POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

JULHO DE 2022

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA
SPINNAKER INVESTIMENTOS LTDA.

Esta "Política de Segurança da Informação e Segurança Cibernética" ("Política de Segurança da Informação") é de propriedade exclusiva da Spinnaker Investimentos Ltda. ("Spinnaker") e foi elaborado levando-se em consideração a regulação vigente no mercado brasileiro.

Este documento deve ser utilizado apenas para fins informativos, não se tratando de uma oferta de venda ou de uma oferta de compra de cotas de fundos geridos pela Spinnaker.

Nenhuma das informações neste documento modifica ou altera de forma alguma termos e condições estabelecidos em regulamentos, prospectos ou outros documentos de fundos geridos pela Spinnaker.

Sumário

1. INTRODUÇÃO

A Informação é um ativo que tem um alto valor para a organização e pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for a forma pela qual a mesma é apresentada, transmitida, armazenada ou compartilhada, é necessário que a mesma seja protegida adequadamente.

A Política de Segurança da Informação protege a Informação de diversas ameaças ou de seu mal uso, para garantir a continuidade dos negócios, a integridade e a disponibilidade da mesma.

A Política de Segurança da Informação visa preservar a confidencialidade, integridade e disponibilidade das informações, descrevendo a conduta adequada para o seu manuseio, controle, proteção e descarte.

Este documento tem por finalidade descrever a Política de Segurança da Informação e estabelecer diretrizes de utilização dos recursos de informática da Spinnaker.

Todas as normas aqui estabelecidas deverão ser seguidas rigorosamente por todos os colaboradors, parceiros e prestadores de serviços.

Ao receber essa cópia da Política de Segurança, todos que dela tiverem ciência, comprometem-se a respeitar todos os tópicos aqui abordados e declaram estar cientes de que seus e-mails e navegação na internet podem ser auditados.

2. DESCRIÇÃO DA POLÍTICA

A Spinnaker disponibiliza os recursos de informática aos seus colaboradores, visando proporcionar o perfeito desempenho de suas funções.

Todo colaborador deve ser orientado sobre as questões de segurança.

Nenhum pré-requisito técnico é necessário, visto que a política aborda o contexto comportamental do usuário, e não os aspectos técnicos, os quais serão delegados a equipe especializada.

O objetivo desta política é estabelecer procedimentos e responsabilidades relativos à utilização dos recursos computacionais colocados à disposição dos usuários com o objetivo de garantir bom desempenho e de mitigar os riscos associados aos seguintes aspectos:

• Acessos não autorizados aos sistemas, aplicativos e rede corporativa;

• Danos causados por códigos maliciosos (vírus);

• Utilização de software ilegal;

• Mal uso dos recursos computacionais (e-mail, Internet, ferramenta de mensagem instantânea e outros permitidos pela empresa).

2.1 Autenticação

- A identificação do usuário em relação aos recursos de TI é feita através do seu login de rede, o qual é pessoal e intransferível;

- A autenticação nos sistemas de informática é baseada na utilização de usuários e senhas distintas, que é o método mais comum por sua facilidade de implantação e manutenção, também por seu baixíssimo custo;
- Todo colaborador da empresa ao operar os sistemas da rede corporativa, deverá ter seu login e senha pessoal. Não é autorizada a utilização das credenciais de outro colaborador.

2.2 Senhas

- É a assinatura eletrônica pessoal. Portanto, não deverá ser divulgada ou emprestada a outra pessoa, nem mesmo à equipe de TI;
- Deve possuir no mínimo 8 (OITO) caracteres e no máximo 15 (QUINZE), deve possuir caracteres especiais, letras e números. A senha não poderá serrepetida antes de 5 (CINCO) trocas de senha;
- Será bloqueada após 5 (CINCO) tentativas de acesso errado. Caso isso ocorra, o usuário poderá tentar novamente após 30 minutos, ou solicitar o reset pela equipe de TI;
- A cada 90 dias será solicitada automaticamente a troca da senha de acesso a rede interna.

É proibido:

- Salvar senhas em arquivos na rede ou nas estações de trabalho;
- Anotar senhas em Post it ou rascunhos nas mesas e deixar em local visível ou de fácil acesso;
- Tudo que for executado com a senha será de inteira responsabilidade do usuário, por isso devem ser tomadas todas as precauções para mantê-la secreta;
- Qualquer alteração necessária de login e/ou senha deverá ser solicitada ao gestor direto, e este encaminhará por e-mail a solicitação ao departamento de TI.

2.3 Correio Eletrônico (e-mail)

- O acesso ao serviço de correio eletrônico é restrito aos colaboradors para o exercício e desempenho de suas atividades na empresa;
- A liberação do correio eletrônico somente será feita com a autorização do responsável pelo setor, através de requisição formal;
- Todas as contas de e-mail possuem espaço limitado a 100GB para armazenamento das mensagens.
- A empresa se reserva no direito de monitorar eletronicamente a utilização e inibir o mau uso destes recursos;
- O envio de e-mail é limitado a 100 destinatários por mensagem, independente do sistema utilizado;
- Se houver a necessidade de distribuir mensagens para grandes grupos de usuários e/ou arquivos de grande volume, deve-se estudar juntamente com a área de informática formas que não prejudiquem o tráfego da rede, tendo em vista que esta prática requer recursos não contemplados na estrutura atual, a referida solicitação deve ser feita com antecedência;
- Acessos ao webmail, somente serão permitidos, mediante solicitação/autorização pela diretoria da empresa encaminhados ao departamento de TI por e-mail;
- O acesso ao e-mail da empresa por meio de dispositivos móveis (celular, tablet, etc...) deverá ser autorizado pelos gestores da empresa, com registro da solicitação por e-mail, caso contrário implicará em desacordo com o Termo de Confidencialidade de Informações.

É proibido:

- O envio de mensagens com assuntos e conteúdos obscenos, ofensivos e que possam representar qualquer forma de discriminação racial, sexual ou religiosa;

- A utilização do Correio Eletrônico para o envio de “Correntes” (Ex.: Envie este e-mail para 10 amigos para melhorar de vida);
- O envio de mensagens com conteúdo de utilidade pública (Ex.: Lista de radares, pessoas desaparecidas);
- O envio e/ou recebimento de mensagens com arquivos anexos com os seguintes tipos de arquivos: música, executáveis, vídeo e scripts (Ex.: *.bat, *.vbs), ou qualquer outro arquivo que possa ser identificado como nocivo à rede corporativa;
- Redirecionamento de e-mail para contas pessoais, ou não oficiais (Ex.:@gmail.com, @yahool.com, @hotmail.com, etc.);
- Adicionar seu endereço de e-mail pessoal em cópia ou cópia oculta, ou algum endereço não oficial da empresa, que não seja cabido ao assunto;
- Pedir para clientes ou fornecedores enviar e-mails para destinatários não oficiais, ou seja fora do domínio spinnaker.com.br.

2.4 Internet

- O acesso à Internet é restrito aos colaboradors que necessitem para o desempenho de suas atividades na empresa;
- A liberação do acesso à Internet somente será feita com a autorização do gerente responsável pela área, a devida solicitação deverá ser encaminhada ao departamento de TI via sistema de chamados interno. (ver tabela 3.2);
- O acesso aos sites na Internet é monitorado eletronicamente e poderá ser divulgado aos seus superiores quando solicitado pelos mesmos.

É proibido:

- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados;
- Acessar, baixar ou transmitir materiais que possam ser interpretados como obscenos, inadequados, não condizentes com os interesses da empresa, visando lucros pessoais, ou que violem a política de segurança da empresa;
- A conexão de estações a provedores de internet externos utilizando o modem discado, modem 3G, ou outro que permita a navegação de internet visando driblar o monitoramento, exceto através de uma autorização da área de TI e justificada através de registro de exceção o porquê desta tomada de decisão;
- Uso de ferramentas P2P (kazaa, Morpheus,Utorrent etc);
- Uso de IM (Instant messengers) não homologados/autorizados pela equipe de TI e com o aval do gestor direto;
- Acesso a sites de WEBPROXIES (sites que camuflam a navegação driblando assim a inteligência de segurança definida nos equipamentos de monitoração e bloqueio);
- O colaborador que for identificado como usuário de uma das práticas acima, por meio do seu login de registro, estará passível de sofrer sanção por parte da empresa.

2.5 Mensagem Instantânea

- Fica proibida a utilização de qualquer ferramenta de mensagens instantâneas particular do colaborador (Messenger, AIM, ICQ, Skype, Blackberry Messenger etc) na infraestrutura de rede da empresa, sem prévia autorização formal dos gestores da empresa, independente do meio utilizado para isso (SmartPhone, BlackBerry, Ipad, etc);
- Caso autorizado pelos gestores, usuários “chaves” poderão utilizar a ferramenta SKYPE para contato com fornecedores e comunicação pertinentes à empresa, porém, esta autorização deverá ser encaminhada ao departamento de TI via sistema de chamados pelo gestor autorizador.

2.6 Antivírus

- A área TI irá instalar e manter atualizada a versão do antivírus nos equipamentos, orientando os usuários sobre as providências a serem tomadas em caso de contaminação;
- Todo arquivo recebido, proveniente de qualquer mídia, não importando sua origem, deve passar por um processo de verificação de vírus antes de sua utilização.

2.7 Estação de Trabalho

- A disponibilização de equipamento de informática é feita através da abertura de um chamado para a área de TI através de e-mail indicando o local, o departamento, o gestor responsável e caso já tenha algum colaborador designado para o equipamento, informar nome completo do mesmo;
- A manutenção/reparo dos equipamentos de informática é feita exclusivamente pela área de TI;
- A substituição ou alteração de local do equipamento, solicitada pelo responsável do setor através de e-mail, somente poderá ser executada pela área de TI;
- O usuário é responsável direto pela conservação, guarda e utilização dos equipamentos mantidos a sua disposição;
- Equipamentos portáteis (Notebooks, Tablets e Smartphones) devem ser mantidos pelos usuários em lugar seguro, com especial atenção contra roubos, avarias ou uso não autorizado de terceiros;
- Equipamentos portáteis (Notebooks, Tablets e Smartphones) pessoais ou de empresas parceiras, não são de responsabilidade da SPINNAKER CAPITAL, e seu uso na infraestrutura de rede da empresa, só poderá ser realizado mediante autorização formal da diretoria;
- A necessidade de novos equipamentos, bem como as expansões da infraestrutura de informática (redes, novas tecnologias e servidores), devem ser submetidas à área de TI, que efetuará um estudo de viabilidade da aquisição e homologação dos mesmos, como forma de garantir sua aderência aos padrões e à política de segurança da empresa;
- Toda vez que precisar se ausentar da sua estação de trabalho, o colaborador deverá proceder o bloqueio de sua estação, caso não o faça, a política de segurança fará o bloqueio da estação após 15 (quinze) minutos de inatividade.
- Acesso Remoto é executado através do aplicativo TeamViewer (versão corporativa). Este acesso se dá através de senha com dupla autenticação, em que um SMS é enviado ao celular do colaborador pelo aplicativo contendo um código de acesso, sendo este código mandatório para o sucesso da autenticação. A cada acesso são gerados logs de autenticação de login\logout, estes logs serão armazenados para efeito de auditoria e conformidades LGPD.

É proibido:

- A entrada e saída de equipamentos de informática sem o conhecimento e a autorização do gerente de TI ou diretoria da empresa por e-mail;
- A manutenção de equipamentos particulares;
- Instalar software ou hardware sem autorização do gerente de TI;
- Manter arquivos de músicas, filmes, fotos e softwares com violação de direitos autorais ou qualquer outro tipo de pirataria.

2.8 Telefonia

- Solicitação de novos ramais, programação e retirada dos mesmos, deverão ser feitas diretamente à área de TI, pelo gestor do departamento solicitante e por e-mail.

2.9 Software

- A homologação de softwares, mesmo os de domínio público, "*freeware*" e "*shareware*", é responsabilidade da Gerencia de TI. Sendo assim, todo e qualquer software só poderá ser adquirido, instalado, atualizado ou removido nos computadores, através da área de TI. Para qualquer um destes procedimentos, só serão aceitas solicitações encaminhadas ao departamento de TI pelo gestor direto do operador;
- A guarda das mídias dos softwares é de responsabilidade da área de TI, assim como todas as fontes de instalação dos programas utilizados pela empresa;
- A liberação de acesso ao software deve ser formalmente autorizada pela chefia imediata do usuário por e-mail ao departamento de TI;
- Somente será permitida a utilização de cópias de software legal e que tenham passado pelo processo de homologação do departamento de TI.

É proibido:

- A instalação dos softwares da empresa em máquinas particulares, e/ou empréstimos de mídias (cd's) para instalações externas;
- O desenvolvimento de softwares/sistemas para a Organização, pelos usuários, sem o conhecimento da área de TI;
- Instalação de softwares não homologados pela equipe de TI;
- A duplicação, empréstimo, transferência ou retirada de software para outros equipamentos, dentro ou fora de empresa.

2.10 Acesso aos Sistemas de Informação

- O departamento de TI é responsável por conceder o acesso a cada um dos Sistemas de Informação. O departamento somente pode executar qualquer ação sob autorização do gestor direto da área interessada no acesso do sistema ou módulo;
- Esta autorização deve ser formal, por e-mail ou de forma impressa. Nele são indicados quais os Grupos de Acesso que o usuário fará parte. Estes Grupos de Acesso devem ser definidos pelo gestor da área interessada em conjunto com o departamento de TI;
- É de responsabilidade também do gestor da área interessada no acesso, a avaliação sobre capacitação técnica de utilização do usuário;
- Os logins e senhas serão solicitados para o departamento de TI pelo gestor do colaborador, requisição esta que deve ser encaminhada por e-mail informando nome completo, setor de atividade e specificando quaisquer observações necessárias quanto a esta requisição;
- Caso a solicitação seja urgente, e por qualquer motivo o gestor não possa solicitar por e-mail, o mesmo poderá fazê-la por telefone ou pessoalmente, porém, logo após a execução do procedimento, o departamento de TI encaminhará um e-mail ao gestor solicitante informando a execução da atividade ou liberação do referido acesso;

2.11 Desenvolvimento Novas Soluções

- Novas necessidades, relacionadas aos sistemas de informação atuais, deverão ser enviadas formalmente à Gerência de TI. É responsabilidade do departamento de TI, a partir desta requisição, avaliar;
- Adaptar a forma atual como o sistema trabalha para que atenda à nova necessidade;
- Proceder a correções em caso de erro de concepção ou implementações do sistema;
- Desenvolver de forma incremental uma extensão para o sistema, para atender as expectativas e necessidades do grupo, quando o sistema for desenvolvido por sua própria equipe;
- Em caso de implantação de software de equipe externa, o departamento de TI disponibilizará um técnico para acompanhamento da implantação do novo software, ficando a cargo da empresa contratada a integração com os atuais sistemas da empresa;
- O gestor da área solicitante deverá homologar a nova solução. Com isto os interessados certificam que a nova solução está apta para utilização, assumindo que a partir deste momento a mesma sairá da fase de testes para entrar em produção

3. AUDITORIAS

Serão realizadas auditorias periódicas para verificação do grau de cumprimento desta Política.

A empresa poderá monitorar e registrar o envio/recebimento de mensagens do correio eletrônico, a navegação na internet, o acesso aos sistemas aplicativos e os softwares utilizados, respeitando a confidencialidade sobre o conteúdo dos itens auditados, mas dispensando, em razão da divulgação desta política, qualquer notificação prévia.

Qualquer irregularidade ou divergência em relação a esta norma deve ser imediatamente comunicada ao departamento de TI por e-mail, o qual tomará as medidas cabíveis para regularizar a situação.

4. RESPONSABILIDADES

4.1 Reponsabilidade do Departamento de TI

O departamento de TI é responsável pelos aspectos abaixo listados:

• Elaboração desta Política de Segurança da Informação;

• Garantir sua correta execução por parte de seus integrantes;

• Garantir a disponibilidade dos serviços de e-mail para todos os usuários observando suas respectivas características operacionais;

• Efetuar backup de todos os arquivos salvos nos respectivos diretórios dos servidores conforme descritos na tabela do item 1.9 deste documento;

• Gerenciar o uso correto dos e-mails da empresa garantindo sua disponibilidade bem como sua segurança de dados;

• Verificar a correta armazenagem dos dados contidos em servidores, bem como verificar a integridade e segurança dos referidos dados por meio que julgar cabíveis tecnicamente, desde que não firam quaisquer das normas aqui descritas;

• Efetuar a restauração de dados quando solicitados.

4.2 Responsabilidades dos Colaboradores em Geral

É reponsabilidade de todos os colaboradores da empresa os seguintes aspectos sobre este documento:

• Ler e compreender todos os termos aqui descritos;

• Primar pela segurança de seus dados de acesso (login e senha);

• Cuidar de todos os equipamentos que forem disponibilizados pela empresa para o desempenho de suas atividades;

• Primar pelo correto uso que faz dos meios que a empresa lhe disponibiliza para acesso às informações (internet, e-mail, rede de dados, dispositivos de acesso, etc..);

• Informar ao seu gestor direto toda e qualquer não conformidade com suas atividades quando decorrentes de itens compreendidos por esta política;

• Colaborar com toda e qualquer solicitação feita ao mesmo pelo departamento de TI no que se refere ao desempenho de suas atividades dentro da empresa;

• Sempre que se ausentar de sua estação de trabalho deverá proceder o bloqueio da mesma, caso contrário, dentro de 10 (Dez) minutos a Política de Segurança irá proceder o bloqueio da mesma de forma

automática.

5. CASOS ESPECIAIS OU NÃO CONTEMPLADOS

Os casos especiais ou não contemplados nesta Política de Segurança da Informação deverão ser levados ao conhecimento do departamento de TI para que possam ser analisados e discutidos como proceder referente aos mesmos, e se necessário, proceder a atualização desta PSI.

Sempre que houver um caso especial ou não contemplado por esta PSI, o mesmo deverá ser um fato gerador de atualização da PSI.

Para que esta política possa surtir seus referidos efeitos, todos os colaboradores, prestadores de serviços e demais usuários de quaisquer meios aqui descritos, quando nas dependências da empresa ou por força de suas atividades profissionais, deverão assinar o Termo de Responsabilidade e Ciência deste documento, os quais permanecerão arquivados junto com uma cópia impressa e assinada por todos os gestores da empresa dando ciência do conhecimento desta PSI.

Será requerido um Termo de Responsabilidade para cada usuário, não podendo o mesmo ser assinado em conjunto.

Em casos especiais será solicitada a assinatura também do Termo de Confidencialidade de Informações.

6. DISTRIBUIÇÃO

Esta Política será apresentada a todos os colaboradores no processo de admissão. Para os demais colaboradores a Política será distribuída internamente por meio eletrônico e disponibilizada via sistema interno, ou ainda em arquivo PDF, disponível para consulta em qualquer momento por parte dos usuários.

Esta Política foi registrada na ANBIMA em sua versão integral e atualizada, ficando disponível para a consulta pública, sem restrições, no seguinte endereço eletrônico: http://www.spinnaker.com.br

7. VIGÊNCIA E ALTERAÇÕES

Esta Política de Segurança da Informação (PSI) entrará em vigência na sua data e publicação, e assim permanecerá até que passe por revisão e seja eventualmente alterada sua redação inicial.

Nenhuma alteração será redigida de forma arbitrária por nenhuma das partes aqui envolvidas, visto que, este documento é orientador às atividades de todos os setores da empresa que utilizem os meios aqui descritos, desta forma, toda e qualquer alteração deve ser antes analisada em conjunto com todos os interessados, e suas

alterações devidamente registradas por meio de nova redação do documento, indicando quais alterações foram procedidas.