporativo que possui valor para a companhia e deve ser protegido através de práticas e políticas que garantam sua segurança. Esses ativos podem ser elementos informacionais que representam valor para a empresa, como banco de dados, arquivos, documentos, contratos, entre outros. Eles podem se apresentar tanto na forma física (Equipamentos e estrutura física) quanto digital. As pessoas contratadas e as informações produzidas por elas no ambiente de trabalho, em qualquer que seja o regime de contratação e natureza jurídica, também é ativo de informação da CST;

h) Controle: Medida de segurança adotada pela CST para o tratamento de um risco específico;

i) Controle de acesso: Assegurar que o acesso físico e lógico aos ativos (2.g) seja autorizado e restrito com base em requisitos de negócio e de segurança da informação;

j) Segurança da informação: É o conjunto de ações e controles que tem como objetivo garantir a preservação dos aspectos de confidencialidade, integridade, disponibilidade, autenticidade e conformidade das informações, contribuindo para o cumprimento dos objetivos estratégicos da companhia;

k) Usuários da informação: Empregados com vínculo empregatício de qualquer área da CST ou terceiros alocados na prestação de serviços A CST, indiferente do regime jurídico a que estejam submetidos, assim como outros indivíduos ou organizações devidamente autorizadas a utilizar manipular qualquer ativo de informação da CST MEDICINA DO TRABALHO para o desempenho de suas atividades profissionais;

l) Gerência de Segurança da Informação: Profissional ou área designada pela Alta Direção da CST para propor, implementar, monitorar e aprimorar continuamente todos os processos e aspectos de segurança da informação da organização, em conformidade com as normas e boas práticas reconhecidas no mercado;

m) Gestor da Informação: Usuário da informação que ocupe cargo especifico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação;

n) Comitê Gestor de Segurança da Informação – CGSI: Grupo de trabalho multidisciplinar permanente, efetivado pela diretoria da CST, que tem por finalidade tratar questões ligadas à Segurança da Informação;

o) Risco de segurança da informação: Riscos associados à violação da confidencialidade e integridade, bem como da disponibilidade das informações da companhia nos meios físicos e digitais;

p) Incidente de Segurança da informação: Evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades e que afete algum dos aspectos da segurança da informação: confidencialidade, integridade ou disponibilidade;

a) Vulnerabilidade: Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da CST MEDICINA DO TRABALHO;

q) Ameaça: Causa potencial de um incidente, que pode vir a prejudicar A CST MEDICINA DO TRABALHO;

r) LGPD: Lei Geral de Proteção de Dados Pessoais;

s) PGSIP: Política Geral de Segurança da Informação e Privacidade;

t) *Phishing*: É uma técnica de crime cibernético que usa fraude e engano para manipular as vítimas para que cliquem em links maliciosos ou divulguem informações pessoais confidenciais;

u) *Exploit:* É um software ou código malicioso que explora uma falha ou vulnerabilidade relacionada ao software ou hardware de um computador, um *exploit* também pode afetar outros eletrônicos como roteadores, celulares e outros;

v) *Malware*: Software malicioso, e qualquer código ou programa escrito para prejudicar um sistema de dispositivo final;

w) ***Vírus:*** Software ou código malicioso criado para alterar a forma como um computador funciona e desenvolvido para se propagar de um computador para outro;

x) **Vulnerabilidade:** Causa potencial de um incidente de segurança da informação, que pode vir a prejudicar as operações ou ameaçar as informações da CST MEDICINA DO TRABALHO;

y) **Dispositivo Final*:*** Computadores, notebooks, celulares, tablets, impressoras ou qualquer dispositivo utilizado por usuários finais.

z) **Dados sensíveis:** Dados sensíveis são informações pessoais que revelam aspectos íntimos da vida de um indivíduo, incluindo, mas não limitado a dados sobre origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, informações genéticas, dados biométricos, saúde ou vida sexual

aa) **Áreas Sensíveis:** São locais que necessitam de proteção especial devido à sua relevância estratégica ou ao valor dos ativos que abrigam. Tais áreas são destinadas ao processamento e armazenamento de informações críticas. Exemplos incluem Salas de Servidores e locais de armazenamento de arquivos sensíveis.

3 ESCOPO

Esta política se aplica a todos os **Usuários da Informação** (2.k) da CST MEDICINA DO TRABALHO, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a CST, tais como empregados, ex-empregados, prestadores de serviço, ex-prestadores de serviço, colaboradores, ex-colaboradores, que possuíram, possuem ou virão a possuir acesso às informações da CST e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura da empresa.

4 DIRETRIZES

4.1 Patrimônio da Informação

a) Toda informação elaborada, adquirida, manuseada, armazenada, transportada e/ou descartada nas dependências e/ou em ativos da CST é considerada patrimônio da empresa e deve ser utilizada exclusivamente para os interesses corporativos.

4.1.1 Acesso e Uso da Informação

a) O acesso lógico, o controle de acesso físico e o uso da informação da CST devem ser aprovados, controlados, registrados, armazenados e monitorados, de forma a permitir a adequada execução das tarefas inerentes ao seu cargo ou função.
b) Resguardar as informações da CST MEDICINA DO TRABALHO, garantindo requisitos adequados de confidencialidade, integridade e disponibilidade.

4.1.2 Incidentes de Segurança

a) Os incidentes de segurança devem ser identificados, monitorados, comunicados e devidamente tratados de forma a reduzir riscos no ambiente, evitando interrupção das atividades e não afetar o alcance dos objetivos estratégicos da CST MEDICINA DO TRABALHO.
b) Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus empregados, clientes e parceiros.

4.1.3 Monitoramento e Auditoria

a) A CST pode monitorar o acesso e a utilização de seus ativos tecnológicos, como dos ambientes, equipamentos, sistemas da informação, aplicativos de e-mail, aplicativos de mensagens instantâneas, de forma que ações indesejáveis ou não autorizadas sejam detectadas.

b) A CST pode auditar periodicamente as práticas de Segurança da Informação, de forma a avaliar a conformidade das ações de seus colaboradores, estagiários, terceiros, fornecedores e parceiros em relação ao estabelecido nesta Política e na legislação aplicável.

4.1.4 Política Geral de Segurança da Informação

a) O objetivo da gestão de Segurança da Informação da CST é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos à instituição.

b) A Presidência, Diretoria Executiva e o Comitê Gestor de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na CST. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da CST MEDICINA DO TRABALHO.

c) Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação e proteção de dados pessoais.

d) Fornecer orientação quanto a requisitos de conformidade com a Lei Geral de Proteção de Dados Pessoais N° 13.709/2018.

e) Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da CST como resultado de falhas de segurança.

5 POLÍTICA DE MESA LIMPA

Também visando à implementação de medidas simples de segurança da informação, instaura-se, de imediato, a Política da Mesa Limpa, por meio da qual nenhum tipo de dado ou informação pode ser deixado à vista, independente da forma, observando-se, ainda, o seguinte:

a) É obrigação de todos providenciar o bloqueio do computador sempre que se retirar da sua mesa (inclusive em home office), ainda que por curto período. Ao se ausentarem para retorno ao trabalho em outro dia, deverão desligar seu computador e também a tela utilizada se for apartada.

b) É obrigação de todos providenciar para que papéis, lembretes, documentos e outros sejam guardados sempre que o responsável por estes se retirar de sua estação de trabalho.

Visando à confidencialidade das informações da empresa, de seus colaboradores e de seus clientes, não é permitido utilizar como rascunhos papéis que contenham ou possa conter informações sigilosas ou protegidas por lei, tais como: fichas de clientes, contratos, cópias de documentos pessoais, extratos, documentos que contenham algum dado de saúde, dados sobre menores, documentos que contenham dados sensíveis de quaisquer pessoas físicas, informações pessoais de qualquer indivíduo etc.

Na hipótese acima, os papéis deverão ser previamente rasgados em partes mínimas (preferencialmente em fragmentadora) e posteriormente descartados de forma a impossibilitar seu uso ou a extração de quaisquer dados e informações.

6 É RESPONSABILIDADE DA CST MEDICINA DO TRABALHO

6.1 Elaboração e Implementação de Políticas

a) Elaborar, implantar e seguir por completo políticas, normas e procedimentos de segurança da informação, garantindo que os requisitos básicos de confidencialidade, integridade e disponibilidade da informação da CST sejam atingidos através da adoção de controles contra ameaças provenientes de fontes tanto externas quanto internas.

6.1.1 Disponibilização de Políticas

a) Disponibilizar políticas, normas e procedimentos de segurança a todas as partes interessadas e autorizadas, tais como: empregados, terceiros contratados e, onde pertinente, clientes.

6.1.2 Educação e Conscientização

a) Garantir a educação e conscientização sobre as práticas adotadas pela CST de segurança da informação para empregados, terceiros contratados e, onde pertinente, clientes.

6.1.3 Conformidade com Regulamentações

a) Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais.

6.1.4 Tratamento de Incidentes

a) Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades apropriadas.

6.1.5 Continuidade do Negócio

a) Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres.

6.1.6 Melhoria Contínua

a) Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

7 ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

7.1 Comitê Gestor de Segurança da Informação

Fica constituído o COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO – CGSI, contando com a participação de, pelo menos, um representante da Diretoria e um membro Lider das seguintes áreas: Tecnologia da Informação, Segurança da Informação, Recursos Humanos e Jurídico.

7.1.1 É reponsabilidade do Comitê Gestor de segurança da informação

a) Analisar, revisar e propor a aprovação de políticas e normas relacionadas à segurança da informação;

b) Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

c) Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Política geral da Segurança da Informação e Privacidade;

d) Promover a divulgação da PGSIP e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da CST.

7.2 Gerência de Segurança da informação

7.2.1 É responsabilidade da Gerência de Segurança da Informação:

a) Conduzir a Gestão e Operação da segurança da informação, tendo como base esta política e demais resoluções do CGSI;

b) Apoiar o CGSI em suas deliberações;

c) Elaborar e propor ao CGSI as normas e procedimentos de segurança da informação, necessários para se fazer cumprir a PGSIP;

d) Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

e) Tomar as ações cabíveis para se fazer cumprir os termos desta política;

f) Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

7.3 GESTORES DA INFORMAÇÃO

7.3.1 Designação dos Gestores da Informação

a) Profissionais que ocupem cargos ou funções de liderança e que sejam designados como responsáveis por um setor ou área de negócio, ou por uma parte específica de uma área, como, por exemplo: Setor Comercial, Recursos Humanos, Departamento Pessoal, Tecnologia da Informação, Faturamento, Financeiro, entre outros.

7.3.2 É responsabilidade dos colaboradores designados como Gestores da Informação

a) Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte conforme as normas estabelecidas pela CST;

b) Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela CST;

c) Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;

d) Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;

e) Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela CST.

7.4 USUÁRIOS DA INFORMAÇÃO

7.4.1 É responsabilidade dos Usuários da Informação

a) Os usuários da informação devem ler, compreender e cumprir integralmente os termos da Política Geral de Segurança da Informação e Privacidade, bem como as demais normas e procedimentos de segurança aplicáveis;

b) Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Política Geral de Segurança da Informação, suas normas e procedimentos a Gerência de Segurança da Informação ou, quando pertinente, ao Comitê Gestor de Segurança da Informação;

c) Comunicar à Gerência de Segurança da Informação qualquer evento que viole esta Política ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da CST;

d) Assinar o Termo de Uso de Sistemas de Informação da CST, formalizando a ciência e o aceite integral das disposições da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;

e) Responder pela inobservância da Política Geral de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

8 PROGRAMA DE CONSCIENTIZAÇÃO, EDUCAÇÃO E TREINAMENTO EM SEGURANÇA DA INFORMAÇÃO

A CST MEDICINA DO TRABALHO está comprometida em promover uma cultura de segurança sólida em toda a organização. Para alcançar esse objetivo, propomos a criação e manutenção de um Programa de Conscientização, Educação e

treinamento em Segurança da Informação. Este programa visa educar e informar todos os colaboradores, estagiários, fornecedores, parceiros e partes interessadas sobre a importância da proteção de dados e a adoção de práticas seguras.

8.1 Aqui estão os principais pontos a serem considerados nas campanhas da CST

a) Definição de um tema. Cada campanha de conscientização abordará um tema específico por vez. Sugestões de temas incluem: *Phishing, Malwares, Exploits, Vírus* vulnerabilidades em depósitos finais, Identificação de ameaças, perigos associados e como evitar a propagação;

b) Importância das senhas, proteção, tamanho e complexidade;

c) LGPD, conformidade com a Lei Geral de Proteção de Dados, riscos, multas e processos;

d) Segurança Lógica, proteção de softwares, atualizações e validação da necessidade de uso;

e) Escopo: O programa abrange conscientização, educação e treinamento relacionados às políticas, normas e procedimentos de segurança da informação. Inclui proteção de ativos de informação, dados pessoais, prevenção de ameaças internas e externas, segurança de dispositivos móveis e privacidade ou qualquer outro tema relacionado.

8.2 Objetivos do programa treinamento e educação

- Reduzir riscos de incidentes de segurança por meio de práticas seguras;
- Garantir conformidade com regulamentações;
- Proteger ativos digitais e informações críticas;
- Evitar divulgação não autorizada de dados confidenciais;

- Mudar o comportamento dos usuários em relação à segurança da informação;
- Desenvolver estratégias de conscientização, educação e treinamento;
- Divulgar políticas, regras e procedimentos;
- Realizar exercícios de simulação e promover boas práticas;
- O programa será realizado periodicamente, sem prazo mínimo ou máximo definido;
- Lembramos a todos que a segurança da informação é responsabilidade de cada um. Vamos trabalhar juntos para fortalecer nossa cultura de segurança na CST MEDICINA DO TRABALHO.

9 SANÇÕES E PUNIÇÕES

As violações, mesmo que por mera omissão ou tentativa não consumada, desta política, bem como demais normas e procedimentos de segurança, serão passíveis de penalidades que incluem advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

A aplicação de sanções e punições será realizada conforme a análise do Comitê Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o CGSI, no uso do poder disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave.
No caso de terceiros contratados ou prestadores de serviço, o CGSI deve analisar a ocorrência e deliberar sobre a efetivação das sanções e punições conforme termos previstos em contrato.

Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a CST MEDICINA DO TRABALHO, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

Para toda e qualquer infração à PGSIP e às Normas e termos de uso, deverá ser aberto um incidente de segurança da informação, tratado de acordo com a Norma de Gestão de incidentes de Segurança da informação e apurado de acordo com os procedimentos internos, que deverão ser conduzidos pelo Gestor da área juntamente com o departamento de recursos humanos.

10 CASOS OMISSOS

Os casos omissos serão avaliados pelo Comitê Gestor de Segurança da Informação para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da CST adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da CST.

11 REVISÃO DA POLÍTICA

Esta política é revisada com periodicidade anual ou conforme o entendimento do Comitê Gestor de Segurança da Informação.

12 GESTÃO DA POLÍTICA

A Política Geral de Segurança da Informação é aprovada pelo Comitê Gestor de Segurança da Informação, em conjunto com a Diretoria da CST MEDICINA DO TRABALHO.