# Política de Segurança da Informação e Segurança Cibernética

**Fevereiro/2023**

**Responsável: Compliance e Riscos**

**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA**

**INTRODUÇÃO**

As medidas de segurança da informação têm por finalidade minimizar as ameaças aos negócios da StepStone. A presente Política ("Política de Segurança da Informação e Segurança Cibernética") objetiva preservar, melhorar e responder pelo sigilo, integridade e disponibilidade das informações da StepStone, a fim de proteger tais informações de uma variedade de ameaças, tais como erro, fraude, violação de privacidade e interrupção de serviços.

A StepStone adota programas específicos para resguardar a segurança dos arquivos internos, tais como o KnowBe4 – desenvolvido por empresa de mesmo nome, que permite treinar os profissionais para prevenção de e-mails de *phising*, o Cisco Firesight e o Sophos, dedicados a prevenção de ataques on-line e proteção dos arquivos internos, e o Zabbix, que permite monitoramento das redes internas e servidores da StepStone.

A Política de Segurança da Informação e Segurança Cibernética concentra informações relevantes e define ações e proibições com as quais todos os Colaboradores que desenvolvem, mantêm, armazenam, acessam, processam ou transmitem informações devem seguir e estar familiarizados, fornece diretrizes e procedimentos relativos ao uso aceitável dos computadores, recursos de tecnologia e processamento das informações da StepStone.

Tais informações incluem, sem limitação, informações técnicas, como programas de computador e bases de dados, informações comerciais, tais como os objetivos da StepStone e suas estratégias, segredos comerciais, processos, análises, gráficos, desenhos, relatórios, vendas, lucros, estatísticas, relações com clientes, estratégias de marketing, materiais de treinamento, remuneração de Colaboradores e registros, e outras informações de natureza semelhante.

A segurança das informações requer a participação e o apoio de todos os Colaboradores. Todos os Colaboradores da StepStone receberão treinamento e materiais de referência de apoio suficientes que permitam aos mesmos protegerem e administrarem adequadamente os ativos de informação da StepStone. Os materiais de treinamento sempre irão destacar que a segurança da informação é parte integral dos nossos negócios, devendo ser considerada tão vital quanto outras funções comerciais contínuas.

Ao término de seu vínculo empregatício com a StepStone, o Colaborador deverá devolver para a StepStone todos os documentos aos quais teve acesso em razão do desempenho de suas atividades.

**OBJETIVO**

Os objetivos da Política de Segurança da Informação e Segurança Cibernética são:

**(i)** assegurar e manter o sigilo, a integridade e a disponibilidade dos ativos de informação da StepStone em uma medida condizente com a sensibilidade e o valor dos dados;
**(ii)** proteger os ativos de informação da StepStone contra uso indevido, abusivo e/ou não autorizado ou utilização de informações ou registros de clientes que possam resultar em danos, em uma medida condizente com a sua sensibilidade e o seu valor;
**(iii)** educar todos os Colaboradores autorizados a não acessar ativos de informação sobre persuasão, indução, coerção e ameaças;
**(iv)** garantir a segurança e a confidencialidade das informações e registros de clientes da StepStone;
**(v)** proteger a StepStone contra quaisquer ameaças ou riscos à segurança ou integridade das informações e registros de clientes;
**(vi)** identificar e avaliar os riscos cibernéticos aos quais a StepStone está sujeita bem como delinear ações que possam mitigar estes riscos de modo a estabelecer um plano de ação para prevenção.

Adicionalmente, a Política de Segurança da Informação e Segurança Cibernética tem por objetivo documentar os procedimentos aplicáveis à segurança da informação com detalhes suficientes para que todos os Colaboradores entendam e tomem conhecimento das suas responsabilidades no que diz respeito à matéria.

**RESPONSABILIDADE DOS COLABORADORES**

Os Colaboradores são responsáveis pela segurança de toda informação que tiverem acesso ou contato, e a StepStone é responsável por oferecer treinamentos constantes para manter todos os Colaboradores informados sobre a Política de Segurança da Informação e Segurança Cibernética. É de responsabilidade da Diretora de Compliance e Riscos da StepStone, do *Chief Compliance Officer* do *Stepstone Group* juntamente com a equipe de Tecnologia do *Stepstone Group* responder as questões referentes à Segurança da Informação e Segurança Cibernética.

São responsabilidade dos Colaboradores:

- **(i)** bloquear os seus computadores quando ausentes ou não o estiverem usando; (ii)
- **(ii)** utilizar apenas computadores de propriedade da StepStone e softwares autorizados e instalados pela StepStone; e
- **(iii)** entender que tudo que for desenvolvido pelos Colaboradores ou fornecido por consultores ou provedores de serviços em benefício da StepStone são propriedade da StepStone.

**ATIVIDADES PROIBIDAS**

Os Colaboradores estão proibidos de:

- **(i)** derrubar deliberadamente qualquer sistema da StepStone;

**(ii)** tentar invadir qualquer sistema da StepStone ou burlar barreiras de segurança;
**(iii)** introduzir ou tentar introduzir qualquer vírus de computador nos sistemas da StepStone;
**(iv)** acessar informação não autorizada pela StepStone;
**(v)** instalar e/ou utilizar software pessoal não autorizado pela StepStone;
**(vi)** violar ou tentar violar os termos de uso ou licença de qualquer software utilizado pela StepStone; e
**(vii)** envolver-se em qualquer atividade ilícita ou contrária às políticas da StepStone.

**ACESSO À INTERNET**

Todos os sistemas de comunicação e todas as mensagens elaboradas ou manuseadas em equipamentos de propriedade da StepStpne são consideradas propriedade da StepStone, incluindo, mas não se limitando a, telefones, e-mails, mensagens de voz, mensagens instantâneas, internet, fax, computadores pessoais e servidores. As comunicações pessoais feitas pelos Colaboradores em computadores ou outros equipamentos fornecidos pela StepStone são permitidas desde que:

**(i)** tomem tempo razoável dos Colaboradores;
**(ii)** não interfiram com suas atividades; e
**(iii)** não descumpram nenhuma política da StepStone.

Os Colaboradores devem ter em mente que toda a comunicação poderá ser monitorada ou encaminhada, interceptada, impressa ou armazenada por terceiros. A StepStone reserva-se o direito, a seu critério, de revisar os arquivos físicos ou eletrônicos dos Colaboradores na medida do necessário para garantir que todos estejam sendo utilizados em conformidade com todas as leis e regulamentos aplicáveis, bem como com as políticas da StepStone.

**SOBRE O DEVER DE RELATAR INCIDENTES**

É responsabilidade de cada funcionário da StepStone reportar qualquer incidente ao supervisor responsável ou Diretor de *Compliance*. Qualquer pessoa autorizada a acessar qualquer tipo de informação é um indivíduo responsável pelo segurança dessa informação. Os Colaboradores devem denunciar formalmente todos os incidentes ou violações à Política de Segurança da Informação imediatamente à área de tecnologia da informação, ao seu supervisor imediato, ao seu chefe de departamento, ou ao Diretor de *Compliance*.

Os relatórios dos incidentes devem ser encaminhados o mais rápido possível, e analisados para determinar se são necessárias alterações na estrutura de segurança existente. Todos os incidentes relatados serão registrados e as medidas cabíveis aplicadas, sendo responsabilidade da StepStone fornecer treinamento sobre quaisquer mudanças ou procedimentos que possam ser necessários após o resultado da investigação de um incidente.

**TRANSFERÊNCIA DE ARQUIVOS E SOFTWARES ENTRE CASA E TRABALHO**

Nenhum software não autorizado pela StepStone pode ser instalado em computadores de propriedade da StepStone ou em sua rede, e nenhuma informação ou dado de propriedade da StepStone, incluindo informações financeiras e de recursos humanos, devem ser transferidos para um computador que não seja propriedade da StepStone. Caso haja necessidade da instalação de software ou transferência de informação deve-se explicar a necessidade de tal ação e obter o consentimento por escrito do Diretor de *Compliance.*

**IDENTIFICAÇÃO DE USUÁRIOS PARA COMPUTADORES**

A identificação de usuário ("Identificação de Usuário") para acessar os recursos de informática da StepStone é um privilégio concedido a todos Colaboradores. Cada pessoa autorizada a acessar os sistemas da StepStone deverá receber uma Identificação de Usuário única, a qual não deverá ser compartilhada com nenhum outro Colaborador. As Identificações de Usuário de Colaboradores são revistas pelo menos duas vezes ao ano e Colaboradores desligados serão imediatamente desativados mediante notificação de término do vínculo empregatício.

**SENHAS E EXIGÊNCIAS DE HARDWARE / SOFTWARE**

As senhas, combinadas com Identificações de Usuário, são utilizadas para autenticar pessoas autorizadas e conferir acesso aos recursos de informática da StepStone. Cada Identificação de Usuário deve estar vinculada a uma senha única usada para autenticar a identidade informada do usuário individual e, quando possível, registrar todas as atividades realizadas por tal pessoa para os fins da sua responsabilidade. Não é permitido aos Colaboradores compartilhar suas senhas com ninguém, inclusive com outros Colaboradores.

A StepStone possui diretrizes para a elaboração das senhas pelos Colaboradores com exigência de que todas as senhas sejam de natureza "forte". Isso significa que todas as senhas devem estar de acordo com as restrições e limitações projetadas de modo a torná-la difícil de adivinhar. As senhas também devem ser alteradas a cada 90 dias para garantir a segurança das informações.

Adicionalmente, todos os Colaboradores devem observar os seguintes procedimentos:

**(i)** As estações de trabalho devem ser fisicamente seguras e as sessões abertas devem ser bloqueadas quando deixadas sem supervisão;

**(ii)** As senhas jamais devem ser armazenadas em um sistema de computação, aparelho, ou por escrito de forma desprotegida;

**(iii)** Nenhum hardware ou software (incluindo hardwares e softwares pessoais) não autorizado deverá ser usado, carregado, instalado e/ou ativado em nenhuma estação de trabalho ou sistema de produção ou estágios sem análise e aprovação prévias; e

**(iv)** Para evitar o acesso indevido por outros Colaboradores ou terceiros, todos os Colaboradores devem fechar os programas após sua utilização e efetuar o *log-off* de seus computadores quando ausentar-se da StepStone por um período prolongado de tempo.

Além disso, são adotados os seguintes procedimentos para mitigar o risco de sistemas de informação:

**(i)** *Backups* diários, semanais e mensais;

**(ii)** O servidor da StepStone está dotado de um sistema automático de antivírus/*firewall* que atualiza as definições de vírus bem como as definições de segurança do *firewall* em todos os postos; e

**(iii)** Por meio de um processo online, diariamente, é feito um *check-up* (antivírus, *firewall* e backup) de todas as estações de trabalho.

**RESTRIÇÕES AO USO DE RECURSOS DE INFORMÁTICA DA STEPSTONE**

Os computadores e recursos de tecnologia da StepStone existem para a finalidade exclusiva de conduzir os negócios oficiais da StepStone.

Todos os Colaboradores devem seguir políticas e procedimentos corporativos para a compra e uso de todos os equipamentos, hardwares e softwares.

É contra a política da StepStone que Colaboradores utilizem quaisquer equipamentos de informática, suprimentos ou instalações para uso pessoal, sendo vedado aos Colaboradores remover qualquer tipo de informações das instalações da StepStone, a menos que necessário para conduzir os negócios da StepStone.

**CONTROLE DE ACESSO**

As informações da StepStone e de seus clientes e projetos estão sujeitas a controle de acesso, incluindo comunicações internas e externas pela internet. Não será concedido acesso à nenhuma informação cujo acesso seja restrito sem o expresso consentimento do indivíduo responsável pela informação. Quaisquer pedidos de alterações de acesso no sistema, direitos de dados ou grupos de distribuição de e-mail serão realizados após o aval do Diretor de *Compliance*.

**AVALIAÇÃO DA POLÍTICA DE USO DA REDE**

A StepStone monitora a utilização da internet pelos seus Colaboradores. Na hipótese de algum funcionário utilizar uma quantidade excessiva de tempo ou consumindo grandes quantidades de dados para uso pessoal, serão tomadas as medidas disciplinares cabíveis.

Para assegurar os procedimentos mencionados, a StepStone reserva o direito de:

**(i)** Empregar softwares e sistemas capazes de monitorar e registrar todos os usos do e-mail corporativo e da Internet através da rede de estações de trabalho da StepStone;

**(ii)** Inspecionar qualquer arquivo armazenado na rede, no *hard drive* do computador ou em áreas privadas da rede a fim de assegurar o cumprimento rigoroso deste Manual; e

**(iii)** Manter um conjunto de softwares e hardwares instalados para proteger a rede interna e a integridade de dados e programas.

**USO DE IMPRESSORAS**

É terminantemente proibido que os Colaboradores façam cópias (físicas ou eletrônicas) ou imprimam os arquivos utilizados, gerados ou disponíveis na rede da StepStone, circulando com estes em ambientes externos à StepStone uma vez que tais arquivos contêm informações confidenciais.

A proibição acima referida não é aplicável quando as cópias (físicas ou eletrônicas) ou a impressão dos arquivos forem em prol da execução e do desenvolvimento dos negócios e dos interesses da StepStone. Nestes casos, o Colaborador que estiver de posse e guarda da cópia ou da impressão do arquivo que contenha a informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

**REVISÃO**

Todos os procedimentos previstos na Política de Segurança da Informação e Segurança Cibernética da Stepstone serão revisados anualmente ou em caso de alterações regulamentares.