Sumário

1.0. OBJETIVO

Prover e estabelecer a orientação e apoio para a gestão de segurança da informação de acordo com as leis e regulamentações normativas alinhadas ao negócio da Fast Solutions.

2.0. ABRANGÊNCIA

Todos os colaboradores que utilizam serviços e recursos tecnológicos disponibilizados e de propriedade da Fast Solutions, incluindo terceiros, parceiros de negócios e prestadores.

3.0. CONSIDERAÇÕES PRELIMINARES

- Segurança da Informação trata-se da preservação da confidencialidade, disponibilidade, integridade e legalidade da informação.
- Política de segurança da informação é um documento de diretrizes apoiado por manuais e procedimentos, visando garantir a Segurança da Informação da empresa junto à conformidade a PCI* e ISO/IEC 27001*.

4.0. PROPRIEDADE E PROTEÇÃO DA INFORMAÇÃO

Toda a informação gerada, adquirida ou custodiada pela Fast Solutions, independente da forma de apresentação ou armazenamento, é importante ativo da empresa e deve ser adequadamente protegida.
As informações devem ser utilizadas exclusivamente para fins relacionados aos interesses da Fast Solutions, observando as orientações contidas nas diretrizes organizacionais e desta Política de Segurança da Informação, sendo facultado à Fast Solutions monitorar a qualquer momento, o tráfego e armazenamento de dados sem prévia notificação aos colaboradores, prestadores de serviço e demais usuários autorizados conforme descritos no terno de compromisso, sigilo e anuência.

5.0. PAPÉIS E RESPONSABILIDADE.

5.1. Comitê de Segurança da Informação.

As responsabilidades do Comitê de Segurança da Informação incluem, mas não se limitam a:

- Estabelecer diretrizes e aprovar as políticas e procedimentos relacionados à Segurança da Informação;
- Designar, definir ou alterar as atribuições da estrutura de Segurança da Informação;
- Garantir que a segurança seja parte do processo de planejamento;
- Aprovar e suportar as principais iniciativas de Segurança da Informação para melhoria contínua das medidas de proteção visando minimizar os riscos identificados;

- Direcionar os esforços e recursos propostos pela área de Segurança da Informação conforme a estratégia de negócios e de Tecnologia da Informação (TI);
- Acompanhar indicadores de segurança e incidentes reportados pela área de Segurança da Informação, e;
- Atuar como fórum de discussão e tratar outros aspectos de segurança não contemplados pela Política de Segurança da Informação.

5.2. Security Officer.

São atribuições do Security Officer atividades gerenciais como:

- Planejar e participar das atividades do Comitê de Segurança da Informação intermediando as interações com entidades internas ou externas em assuntos relacionados à Segurança da Informação;
- Definir as principais funções e responsabilidades quanto à segurança da informação de todos os departamentos da companhia;
- Planejar a Segurança da Informação;
- Organizar recursos, atividades e responsabilidades;
- Integrar e monitorar objetivos de acordo com metas estabelecidas, e;
- Aferir e controlar o custo-benefício dos resultados alcançados, dando visibilidade destes resultados ao Comitê de Segurança da Informação.

5.3. Equipe de Segurança da Informação.

Cabe à Equipe de Segurança da Informação, formada por especialistas com a devida capacitação técnica, a responsabilidade de atuar de forma proativa nas questões de segurança para toda a organização.
Algumas das atividades da área de Segurança da Informação incluem, mas não se limitam a:

- Monitorar as violações de segurança e tomar ações corretivas para assegurar que não haja recorrência;
  • Orientar testes da infraestrutura de tecnologia e de sistemas para avaliar pontos fracos e detectar possíveis vulnerabilidades e ameaças;
- Revisar, publicar, zelar e manter as políticas e procedimentos relacionados à Segurança da Informação e sugerir as alterações necessárias;
- Orientar o desenvolvimento, a implantação e o teste dos controles técnicos e processuais de segurança da informação necessários para garantir a segurança do ambiente de tecnologia;
- Desenvolver, manter e implantar em parceria com a área de Treinamento e Desenvolvimento, programas de treinamento e conscientização aos colaboradores, prestadores de serviços e demais usuários autorizados sobre a política de segurança da informação, a forma como ela está estruturada e os conceitos necessários;
- Assessorar as demais áreas da companhia no processo de classificação da informação;
- Implantar programas regulares de avaliação de riscos nas áreas de negócio, auxiliando os responsáveis destas, sempre que necessário;
- Auxiliar as áreas de negócio na elaboração do Plano de Continuidade e Disponibilidade do Negócio; • Fornecer orientação aos recursos envolvidos para a tomada de ações rápidas caso sejam detectados e/ou alertados para incidentes de segurança da informação e;
- Auxiliar áreas de desenvolvimento de sistemas durante fase de planejamento a fim de que estes contenham controles de segurança.

5.4. Gestores.

Colaboradores que, devido a sua posição na organização, são responsáveis por garantir o cumprimento desta política para funcionários sob sua gerência ou prestadores de serviço vinculados a contratos sob sua gestão. Devido a sua responsabilidade, fica atrelado ao gestor, estabelecer a forma de atuação do colaborador ou prestador de serviço, bem como seu acompanhando e verificação da realização do seu(s) trabalho(s) e quando necessário atuar, colaborar, orientar e identificar junto com a equipe de Segurança da Informação nos casos de auditoria do trabalho(s) realizados(s).

5.5. Administração de Pessoal.

É de responsabilidade do setor de Administração de Pessoal (Recursos Humanos), a seleção, contratação (baseada nos requisitos de capacitação profissional, habilidade e no perfil do cargo exigido), acompanhamento do exercício da função ou atividade exercida, os controles necessários para o acesso às dependências da empresa durante a vigência do vinculo de trabalho, bem como os bloqueios necessários no caso de doença, férias, afastamento, desligamento, etc., do colaborador. Cabe ao setor, cuidar da sistemática envolvendo o treinamento interno dos colaboradores, bem como as reavaliações destes, quando necessário, elaborar planos e procedimentos para uso dos colaboradores nas dependências da empresa, a Saúde e Segurança Ocupacional.

5.6. Colaboradores, Prestadores de Serviço e demais usuários autorizados.

Os colaboradores, prestadores de serviço e demais usuários autorizados a usar informações da companhia, configuram-se em importante elo da Segurança da Informação. Com base em suas atividades fornecem subsídios para os agentes de segurança da informação da Fast Solutions e devem estar comprometidos com o manuseio e utilização adequada das informações e recursos computacionais oferecidos pela empresa.

6.0. CLASSIFICAÇÃO DA INFORMAÇÃO.

As informações da Fast Solutions devem ser classificadas em uma das seguintes categorias: confidencial, restrita, interna e pública conforme definido na Política de Tratamento e Classificação da Informação. Todas as Informações, enquanto não devidamente classificadas e divulgadas de forma oficial, são consideradas reservadas. Com base na classificação atribuída, toda divulgação de informação deve ser controlada.
Os colaboradores, prestadores de serviço e demais usuários autorizados são responsáveis por garantir a segurança da informação sob a sua guarda, não lhes sendo permitido divulgá-las sem a prévia autorização.

6.1. Tratamento da Informação.

Aos colaboradores, prestadores de serviço e demais usuários, não é permitido realizar cópias para uso pessoal ou divulgação das informações da Fast Solutions. Toda informação deverá ter um proprietário ou responsável, e

a ele cabe à responsabilidade por autorizar acessos à informação, bem como classificá-la como confidencial, restrita, interna e pública.

Informações confidenciais e restritas não podem ser acessadas ou copiadas para mídias, e para ambientes externos (incluindo a Internet) sem a devida autorização.

Informações confidenciais só podem ser transmitidas ou armazenadas quando houver autorização do responsável pela informação conforme o procedimento de Uso de Criptografia.

As Informações devem ser manuseadas e armazenadas de forma segura e adequadamente descartadas quando não mais necessárias conforme o procedimento de Classificação e Tratamento de Informações.

No momento do descarte de qualquer informação, quando esta estiver em forma de papel, este(s) deve(m) ser levado(s) à trituradora e obedecidos os procedimentos documentados nas políticas internas do setor de controle de qualidade (normas ISO); o mesmo quando se referir aos dispositivos de rede como disco rígido (por exemplo, pelo motivo de reformatação de equipamento), estes deverão ter realizados os procedimentos (por exemplo, wipe disk, antes da instalação do novo sistema operacional) descritos no procedimento de Tratativa e Classificação de Segurança da Informação.

7.0. SEGURANÇA FÍSICA E DO AMBIENTE.

7.1. Acesso Físico.

Todo o acesso deve ser controlado. Cabem à Recursos Humanos o fornecimento e controle de crachá de colaboradores e prestadores de serviço. Cabe à portaria/segurança controlar o acesso de pessoas que circulam nas dependências da empresa, fornecendo aos visitantes o respectivo crachá que deve segregar o seu acesso às áreas específicas, de acordo com a função ou finalidade de sua presença.

É responsabilidade dos colaboradores e prestadores de serviço se identificar, quando solicitado, para a Segurança Patrimonial da Fast Solutions e zelar pela proteção de acesso às diversas áreas da empresa. Apenas colaboradores da Fast Solutions e prestadores de serviço autorizados podem permitir a entrada de visitantes, quando relevante para os interesses da Fast Solutions, sob sua responsabilidade e acompanhados durante toda a sua permanência.

O crachá deve ser portado, de forma sempre visível por todos que circulem nas dependências da Fast Solutions. Em caso de extravio de crachá deve-se comunicar imediatamente a área de Recursos Humanos.

O responsável pela Segurança Patrimonial da Fast Solutions deve ser informado sobre a presença de qualquer pessoa não identificada, não autorizada ou de qualquer visitante não acompanhado, considerando-se sempre as permissões de acesso específicas para as diversas dependências da Fast Solutions.

Não é permitida a utilização de equipamento de gravação ou de fotografia, sem autorização, em áreas com informações confidenciais ou em centro de processamento de informações.

Para o envio de qualquer item de informática, será necessário o preenchimento do respectivo documento de transferência de ativo denominado Guia de Transferência de Bem Patrimonial.

Atividades que possam afetar o funcionamento dos recursos de TI da Fast Solutions devem ser autorizadas e executadas com perícia, assim como manipular ou remover qualquer recurso da Fast Solutions. Deve-se consultar o procedimento de Controle de Acesso para maior detalhamento

A área de Recursos Humanos informará ao setor de TI da Fast Solutions uma relação de colaboradores e prestadores de serviço desligados da empresa para acompanhamento e controle de segurança.

Áreas que possuem informações sensíveis (CPD, Sala de Senhas, RH, Infraestrutura e Desenvolvimento) estão segregadas fisicamente dos demais locais, onde somente, a acompanhamento de funcionários que possuem este acesso, será permitida a entrada de visitantes em geral.
As entregas referentes aos insumos de fornecedores o acesso será apenas pela a portaria 02, onde e feito seu cadastro e liberado para a doca, porem o motorista não tem acesso as dependências da empresa.

8.0. ZELO DAS INFORMAÇÕES.

Informações confidenciais ou restritas não devem ser deixadas sobre a mesa de trabalho, dentro de gaveta ou armário sem chave. Cuidados semelhantes se aplicam ao material impresso deixado nos escaninhos/bandejas de impressoras.
É expressamente proibido que informações Confidenciais e/ou Restritas fiquem no diretório “Público” da rede Fast Solutions, mesmo que por breve período, o repositório será auditado pela segurança da informação a qualquer momento. Ao ausentar-se de sua estação, mesmo que por breve período, o colaborador deve protegêla de acessos com senha de acesso.

9.0. MESA LIMPA E TELA LIMPA

Não deve ser deixada sobre a mesa de trabalho, dentro de gaveta ou armário sem chave informação confidencial ou restrita. Cuidados semelhantes se aplicam ao material impresso e deixado nos escaninhos de impressoras da empresa.
Ao ausentar-se de sua estação de trabalho mesmo que por breve período, o usuário deve protegê-la de acessos indevidos com senha de acesso. As estações de trabalho devem estar configuradas para trancar a sessão do usuário depois de 3 minutos de ociosidade (Esta regra se aplica para os recursos locais e remotos).
Será efetuada pela segurança patrimonial da empresa, uma verificação regular (ronda), que acontecerá no mínimo de 15 em 15 dias.

10.0. COMPUTAÇÃO MÓVEL.

A utilização de computação móvel no ambiente de rede só será permitida para realizar atividades na Fast Solutions seguindo os requisitos de aprovação. Apenas colaboradores e prestadores de serviço, devidamente autorizados, poderão conectar computador móvel à rede da Fast Solutions.
A cópia de informações confidenciais para dispositivos móveis será restrita, devendo obedecer ao fluxo de autorização, e devendo ser permitida apenas quando estritamente necessária.
Cabe à área de TI implantar e divulgar mecanismos que maximizem a segurança dos equipamentos.
Cabe ao colaborador zelar pelo equipamento sob sua guarda, devendo manuseá-lo atendendo exclusivamente aos interesses da empresa conforme descrito no procedimento Computação Móvel.

11.0. GERENCIAMENTO DO AMBIENTE COMPUTACIONAL.

11.1. Conexões de Rede.

A conexão de quaisquer equipamentos à rede interna da Fast Solutions somente deve ser realizada pelos representantes autorizados da TI e por eles conduzida. Somente colaboradores prestadores de serviço e parceiros de negócios, devidamente autorizados, podem ter acesso à rede da Fast Solutions.
Acessos remotos à rede da Fast Solutions, excetuando-se acessos a serviços públicos, devem ser autorizados, sendo estes apenas para atividades relevantes para o negócio da empresa e utilizando computador disponibilizado pela Fast Solutions e adequado aos requisitos de segurança.
É permitida a conexão de prestadores de serviço ou parceiros na rede da empresa, tanto no modo local quanto no modo remoto, desde que sejam garantidos os requisitos de segurança, conforme o procedimento de Acesso à rede, os quais são verificados e avalizados pela área de Segurança da Informação.
Computadores não pertencentes à Fast Solutions só podem ser conectados à rede da empresa quando autorizados pelo Gestor do contrato e pela TI, depois de executado procedimento de adequação às políticas e configurações de segurança. A Fast Solutions poderá auditar os equipamentos de prestadores de serviço ou parceiros para garantir a segurança de sua informação.
É proibido utilizar qualquer tipo de conexão remota (telefônica, cabo, rede wireless, etc.) nos equipamentos que estejam ao mesmo tempo conectados nas redes locais da empresa.

11.2. Senha.

A senha é pessoal e intransferível, devendo obedecer aos padrões divulgados no procedimento de Usuários e Senhas. É responsabilidade do usuário autorizado qualquer ação executada com o seu usuário/senha (login/password), constituindo-se grave violação da Política de Segurança da Informação, o compartilhamento dos mesmos. O usuário autorizado não deve armazenar senha em arquivos de computador e tampouco escrevêla em papéis ou outras mídias. Não poderá utilizar senhas “fracas” como as baseadas em nomes próprios ou dados pessoais tais como nome, data de nascimento, RG, CPF, etc.
Serão de responsabilidade da Equipe da Segurança da Informação, a segurança, manutenção e utilização quando necessário das senhas “dupla custódia” de todos os servidores.

11.3. Alterações de Configuração.

O colaborador, prestador de serviço ou usuário autorizado não pode realizar alterações nas configurações dos recursos computacionais Fast Solutions. Toda alteração deve ser conduzida pelos representantes autorizados de TI.

11.4. *Entrega/Devolução de Equipamento*

Ao conceder um equipamento (ex: desktop) para uso de um funcionário o mesmo devera preencher e assinar o “Termo de Recebimento” onde devera conter os dados de identificação do equipamento e os dados pessoais do funcionário.

No momento da devolução do equipamento um colaborador da equipe de TI verificara se o equipamento se encontra nas mesmas condições que foi disponibilizado, o "Termo de Devolução" devera ser preenchido e assinado.

11.5. Internet.

A Internet é uma ferramenta de trabalho, não sendo permitido seu uso para acesso a sites de conteúdos considerados impróprios ou fora dos padrões adotados pela empresa, ou seja, conteúdos que não estejam em conformidade com as normas legais, a moral, a integridade e os bons costumes, tais como os relativos à: pornografia, obscenidades, discriminação racial, política ou religiosa, e terrorismo, etc. Adicionalmente, a Fast Solutions proíbe acesso a sites que possibilitem jogos, salas de bate papo, cópias de músicas e filmes. Sendo, porém, permitido ao colaborador e demais usuários autorizados à utilização da Internet como um recurso pessoal, desde que não interfira na execução de suas atividades profissionais e em observância às normas da Política de Segurança da Informação, e estando-se ciente de que a Fast Solutions poderá monitorar o uso da internet identificando os usuários e as páginas visitadas a qualquer momento. Constitui-se grave violação da Política de Segurança da Informação tentar burlar as restrições de acesso à Internet.

11.6. Proteção Contra Software.

Todo computador conectado à rede da Fast Solutions, de forma local ou remota, deve ter obrigatoriamente instalado, atualizado e ativado software de proteção contra vírus homologado pela área de Segurança da Informação. Sua desativação é proibida a todos colaboradores, prestadores de serviço e demais usuários autorizados. Ao ter conhecimento de computador fora de conformidade com os padrões da empresa ou apresentando comportamento suspeito, cabe ao colaborador, prestador de serviço ou usuário autorizado comunicar ao Suporte através de abertura de chamado.

11.7. Cópias de Segurança.

Cabe aos representantes autorizados de TI realizarem regularmente o backup de informações mantidas nos servidores da companhia conforme o procedimento de Backup. Arquivos de conteúdo impróprio ou pessoal não devem ser armazenados nos servidores da companhia, independente de sua origem ou formatação. Nos drivers internos (C: e D: por exemplo) não devem ser armazenadas informações relevantes à companhia, e tampouco arquivos de conteúdo impróprio.

11.8. Uso do Correio Eletrônico.

O Correio Eletrônico é uma ferramenta de trabalho, não sendo permitido seu uso para a transmissão de mensagens ou arquivos de conteúdos considerados impróprios pela companhia, ou seja, conteúdos que não estejam em conformidade com as normas legais, a moral, a integridade e os bons costumes. Adicionalmente, a Fast Solutions proíbe mensagens contendo campanhas políticas, religiosas, vendas de produtos, "correntes", boatos, jogos, músicas, filmes. Não é permitido ao colaborador a utilização do correio eletrônico como um recurso pessoal, em observância às normas da Política de Segurança da Informação, e estando-se ciente de que os endereços de correio eletrônico oficiais da empresa ("@fastsolutions.com.br"), assim como as caixas postais

a eles associadas, são de propriedade da Fast Solutions que poderá monitorar seu uso a qualquer momento. Todas as mensagens para fora da empresa devem conter “assinatura”, elaborada em conformidade com os padrões estabelecidos no procedimento de Uso de Correio Eletrônico para maior detalhamento.

11.9. Uso de Criptografia.

Apenas é permitida a utilização de mecanismos de criptografia homologados e somente nos casos autorizados, conforme descrito no procedimento de Uso de Criptografia.

11.10. PENTEST.

Pode ser classificado como método de auditoria de segurança que o Administrador de Redes, Analista de Teste ou até mesmo Analista de Segurança, que são profissionais especializados em realizar Teste de Intrusão, simulam ataques com o intuito de mensurar o impacto da varredura caso seja bem-sucedido e seja descobertas falhas ou bug. Desta forma é possível descobrir o conjunto de vetores de ataques, vulnerabilidade de alto e baixo risco, identificarem os que podem ser difíceis ou impossíveis de detectar, os impactos operacionais, testar a capacidade defensiva da rede e identificar a reação do sistema aos ataques. Dentre vários motivos para realizar um ataque a um software, se destaca as invasões por questões financeiras, pessoais, cometer fraudes, sabotagem ou espionagem. O invasor é uma pessoa com alto nível de conhecimento técnico, seus ataques são minuciosamente planejados, é importante que haja o estudo do comportamento do alvo, assim ira descobri uma brecha na segurança dando início ao seu objetivo depois de passar por várias etapas ou fases.
A FAST se compromete a realizar PENTEST uma vez ao ano, sempre através de empresa externa altamente qualificada, a fim de localizar possíveis falhas de segurança e resolvê-las reduzindo assim ao máximo os possíveis ataques à rede produtiva da FAST.

11.11. Serviço NTP

Todos os computadores do ambiente Fast tem seu horário controlado pelo servidor NTP da Fast, esta imposição e aplicada pela Diretiva de Grupo, “GPO”, garantindo o sincronismo de hora em todas as máquinas.

12.0. RECURSOS DE INFORMÁTICA.

12.1. Instalação e Configuração de Software e Hardware.

Em recursos computacionais de propriedade da Fast Solutions somente é permitida a utilização de software ou hardware homologado, licenciado e controlado pela TI. É restrito apenas para os representantes autorizados da TI, a instalação e configuração de software ou hardware em qualquer recurso computacional de propriedade da Fast Solutions.
Recursos computacionais custodiados (alugados, etc.) devem ser homologados pela TI e, apenas seus representantes autorizados podem instalar e configurar software e hardware. Aos prestadores de serviço o suporte atenderá somente recursos computacionais Fast Solutions.
Todos os computadores da rede, laptops, notebooks e demais equipamentos móveis, devem ter seu aceso controlado de acordo com o perfil do usuário conforme descrito no Manual de Acesso à Rede. Esses respectivos

equipamentos devem ter instalado um Firewall pessoal, sem permissão de controle pelo usuário e não devem possuir habilitados gravadores de CD/DVD, interfaces USB (de nenhum tipo) e tampouco drives de disquete.

12.2. Movimentação de Recursos de Informática.

Somente representantes autorizados da TI podem movimentar recursos computacionais de propriedade da Fast Solutions. Sendo permitido, adicionalmente, que usuários movimentem computadores móveis sob sua guarda.

12.3. Notificação de Mau Funcionamento de Software ou Hardware.

Qualquer mau funcionamento de recurso computacional Fast Solutions, software ou hardware, deve ser imediatamente notificado ao Suporte.

13.0. CONTROLE DE ACESSO LÓGICO.

O colaborador, prestador de serviço e demais usuários autorizados devem ter acesso somente às informações e recursos que forem necessários para a realização de suas atividades devendo ser respeitada a segregação de funções. Constitui-se grave violação da Política de Segurança da Informação tentar acessar qualquer serviço de TI ou informação sem a devida autorização, tentar burlar as restrições de segurança, tentar prejudicar serviço de informação, interceptar comunicação de forma não autorizada ou utilizar os recursos de TI da Fast Solutions para atividade maliciosa.

Todo sistema deve possuir controle de acesso de modo a assegurar o uso apenas por usuário autorizado, e sistemas críticos devem permitir o registro de trilhas de auditoria (logs) que possibilitem o monitoramento das atividades executadas.

As movimentações de pessoal (admissão, transferência, promoção, demissão) devem ser comunicadas pela Administração de Pessoal, de forma imediata, para a área de TI, que providenciará as atualizações necessárias no ambiente computacional. Cabe ao gestor de colaborador garantir que a Administração de Pessoal tenha conhecimento destas movimentações. Cabe aos gestores de contratos com fornecedores, ou seus representantes designados, solicitar permissões, renovações e cancelamento de acessos aos prestadores de serviço decorrentes destes contratos. Não ocorrendo renovação o acesso destes usuários será bloqueado. Em caso de desligamento, o acesso é bloqueado e os dados armazenados no correio eletrônico e servidor de arquivos serão excluídos após 45 dias, durante este período o gestor pode solicitar acesso a estes dados.

As permissões de acesso (login ou conta), concedidas e implantadas pela área de TI, são únicas e intransferíveis. É de responsabilidade do usuário qualquer ação executada através de sua conta de acesso.

14.0. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE APLICATIVOS.

Toda aquisição, desenvolvimento ou manutenção de aplicativos voltados a suportar processos de negócio é de competência exclusiva da área de TI, que encaminhará a solução.

15.0. PLANO DE CONTINUIDADE OPERACIONAL.

Cabe à área de Segurança da Informação, apoiado pela área de TI, coordenar a elaboração, atualização e testes periódicos de Plano de Continuidade para os recursos computacionais de TI da organização.

16.0. CONFORMIDADE.

A Fast Solutions, seus colaboradores, prestadores de serviço e demais usuários autorizados devem submeter-se não somente às Diretrizes Organizacionais e à Política de Segurança da Informação, mas também a qualquer lei, estatuto, regulamento ou contrato a qual esteja sujeita a organização.
Devem ser disponibilizados recursos e informações que permitam a realização periódica de auditorias.
Os contratos efetuados pela Fast como contratante ou contratada, deve sempre constar uma cláusula de confidencialidade das informações. Para os casos de parceiros de negócios, deve-se sempre atentar para a conformidade da PCI aplicada nos mesmos. Ou seja, a conformidade a PCI, deve ser recíproca.

17.0. VIOLAÇÃO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO.

A violação a esta política, esta sujeita às sanções disciplinares, passíveis de punições conforme abaixo descritas, e em conformidade com a legislação trabalhista e a gravidade da infração.
Ao identificar ou suspeitar de possível violação da Política de Segurança da Informação, deve-se buscar orientação com o Gestor da área, que, juntamente com a Equipe de Segurança da Informação, apurará os fatos.
Os colaboradores, prestadores de serviço e demais usuários autorizados devem notificar imediatamente para o Gestor da área e para a área de Segurança da Informação, quaisquer fragilidades, ameaças ou incidentes ocorridos ou suspeitos, na segurança de sistemas, em controles ou serviços. Não é permitido, sob nenhuma circunstância, tentar averiguar uma falha de segurança ou uma atividade suspeita, pois a investigação de uma fragilidade pode ser interpretada como uso impróprio do sistema ou da informação, estando tais averiguações restritas à Equipe de Segurança. (security@fastsolutions.com.br).

Infração:

Leve: Aviso para o colaborador com cópia para o gestor, não sendo a falta registrada na pasta funcional do mesmo.
Média: Advertência escrita pelo gestor imediato e a ocorrência registrada na pasta funcional do colaborador.
Grave: Advertência escrita pelo gestor imediato e a ocorrência registrada na pasta funcional do colaborador. Falta passível de ações mediante a análise da empresa.

Em caso de reincidência, a infração deve ser considerada no próximo grau de escala. Ex: Duas faltas leves referentes à mesma matéria constituem falta média.

18.0. GERENCIAMENTO DE MUDANÇAS

O Gerenciamento da mudança é fundamental no ambiente, onde toda a mudança deve ser controlada, mitigando riscos e garantindo a disponibilidade de serviços, entrega de resultados aos clientes e a continuidade do negocio no ambiente produtivo, sendo assim e quando aplicável toda alteração ou mudança que possa interferir no ambiente físico ou computacional será motivo de estudo prévio no processo de gerenciamento de mudanças - GMUD.
No caso que envolve a utilização de programas para o processamento de arquivos do(s) cliente(s), o setor de desenvolvimento, possuiu os formulários e processos específicos.

19.0. ATUALIZAÇÃO DA POLÍTICA

A atualização da política e controlada pelas informações contidas no cabeçalho e rodapé da mesma.
A política de segurança da informação e suas respectivas normas são revistas pelo menos “1” (uma) vez ao ano e eventualmente de acordo com a necessidade de mudança.

20.0. HISTÓRICO DE ATUALIZAÇÃO

Data	Versão	Descrição	Responsável
03/04/2008	01	Política de segurança.	Edson Geryn
18/07/2011	02	Política de segurança.	Tabajara Chelli Ferracini
30/08/2011	03	Gerenciamento de Mudanças	Tabajara Chelli Ferracini
10/07/2012	04	Atualização da Política	Tabajara Chelli Ferracini
14/11/2012	05	Atualização da Política	Tabajara Chelli Ferracini
01/02/2013	06	Atualização da Política	Tabajara Chelli Ferracini
24/11/2014	07	Revisão Anual	Tiago Cunha

22/12/2015	07	Revisão Anual	Tiago Cunha
21/08/2016	08	Atualização da Política	Tiago Cunha
15/06/2017	09	Atualização da Política	Tiago Cunha
04/06/2018	10	Atualização da Política	Tiago Cunha
04/06/2019	11	Atualização da Política	Tiago Cunha
20/09/2019	12	Revisão geral procedimento e alteração do logo	Michel Aquino
23/01/2020	13	Inclusão do formulário devolução (recebimento/	Michel Aquino
15/02/2021	14	Revisão Anual	Michel Aquino
14/02/2022	15	Revisão Anual	Álvaro Rodrigues
02/08/2023	16	Revisão anual	Thiago Costa