PSI – Política de Segurança da Informação

Documento de Diretrizes e Normas Administrativas

DISTRIBUIÇÃO E VIGÊNCIA

Este documento consiste na Política de Segurança da Informação –FLYTEL TELEMÁTICA COMÉRCIO LTDA, que deve ser mantida como uma medida de boas práticas, estabelecendo diretrizes para a proteção de ativos e prevenção de responsabilidades. Destaca-se que a mesma deve ser adotada, cumprida e aplicada em todas as áreas da empresa.

Há qualquer momento, essa versão poderá sofrer alteração, uma vez que os pontos apontados sofram alguma mudança, devendo ser revisada periodicamente.

Versão 2.0 de dezembro de 2022.

Índice

GLOSSÁRIO

Ativo: Algo que tenha valor para a organização.

Evento: Acontecimento que acarrete a mudança do estado atual de um processo.

Incidente: Evento que possa trazer prejuízos à empresa.

Mail bombing: Envio de mensagens eletrônicas em massa para um determinado destinatário com o objetivo de sobrecarregar o serviço de e-mail e torná-lo inutilizável ou indisponível.

Malwares: O nome malware vem do inglês malicious software (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode ou não trazer danos ao computador.

Phishing: Mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamentos para sites ou números de telefone, a fim de roubar sua identidade.

Risco: Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos.

SPAM: É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para muitas pessoas.

Vulnerabilidade: Fragilidade, vulnerabilidade de segurança pode ser vista como qualquer fator que possa contribuir para possibilitar invasões, roubos de dados ou acessos não autorizados, podendo gerar danos a terceiros e/ou a empresa.

INTRODUÇÃO

A presente Política de Segurança da Informação – PSI está baseada nas recomendações da norma ABNT NBR ISSO/IEC 27002:2005, e ainda buscando estar em conformidade com os preceitos da Lei Geral de Proteção de Dados, sob o nº 13.709/2015, visando em todos os aspectos a segurança e a proteção dos dados.

A informação é um ativo de grande valor para a FLYTEL, por isso necessita ser adequadamente protegida.

> "Segurança da Informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio" (ABNT NBR ISO/IEC 17799:2005).

Por princípio, a Segurança da Informação deve abranger três propriedades básicas:

- **Confidencialidade**: Propriedade que estabelece que a informação deva estar acessível apenas para pessoas autorizadas;
- **Integridade**: Propriedade que estabelece que a informação esteja correta, confiável e sem a ocorrência de mudanças não autorizadas;
- **Disponibilidade**: Propriedade que estabelece que a informação esteja sempre acessível para uso legítimo de pessoas autorizadas.

Dessa forma, é imprescindível a criação de uma política que normatize e direcione os procedimentos necessários para garantir a segurança das informações e a consequente excelência no atendimento aos nossos clientes, sendo este o caráter do documento ora apresentado.

1. A EMPRESA E A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A FLYTEL tem como missão atuar com excelência e prestar um serviço de inquestionável qualidade, sendo assim, a segurança da informação faz parte do rol de medidas para alcançar os objetivos da empresa.

De acordo com a ABNT, "A segurança da informação que pode ser alcançada por meios técnicos é limitada e deve ser apoiada por uma gestão e por procedimentos apropriados" (ABNT NBR ISO/IEC 17799:2005).

O objetivo dessa PSI é estabelecer normas, diretrizes e procedimentos que assegurem a segurança das informações, ao tempo que não impeçam e/ou dificultem o processo do negócio, mas que garantam:

- **A confiabilidade das informações** através da preservação da confidencialidade, integridade e disponibilidade dos dados da empresa e de clientes;

- **O compromisso da empresa** com a proteção das informações de sua propriedade e/ou sob sua guarda;

- **A participação e cumprimento** por todos os colaboradores em todo o processo.

2. OS COLABORADORES DEVEM SE PREOCUPAR COM SEGURANÇA

O processo de segurança da informação deve envolver todos os colaboradores, independentemente do nível hierárquico, posto que, de posse de uma informação específica qualquer pessoa pode, por descuido e/ou com má intenção, se tornar um agente de divulgação não autorizada, sendo assim, todos são responsáveis por salvaguardar os dados da FLYTEL e outros quais a empresa venha ter acesso.

Diante do exposto, a PSI vem propor uma Gestão de Segurança da Informação baseada em controles e procedimentos técnicos, considerando e promovendo o comportamento dos colaboradores de forma que possa aplicar a tecnologia adequada em todo o processo e atingir efetividade em seu objetivo: entender o negócio e aplicar segurança a ele.

3. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações devem ser classificadas e identificadas por rótulos, considerando os seguintes níveis:

- Pública;
- Interna;
- Confidencial;

a) Pública

São informações explicitamente aprovadas por seu responsável para consulta irrestrita e cuja divulgação externa não compromete o negócio e que, por isso, não necessitam de proteção efetiva ou tratamento específico.

São exemplos de informação pública:

- Editais de licitação;

b) Interna

São informações disponíveis aos colaboradores da FLYTEL para a execução de suas tarefas rotineiras, não se destinando, portanto, ao uso do público externo.

São exemplos de informações internas:

- Procedimentos internos;
- E-mails;
- Avisos e campanhas internas;

c) – Confidencial

São informações de acesso restrito a um colaborador ou grupo de colaboradores. Sua revelação pode violar a privacidade de indivíduos, violar acordos de confidencialidade, dentre outros.

São exemplos de informações confidenciais:

- Contratos empresariais,
- Segredos empresariais:
- Processos judiciais;
- Dados cadastrais de funcionários.

4. DAS RESPONSABILIDADES

a) Colaboradores

Será de inteira responsabilidade de funcionários, terceirizados e demais colaboradores da FLYTEL:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação;
- Buscar sempre informação para esclarecimentos de dúvidas referentes à PSI;
-Proteger as informações contra acesso, divulgação, modificação e/ou destruição não autorizados pela empresa;
- Garantir que equipamentos e recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela FLYEL;
- Descarte adequado de documentos de acordo com seu grau de classificação;

- Comunicar prontamente, de imediato qualquer violação a esta política, suas normas e procedimentos.

b) Gestores de Pessoas e/ou Processos

Em relação à segurança da Informação, cabe aos gestores de pessoas e/ou processos:

- Aprovar a Política de Segurança da Informação e suas atualizações;
- Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob sua gestão;
- Dar ciência, na fase de contratação e formalização dos contratos individuais de trabalho, à responsabilidade do cumprimento da PSI da FLYTEL;
- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Exigir de parceiros, prestadores de serviços e outras entidades externas, a assinatura do termo de confidencialidade referente às informações às quais terão acesso;
- Informar, sempre que necessário, atualizações referentes a processos e/ou cadastros de funcionários para que as permissões possam ser concedidas ou revogadas de acordo com a necessidade;

c) Responsável pelo setor de Tecnologia da Informação

Cabe ao responsável pelo setor da Informação e Informática:

- Definir as regras para instalação de software e hardware;
- Monitorar os acessos às informações e aos ativos de tecnologia (sistemas, bancos de dados, recursos de rede etc.), tendo como referência a Política e as Normas de Segurança da Informação;
- Mediante informações, manter registro e controle atualizados de todas as liberações de acesso concedidas, providenciando sempre que demandado formalmente, a pronta suspensão ou alteração de tais liberações;
- Propor as metodologias e processos referentes à segurança da informação, como classificação da informação, avaliação de risco, análise de vulnerabilidades etc.;
- Promover o envolvimento entre toda a equipe, através de palestras de conscientização dos colaboradores em relação à importância da segurança da informação para negócios da FLYTEL.
- Manter comunicação efetiva sobre possíveis ameaças e novas medidas de segurança;

5. POLÍTICA DE UTILIZAÇÃO DA REDE

O ingresso à rede interna da FLYTEL deve ser devidamente controlado para que os riscos de acessos não autorizados e/ou indisponibilidade das informações sejam mitigados. Assim, é preciso que sejam instauradas algumas regras, listadas a seguir:

1) A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade da FLYTEL, com a finalidade restrita à realização de atividades inerentes ao desempenho de tarefas laborais dos colaboradores;

2) A Senha da Internet sem fio deverá ser criada pelo gestor da rede.

3) A FLYTEL reserva-se o direito de monitorar e registrar o acesso à Internet como forma de inibir a proliferação de programas maliciosos, garantindo a integridade da rede, sistemas e dados internos;

4) Os equipamentos, tecnologias e serviços fornecidos para o acesso à Internet são de propriedade da FLYTEL, que pode analisar e, se necessário, bloquear qualquer arquivo, site, e-mail, domínio ou aplicação, visando assegurar o cumprimento de sua Política de Segurança da Informação.

5) A Internet disponibilizada pela FLYTEL aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que seja autorizada e não prejudique o andamento dos trabalhos na empresa;

6) Apenas colaboradores devidamente autorizados a falar em nome do FLYTEL para meios de comunicação e/ou entidades externas poderão manifestar-se, seja por e-mail, entrevistas, documento físico, ligação telefônica etc.;

7) É proibida a divulgação e/ou o compartilhamento indevido de informações, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;

8) Os colaboradores com acesso à Internet só poderão fazer o download programas necessários às suas atividades na FLYTEL;

9) O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo responsável do setor de tecnologia e informação;

10) Os colaboradores não poderão em hipótese alguma utilizar os recursos da FLYTEL para fazer o download ou distribuição de software falsificado, atividade considerada delituosa de acordo com a legislação nacional;

11) Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer equipamento e/ou ambiente físico da FLYTEL.

12) Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;

13) Os colaboradores não poderão usar os recursos da FLYTEL para deliberada ou inadvertidamente propagar qualquer tipo vírus, worms, cavalos de troia, spam;

14) Não serão permitidos os acessos a softwares peer-to-peer (Kazaa, BitTorrent, µtorrent e afins);

15) Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: mega, uploaded, bitshare, depositfiles, etc;

16) Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de bypass de firewall;

17) Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando o setor responsável deverá estar devidamente ciente e concedido autorização para tal;

18) Os arquivos inerentes a FLYTEL, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;

19) Não será permitida a alteração das configurações de rede, inicialização das máquinas ou modificações que possam trazer algum problema futuro quanto a segurança das informações;

20) Haverá geração de relatórios de sites e downloads acessados por usuário.

6. POLÍTICA DE SENHAS

A forma mais convencional de identificação e acesso do usuário é através da utilização de senha. É um recurso pessoal e intransferível que protege a identidade do colaborador, evitando que uma pessoa se faça passar por outra.
O uso de dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).
Assim, com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:
1) A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo ser imediatamente alterada no caso de suspeita de sua divulgação;

2) É proibido o compartilhamento de login para funções de administração de sistemas;

3) As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);

4) O acesso do usuário deverá ser imediatamente cancelado ou modificado nas seguintes situações: desligamento do colaborador, mudança de função do colaborador e quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.

7- POLÍTICA DE E-MAIL

O e-mail é uma das principais formas de comunicação. No entanto, é, também, uma das principais vias de disseminação de malwares, por isso, surge a necessidade de normatização da utilização deste recurso.

1) O e-mail corporativo é destinado a fins profissionais, relacionados às atividades dos colaboradores;

2) Os e-mails enviados ou recebidos de endereços externos serão monitorados com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação da FLYTEL;

3) É proibido enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo "corrente", campanhas ou promoções etc.;

4) É necessário cuidado ao abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;

5) É proibido enviar qualquer mensagem por meios eletrônicos que torne a FLYTEL vulnerável a ações civis ou criminais;

6) É proibido falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

7) É proibido produzir, transmitir ou divulgar mensagem que:

- Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Vise burlar qualquer sistema de segurança;
- Vise vigiar secretamente ou assediar outro usuário;
- Vise acessar informações confidenciais sem explícita autorização do proprietário;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal;
- Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

8) O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:

- Não contrariar as normas aqui estabelecidas;
- Não interferir, negativamente, nas atividades profissionais individuais ou de outros colaboradores;
- Não interferir, negativamente, na FLYTEL e na sua imagem.

8- POLÍTICA DE USO DAS ESTAÇÕES DE TRABALHO

As estações de trabalho devem permanecer operáveis durante o maior tempo possível para que os colaboradores não tenham suas atividades prejudicadas. Assim, algumas medidas de segurança devem ser tomadas, são elas:

- É de responsabilidade do colaborador do equipamento zelar pelo mesmo, mantendo-o em boas condições;
- Não é permitido personalizar o equipamento por adesivos, fotos, riscos, raspar ou retirar a etiqueta de patrimônio;
- É vedada a abertura de computadores para qualquer tipo de reparo pelos colaboradores, somente possível quando previamente autorizado;
- As estações de trabalho só estarão acessíveis aos colaboradores através de contas de usuário limitadas.
- É proibida a instalação de softwares ou sistemas nas estações de trabalho pelos usuários finais sem autorização;
- Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
- Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;
- É proibido o uso de estações de trabalho para:
  -Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
  -Burlar quaisquer sistemas de segurança;

-Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;

-Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;

- As estações de trabalho possuem códigos internos, os quais permitem que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.
- Quanto ao USO DE IMPRESSORAS é proibida a impressão ou cópia de documentos de cunho ilegal; O chefe de cada setor / unidade será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões/cópias excessivas;

9.POLÍTICA SOCIAL

Nós, seres humanos, somos seres sociáveis, quando tratamos de segurança, isso muitas vezes pode ter uma desvantagem. Para tanto observe as seguintes orientações:

a) Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos;
b) Não divulgue sua senha com terceiros;
c) Relate aos seus superiores qualquer suspeita de tentativa que violação à segurança da informação.

10. SEGURANÇA DO AMBIENTE DE TI

Na política de segurança da Informação estabelecida pela FLYTEL, define-se que os analistas de TI, mediante ciência do responsável pela Segurança da Informação, devem ser os únicos a terem permissão para ler/editar as informações, obedecendo as atribuições de sua área de atuação.

Somente os colaboradores credenciados e/ou autorizados pelo Gestor de Segurança da Informação podem ter acesso aos dados armazenados;

Os logs dos ativos de rede devem ser monitorados constantemente, afim de evitar acessos indevidos.

11. VÍRUS E CÓDIGOS MALICIOSOS

Mantenha o seu antivírus atualizado. Caso você perceba a necessidade de atualização e tenha alguma dificuldade acione o gestor de segurança da informação.

Não introduza nas máquinas da empresa nenhum pen drive, HD, CD/DVD, etc. não autorizados;

Qualquer suspeita de vírus ou invasão o gestor de segurança da informação deve ser comunicado, através dos dados abaixo:

GESTOR DA SEGURANÇA DA INFORMAÇÃO

NOME	E-MAIL	RAMAL	CELULAR
PAULO HENRIQUE	**phenrique@flytel.com**	**30**	**(11) 99933-8267**

12. VIOLAÇÃO DA POLÍTICA E PENALIDADES

No caso de não cumprimento das normas estabelecidas nesta Política de Segurança, o funcionário ou colaborador poderá sofrer as seguintes penalidades:

- Advertência verbal

O colaborador será comunicado verbalmente que está infringindo as normas da Política de Segurança da Informação da FLYTEL e será recomendado à releitura desta Norma;

- Advertência formal

A primeira notificação será enviada ao colaborador informando o descumprimento da norma, com a indicação precisa da violação cometida.

A segunda notificação será encaminhada para os superiores.

CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação deverão ser encaminhadas aos Gestores para avaliação e decisão.

Esta PSI entra em vigor a partir desta data e pode ser alterada a qualquer tempo, por decisão dos Gestores, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento. Ficando os gestores responsáveis pela divulgação e fácil acesso quanto conteúdo alterado e/ou acrescido.

São Paulo, 07 dezembro de 2020.