Sumário

1. Introdução

A Tecnologia da Informação, TI, está cada dia mais presente nas empresas, mudando radicalmente os hábitos e a maneira de comunicação, sendo de vital importância a definição de normas de segurança que visem disciplinar o uso da tecnologia da informação.

A SF3 baseada na norma NBR ISO/IEC 27.002 e na Lei Geral de Proteção de Dados (Lei 13.709/2018) definiu sua Política de Segurança da Informação - PSI.

2. Objetivo

Definir responsabilidades e orientar a conduta dos usuários de TI, visando a continuidade dos negócios através da confidencialidade, da integridade e da disponibilidade das informações da SF3

3. Aplicação

Esta PSI aplica-se a todos os usuários de TI e a qualquer colaborador ou pessoa custodiante de informações da SF3 ou de seus clientes.

4. Princípios

A informação produzida ou recebida como resultado de sua atividade profissional pertence à SF3.

Divulgar informações confidenciais ou estratégicas é crime previsto nas leis de propriedade intelectual, industrial (Lei nº 9279) e de direitos autorais (Lei nº 9610).

A segurança da informação depende de pessoas comprometidas, processos gerenciais de controle e sistemas de segurança da informação.

5. Usuários de Informática

São reconhecidos como usuários da infraestrutura de TI todos os colaboradores, profissionais autônomos, temporários ou de empresas prestadoras de serviço que obtiverem a aprovação por escrito do responsável hierárquico e da gestão de liberações da área de TI, para prescrição de senhas de acesso aos recursos computacionais.

6. Responsabilidades

A SF3 entende que o sistema de segurança da informação somente será eficaz com o

comprometimento de TODOS!

7. É responsabilidade dos Usuários

- Respeitar esta Política de Segurança da Informação
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- Responder pelo uso exclusivo e intransferível de suas senhas de acesso;
- Ativar suas senhas de proteção para Correio Eletrônico e Sistema Operacional, sob orientação do Gestor de Liberações da área de TI;
- Buscar conhecimento necessário para a correta utilização dos recursos de hardware e software.
- Relatar prontamente à área de TI qualquer fato ou ameaça à segurança dos recursos, como quebra da segurança, fragilidade, mau funcionamento, presença de vírus, etc;
- Assegurar que as informações e dados de propriedade da SF3 não sejam disponibilizados a terceiros, a não ser com autorização por escrito do responsável hierárquico.
- Relatar para o seu responsável hierárquico e à Gerência de TI, o surgimento da necessidade de um novo software para suas atividades.
- Responder pelo prejuízo ou dano que vier a provocar a SF3 ou a terceiros, em decorrência da não obediência as diretrizes e normas aqui referidas.

8. Dos Responsáveis Hierárquicos

- Apoiar e zelar pelo cumprimento desta PSI, servindo como modelo de conduta para os colaboradores sob a sua gestão.
- Atribuir na fase de contratação e de formalização dos contratos individuais de trabalho CLT, prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI.
- Autorizar o acesso e definir o perfil do usuário junto ao gestor de liberações da área de TI,
- Autorizar as mudanças no perfil do usuário junto ao gestor de liberações da área de TI,
- Educar os usuários sobre os princípios e procedimentos de Segurança da Informação,

- Notificar imediatamente ao gestor de liberações da área de TI quaisquer vulnerabilidades e ameaças a quebra de segurança;

- Assegurar treinamento para o uso correto dos recursos computacionais e sistemas de informação;

- Advertir formalmente o usuário e aplicar sanções cabíveis quando este violar os princípios ou procedimentos de segurança, relatando imediatamente o fato ao gestor de liberações da área de TI.

- Obter aprovação técnica do gestor de liberações da área de TI antes de solicitar a compra de hardware, software ou serviços de informática.

- Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

9. Da Área de TI

- Configurar os equipamentos e sistemas para cumprir os requerimentos desta PSI,

- Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais.

- Restringir a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

- Garantir segurança do acesso público e manter evidências que permitam a rastreabilidade para auditoria ou investigação.

- Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes.

- Administrar, proteger e testar as cópias de segurança dos programas e dados ao negócio da SF3.

- Gerenciar o descarte de informações a pedido dos custodiantes,

- Garantir que as informações de um usuário sejam removidas antes do descarte ou mudança de usuário.

- Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

- Criar a identidade lógica dos colaboradores na empresa.

- Atribuir contas e senhas identificáveis a pessoa física para uso de computadores, sistemas, bases de dados e qualquer outro ativo de informação.

- Proteger todos os ativos de informação da empresa contra códigos maliciosos e ou vírus.

- Garantir que processos de mudança não permitam vulnerabilidades ou fragilidades no ambiente de produção.

- Definir as regras formais para instalação de software e hardware, exigindo o seu cumprimento dentro da empresa.

- Realizar inspeções periódicas de configurações técnicas e análise de riscos.

- Gerenciar o uso, manuseio e guarda de assinaturas e certificados digitais.

- Garantir assim que solicitado o bloqueio de acesso de usuários por motivo de desligamento da empresa,

- Propor as metodologias sistemas e processos específicos que visem aumentar a segurança da informação,

- Promover a conscientização dos colaboradores em relação a relevância da segurança da informação,

- Apoiar a avaliação e a adequação de controles de segurança da informação para novos sistemas ou serviços.

- Buscar alinhamento com as diretrizes corporativas da empresa.

- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

- Monitorar o ambiente de TI a capacidade instalada da rede e dos equipamentos, tempo de resposta no acesso à internet e aos sistemas críticos da SF3 indisponibilidade aos sistemas críticos, incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante); atividade de todos os colaboradores durante os acessos as redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

- Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior).

- Realizar, a qualquer tempo, inspeção física nas máquinas de propriedade da SF3.

10. Identificação – LOGIN E SENHA

- Os sistemas de Login e senha protegem a identidade do usuário, evitando e prevenindo que uma pessoa se faça passar por outra. Código Penal Brasileiro art. 307 – falsa identidade.

- Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade será dos usuários que dele se utilizarem. Se for identificada solicitação do gestor para uso compartilhado ele deverá ser responsabilizado.

- Os usuários deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo).

- É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel etc.), não devem ser baseadas em informações pessoais, como próprio nome, familiares, nascimento, endereço, placa de veículo, nome da empresa, e ou não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

- Os usuários devem proceder a troca de senha, caso suspeitem de quebra por terceiros.

- O Login e Senha devem ser imediatamente bloqueados quando se tornarem desnecessários.

- Tentativa de violação e burla de senhas de acesso, criptografia ou identificação biométrica se identificada será alvo de ação disciplinar.

- Os acessos externos à rede de informações da SF3 fora do expediente de trabalho serão bloqueados atendendo a Lei 12.551, teletrabalho que altera o Art. 6° da CLT, exceto para cargos de confiança.

11. Recurso Computacionais

- Os recursos de TI alocados pela SF3 aos seus usuários são destinados exclusivamente às atividades relacionadas ao trabalho.

- Quando o colaborador utilizar dispositivos de sua propriedade como ferramenta de trabalho na SF3 , seu uso será disciplinado por esta PSI.

- É proibida a intervenção do usuário para manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, bem como a transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros (pirataria).

- Todo computador em desuso, deverá ser encaminhado a área de TI para a remoção das informações, descarte ou reuso.

12. Tela Limpa e Mesa Limpa

- A partir desta data, o papel de parede e proteção de tela de todos os micros deverá seguir a padronização da SF3.

- O usuário deve cuidar para que papéis, mídias e imagens nos monitores não fiquem expostas ao acesso não autorizado.

- Os computadores deverão ser bloqueados por senha quando não estiverem sendo utilizados.

13. Descarte de Mídias

- Mídias contendo informações referentes a SF3 deverão ser destruídas antes de seu descarte.

- CD’s, DVD’s, e documentos em papel deverão ser PICOTADOS antes de serem encaminhadas ao lixo, HD’s deverão ser encaminhados a TI para a destruição da informação antes do descarte ou reutilização.

14. Classificação da Informação:

- O gestor de cada área deve estabelecer os critérios relativos ao nível de confidencialidade da informação gerada por sua área em Pública, Confidencial ou Interna.

15. Antivírus

A SF3 por intermédio do Gestor de Liberações da área de TI disponibiliza software corporativo de antivírus instalado para todos os usuários.

- O antivírus é atualizado automaticamente na estação de trabalho do usuário sempre que uma nova versão é disponibilizada pelo fabricante através do aplicativo servidor;

- A área de TI da SF3 não recomenda que o usuário remova ou altere as configurações do antivírus a fim de não comprometer a segurança que o fabricante do software proporciona.

- As checagens periódicas do disco rígido, HD, da estação de trabalho estão programadas para execução periódica automática conforme definições da área de TI no aplicativo servidor.

16. Armazenamento de Arquivos

- Todos os arquivos contidos nos servidores de rede ou nas estações de trabalho dos usuários devem ser exclusivamente de interesse da SF3.

- É proibida a criação de pastas pessoais nos servidores de rede.
- A criação de pastas departamentais nos servidores de rede deverá refletir a estrutura organizacional da SF3 e ser solicitada pelo responsável hierárquico ao gestor de liberações da área de TI.

- O acesso às pastas departamentais nos servidores de rede exige autorização do responsável hierárquico e do gestor de liberações para o controle do acesso de cada usuário.

- A partir da implantação desta Política, todos os arquivos que não sejam do interesse da

SF3 deverão ser excluídos dos equipamentos para evitar problemas futuros com as auditorias.

17. Salvaguarda de Arquivos

- Compete ao gestor de continuidade da área TI criar e manter cópias de segurança (backups) apenas dos dados armazenados nos servidores de rede;

- Os usuários devem manter obrigatoriamente os documentos, planilhas, e-mails, apresentações, desenhos, e outros dados críticos da SF3, nas pastas departamentais dos servidores de rede;

- É de responsabilidade exclusiva do usuário a cópia de segurança (backup) e a guarda dos dados gravados da sua estação local de trabalho.

18. Utilização da Internet

- A Internet foi instalada para viabilizar a busca de informações e agilizar determinados processos da SF3, sendo proibido o uso pessoal durante o horário de trabalho.

- O uso indevido do acesso à Internet é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado legalmente pelos danos causados.

- A auditoria dos acessos à Internet poderá levar ao conhecimento dos responsáveis hierárquicos, relatórios com nomes dos usuários, páginas consultadas, tempo de consulta, e o conteúdo navegado.

19. Jogos

- Jogos estão terminantemente proibidos.

20. Softwares Piratas

- Os softwares homologados e instalados nos computadores e servidores de rede são de propriedade exclusiva da SF3, sendo proibidas as cópias integrais, ou mesmo as parciais, bem como a instalação de softwares piratas.

- Pirataria é considerada crime e softwares piratas causam prejuízos tanto materiais como funcionais além de denegrir a imagem da Instituição. Por esta razão, estão terminantemente proibidos.

- A instalação de softwares não autorizados (Pirataria) constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/98, e o infrator está sujeito à pena de detenção e multa;

21. E-mail e Mensagens Instantâneas

- É proibido o uso de e-mails, correios eletrônicos ou mensagens instantâneas de forma contrária a lei, a moral, aos bons costumes, à ordem pública ou que infrinjam os direitos a propriedade intelectual ou industrial pertencente a terceiros.

- O conteúdo e a utilização de e-mails, correios eletrônicos ou mensagens instantâneas deve ser de caráter exclusivamente profissional.

- Os serviços de mensagens instantâneas são permitidos apenas para os usuários autorizados pela hierarquia da SF3 de acordo com a atividade exercida.

- A salvaguarda dos e-mails e conteúdo anexo é de responsabilidade exclusiva do usuário, ficando a SF3 isento de tal obrigação.

- O uso de software de e-mail, mensagens instantâneas e correio interno não homologado pela Gerência de Liberações são de responsabilidade do usuário e podem trazer riscos à segurança da informação além de dificultar o suporte técnico.

- Quaisquer comunicados em massa, propagandas, informativos, imagens etc., deverão ser previamente aprovados pelo gestor de capacidades da área de TI, a fim de não serem tratados como Spam ou comprometerem o funcionamento dos sistemas de e-mail.

- Mensagens recebidas de origem desconhecida deverão ser pré-visualizadas e eliminadas imediatamente, sem leitura de seu conteúdo, para evitar contaminação por vírus e outros riscos.

- O uso indevido do e-mail é de inteira responsabilidade do usuário, podendo o mesmo ser responsabilizado pelos danos causados.

- As mensagens trafegadas sob o domínio da SF3 poderão ser auditadas, mediante solicitação, conforme definição do TST, Tribunal Superior do Trabalho. Desta forma é proibida a utilização particular.

- Em nenhuma hipótese a SF3 será responsabilizada perante quaisquer usuários ou terceiros pela perda de mensagens e/ou respectivo conteúdo.

22. Auditorias

- Auditorias serão realizadas e relatórios serão gerados periodicamente.

- A Diretoria da SF3 poderá solicitar à Gerência de TI, relatórios de auditoria contendo o nome, mensagens trafegadas, acessos a Internet e demais informações do usuário conforme resolução do TST.

23. Disposições Finais

- Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna da SF3. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

- Todas as práticas que ameacem à segurança da informação serão tratadas com a aplicação de ações disciplinares, desde uma advertência verbal até rescisão contratual por justa causa, levando em consideração fatores como: função exercida pelo colaborador, período utilizado, local de utilização, horário de utilização, prejuízo real ou potencial causado a SF3, entre outros.