POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

REVISÃO 04/2024
VERSÃO 3

Índice

OBJETIVO

A Política de Segurança da Informação ("**Política**") da SIG Capital Gestão de Recursos Ltda. ("**SIG Capital**") visa proteger as informações de propriedade e/ou sob guarda da SIG Capital, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Sendo assim, nenhuma informação sigilosa deve, em qualquer hipótese, ser divulgada a pessoas, dentro ou fora da SIG Capital, que não necessitem de, ou não devam ter acesso a tais informações para desempenho de suas atividades profissionais.

ABRANGÊNCIA

As diretrizes estabelecidas nesta Política devem ser observadas por todos os sócios, diretores, funcionários e estagiários que utilizam os recursos de tecnologia da informação disponibilizados pela SIG Capital, sendo de responsabilidade individual e coletiva o seu cumprimento ("**Colaborador**" e em conjunto como os "**Colaboradores**").

GESTÃO DA POLÍTICA

Cabe a todos os Colaboradores:

(a) Cumprir fielmente esta Política;

(b) Buscar orientação do superior hierárquico imediato ou a da área de *Compliance* em caso de dúvidas relacionadas à segurança das informações;

(c) Proteger as informações contra acesso, modificação, destruição ou divulgação não autorizados pela SIG Capital;

(d) Assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente pela SIG Capital;

(e) Cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às informações sigilosas; e

(f) Comunicar imediatamente a área responsável pela Tecnologia da Informação sobre qualquer descumprimento ou violação desta Política.

DIRETRIZES

Comportamento Seguro

É fundamental para a proteção das informações da SIG Capital que os Colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

(a) Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das informações sigilosas;

(b) Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das informações sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;

(c) Todo tipo de acesso aos dados e informações da SIG Capital que não for expressamente autorizado é proibido;

(d) Assuntos relacionados ao desempenho de atividades e funções na SIG Capital não devem ser discutidos em ambientes públicos ou em áreas expostas;

(e) As senhas de acesso do Colaborador aos sistemas da SIG Capital, bem como *tokens*, chaves e/ou senhas de acesso à arquivos físicos e/ou às dependências da SIG Capital, são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores), anotadas em papel ou em sistema visível ou de acesso não protegido;

(f) Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;

(g) Somente *softwares* homologados e previamente aprovados pela SIG Capital podem ser instalados e usados nas estações de trabalho, o que deve ser feito com exclusividade pela equipe terceirizada de serviços de informática da SIG Capital;

(h) Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da SIG Capital;

(i) Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter informações sigilosas. Portanto, não podem ser parciais ou totalmente divulgadas, usadas ou reproduzidas sem o consentimento prévio do remetente ou do autor. Toda e qualquer divulgação, uso e/ou reprodução não expressamente autorizada é proibida;

(j) Documentos impressos e arquivos contendo informações sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da SIG Capital sem a autorização prévia do superior hierárquico do Colaborador; e

(k) O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela SIG Capital. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento à terceiros, bem como com conteúdo político ou outro que possa colocar a SIG Capital em risco.

Gestão de acessos

O uso de informacões sigilosas e dos recursos de tecnologia disponibilizados pela SIG Capital são monitorados e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política e demais regras internas da SIG Capital, através de monitoramento a ser efetuado pela área de *Compliance*.

Todo acesso às informacões sigilosas, aos ambientes lógicos e à sede da SIG Capital deve ser controlado, de forma a garantir acesso apenas às pessoas expressamente autorizadas pela área de *Compliance*.

A área responsável pela Tecnologia da informação deve:

(a) Assegurar o controle de informações privilegiadas, incluindo, mas não se limitando a, controle de arquivos físicos e eletrônicos e as restrições na divulgação de informações confidenciais, opiniões e recomendações

(b) Assegurar a existência de testes periódicos de segurança para os sistemas de informações, em especial para os mantidos em meio eletrônico;

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

(a) Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;

(b) Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador;

(c) Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da SIG Capital, ou que tenham mudado de função, se for o caso; e

Utilização de internet

O uso da internet deve restringir-se às atividades relacionadas aos negócios e serviços da SIG Capital e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

Monitoramento e controle

Os sistemas, serviços, dados, informações disponíveis na SIG Capital ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito à monitoramento, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware) pela área responsável pela Tecnologia da Informação e de *Compliance* e/ou por prestador de serviços externo.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política e nos demais documentos internos da SIG Capital, e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

Sites na internet

O acesso à sites externos na internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da SIG Capital. Adicionalmente, a área de *Compliance* poderá ser informada sobre acessos e tentativas de acesso à determinados sites.

Ramais telefônicos

Os ramais telefônicos utilizados na sede da SIG Capital pelos Colaboradores via PABX virtual. A área de *Compliance* a este monitoramento, caso seja identificada alguma situação de risco ou infração às políticas internas e/ou legislação, com o propósito de verificação de conteúdo.

Mensagens instantâneas

A comunicação por mensagens instantâneas de texto e voz pela internet também devem ser conduzidas sob as normas e regras contidas neta política, incluindo mas não se limitando, à confidencialidade.

Utilização e conexão de equipamentos

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela SIG Capital.

A utilização de equipamentos pessoais nas instalações da SIG Capital e a conexão destes na rede interna e à internet requer autorização prévia e expressa do responsável pela área de Compliance.

SEGURANCA CIBERNÁTICA

A SIG Capital realiza, avaliações e testes de seu sistema de segurança de informações por meio de uma empresa terceirizada, a fim de identificar possíveis riscos ao seu sistema cibernético. Esta avaliação de riscos visa proteger informações confidenciais de nossos clientes, aprimorar a segurança cibernética da SIG Capital, bem como apresentar um plano de ação quando da ocorrência de algum ataque cibernético.

O Programa de Segurança Cibernética da SIG Capital abarca as seguintes funções:

(a) Identificação e avaliação de riscos internos e externos;

(b) Elaboração de regras e procedimentos para reduzir e minimizar a ocorrência de riscos de um ataque cibernético;

(c) Identificação de ameaças e de possíveis distúrbios no ambiente cibernético em tempo hábil;

(d) Tratamento e recuperação de incidentes;

MANUTENCÃO DOS DOCUMENTOS

Todo o material produzido decorrente desta Política será mantido nos arquivos e diretórios da SIG Capital por, no mínimo, 5 (cinco) anos, conforme disposição regulatória e/ou jurídica.

APROVAÇÃO, VIGÊNCIA E ATUALIZAÇÃO

Esta Política foi aprovado pela Diretoria de Compliance em abril de 2024, e será revisado periodicamente pela equipe de Compliance. Serão utilizadas como base para sua atualização as legislações, instruções normativas, regulamentações e melhores práticas vigentes na data da sua revisão.

Versão	*Data*	*Elaborado / Modificado por:*	*Aprovado por:*
v.03	*04/2024*	*Dir. Risco e Compliance*	*Dir. Risco e Compliance*