CIBERSEGURANÇA

Santa Fé
INVESTIMENTOS

Versão – Dezembro/2020

CONTROLE DE VERSÃO

Versão	Data	Razões para alteração	Origem
1.0	Jun/17	Elaboração documento. Versão Inicial	\Políticas e Formulário de Referência\Base\Arquivo de Versões\2017
1.1	Dez/18	Inclusão Cibersegurança e adaptação ao novo cód. ART – Artigo 16 e Artigo 13 § único	\Políticas e Formulário de Referência\Base\Atual\
1.2	Dez/19	Revisão anual, alteração de layout e armazenamento	G:\Fundos\Compliance\Manuais\Políticas e Formulário de Referência\Base\Atual
1.3	Dez/20	Revisão, alteração de layout	G:\Fundos\Compliance\Manuais\Políticas e Formulário de Referência\Base\Atual

Sumário

1 – Objetivo

A Política de Segurança da Informação é uma declaração formal da SANTA FÉ acerca da aderência a LGPD em vigor no Brasil e de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade da informação necessária para realização do negócio, devendo ser cumprida por todos os seus funcionários e.

Gerir todo o processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

2 – Segurança da Informação

Todo e qualquer usuário de recursos computadorizados da empresa tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática.

A violação desta política de segurança é qualquer ato que:

- Exponha a empresa a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados /ou de informações ou ainda da perda de equipamento.
- Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.
- Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

Toda e qualquer informação que são consideradas confidenciais e/ou sensíveis da SANTA FÉ ou de clientes, serão armazenadas em diretórios de rede com acesso restrito, e controlado pela equipe de Riscos e Compliance.

Toda e qualquer medida têm por finalidade minimizar os riscos, ameaças tecnológicas, à imagem e aos negócios da empresa.

3 – Missão da Tecnologia da Informação

- Criar e gerenciar regras de acesso para os usuários da rede interna, permitindo ou negando acesso conforme o setor/usuário.
- Manter, gerir, solucionar as ocorrências e registrar cada uma no Livro de Ocorrências.
- Impedir que o usuário compartilhe pastas de sua estação de trabalho com outras estações.
- Proibir o acesso remoto ou qualquer outro meio que coloquem em risco a integridade dos dados e da segurança.

4 – É dever de todos da Santa Fé

Considerar a informação como sendo um bem da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para a empresa e deve sempre ser tratada profissionalmente.

Não circularem informações consideradas confidenciais e/ou restritas, como também não deixar relatórios nas impressoras ou em locais de fácil acesso, tendo sempre em mente o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum relatório confidencial e/ou restrito sobre suas mesas.

O Colaborador que estiver na posse e guarda da cópia ou da impressão do arquivo que contenha informação confidencial será o responsável direto por sua boa conservação, integridade e manutenção de sua confidencialidade.

5 – Programas Ilegais

É terminantemente proibido o uso de programas ilegais (PIRATAS) na SANTA FÉ. Os usuários não podem, em hipótese alguma, instalar este tipo de "software" (programa) nos equipamentos da empresa.

Periodicamente, o Setor de T.I. fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

6 – Permissões e Senhas

Quando da necessidade de cadastramento de um novo usuário para utilização da "rede", sistemas, e-mail ou equipamentos de informática da SANTA FÉ, o setor de origem do novo usuário deverá comunicar esta

necessidade ao setor de T.I., por meio e-mail, informando nome completo, nome de usuário e relação contendo as permissões que serão atribuídas ao usuário. O Setor de T.I. fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada no próximo acesso.

Por segurança, o Setor de T.I. recomenda que as senhas tenham sempre um mínimo de 8 (oito) caracteres combinando entre letras maíusculas e mínusculas, caracteres especiais e números.

7 – Cópia de segurança (BACKUP)

Cópias de segurança dos dados dos servidores serão de responsabilidade do Setor de T.I. e devem ser feitas diariamente.

O gerenciamento do(s) banco(s) de dados é responsabilidade exclusiva do Setor de T.I., assim como a manutenção, alteração e atualização de equipamentos e programas.

9 – Cópias de Segurança e Arquivos Individuais

É responsabilidade dos próprios usuários a elaboração de cópias de segurança ("backups") de textos, planilhas, mensagens eletrônicas e outros arquivos ou documentos, desenvolvidos pelos funcionários, em suas estações de trabalho, e que não sejam considerados de fundamental importância para a continuidade dos negócios da SANTA FÉ.

No caso das informações consideradas de fundamental importância para a continuidade dos negócios da SANTA FÉ o Setor de T.I. disponibilizará um espaço nos servidores onde cada usuário deverá manter estas informações conforme o setor e seu conteúdo.

10 – Propriedade Intelectual

É de propriedade da SANTA FÉ, todos os “designs”, criações ou procedimentos desenvolvidos por qualquer funcionário durante o curso de seu vínculo empregatício com a SANTA FÉ.

11 – Uso do Ambiente WEB (Internet)

O acesso à Internet está autorizado para todos usuários que necessitarem da mesma para o desempenho das suas atividades profissionais, sites que não contenham informações que agreguem conhecimento profissional e/ou para o negócio não devem ser acessados.

O uso da Internet será monitorado pelo Setor de T.I., inclusive através de “logs” (arquivos gerados no servidor) que informam qual usuário está conectado, o tempo que usou a Internet e qual página acessou.

Não é permitido instalar programas provenientes da Internet nos microcomputadores da SANTA FÉ, sem expressa anuência do Setor de T.I., exceto os programas oferecidos por órgãos públicos federais, estaduais e/ou municipais.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

Quando navegando na Internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- De estações de rádio;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a determinadas classes;
- Que promovam a participação em salas de discussão de assuntos não relacionados aos negócios;
- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais.

É disponibilizado aos visitantes uma rede Wi-Fi com senha e de acesso publico segregada da rede de trabalho da SANTA FÉ, a mesma não se responsabiliza por eventuais problemas em sua utilização.

12 – Uso do Correio Eletrônico – ("e-mail")

O correio eletrônico fornecido pela SANTA FÉ é um instrumento de comunicação interna e externa para a realização do negócio da SANTA FÉ.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao Setor de T.I., que providenciará a inclusão do mesmo.

Não será permitido o uso de e-mail gratuitos (liberados em alguns sites), nos computadores da SANTA FÉ. O Setor de T.I. poderá, visando evitar a entrada de vírus na SANTA FÉ, bloquear o recebimento de e-mails provenientes destes sites gratuitos.

13 – Necessidades de Novos Sistemas, Aplicativos e/ou Equipamentos

O Setor de T.I. é responsável pela aplicação da Política da SANTA FÉ em relação a definição de compra e substituição de “software” e “hardware”.

Qualquer necessidade de novos programas ("softwares") ou de novos equipamentos de informática (hardware) deverá ser discutida com o responsável pelo Setor de T.I..

Não é permitido a compra ou o desenvolvimento de "softwares" ou "hardwares" diretamente pelos usuários.

14 – Uso de Computadores Pessoais (Notebook) ou de Propriedade da SANTA FÉ

Os usuários que tiverem direito ao uso de computadores pessoais (laptop ou notebook), ou qualquer outro

equipamento computacional, de propriedade da SANTA FÉ, devem estar cientes de que:

- Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais;
- A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário;
- É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo;
- O usuário não deve alterar a configuração do equipamento recebido.

Alguns cuidados que devem ser observados:

Fora do trabalho:

- Mantenha o equipamento sempre com você;
- Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
- Quando transportar o equipamento em automóvel utilize sempre o porta malas ou lugar não visível;
- Atenção ao transportar o equipamento na rua.

Em caso de furto

- Registre a ocorrência em uma delegacia de polícia;
- Comunique ao seu superior imediato e ao Setor de T.I.;
- Envie uma cópia da ocorrência para o Setor de T.I..

15 – Responsabilidades dos Gerentes / Supervisores

Os gerentes e supervisores são responsáveis pelas definições dos direitos de acesso de seus funcionários aos

sistemas e informações da empresa, cabendo a eles verificarem se os mesmos estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, e mantendo cópias de segurança de seus arquivos individuais, conforme estabelecido nesta política.

O Setor de T.I. fará auditorias periódicas do acesso dos usuários às informações, verificando:

- Que tipo de informação o usuário pode acessar;
- Quem está autorizado a acessar determinada rotina e/ou informação;
- Quem acessou determinada rotina e informação;
- Quem tentou acessar qualquer rotina ou informação sem estar autorizado.

16 – Uso de Anti-Vírus

Todo arquivo recebido / obtido através do ambiente Internet deve ser verificado por programa antivírus.

Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática, agendada pelo Setor de T.I., via rede.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

17 – Testes Periódicos

Ao menos uma vez por mês serão realizados os seguintes testes no ambiente de TI, divididos semanalmente e conforme gráu de risco, registrando os períodos no Relatório de Rotina Preventiva e registrando ocorrências no Livro de Ocorrências quando necessário :

- Hardware – Verificar fonte, aquecimento e funcionamento;
- Sistemas – Analisar logs, verificar e instalar atualizações, testar e verificar backup e restauração, avaliar atualizações de anti-virus;
    a- Firewall
    b- Servidores de Dados
    c- Servidores de Anti Vírus
    d- Servidor de Backup

18 – Controle de Acesso ao CPD

O acesso ao CPD é restrito e controlado por chave, uma cópia de segurança fica com o diretor de compliance e a outra com o responsável pelo TI.

19 – Penalidades

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nasseguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou.

20 – Vigência e Atualização

Esta Politica será revisada anualmente e alterada a qualquer tempo caso seja constatada necessidade de atualização de conteúdo.