POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é o documento que reúne as diretrizes da empresa para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. São mandatórios o seu cumprimento e a sua aplicação por todos seus colaboradores. Esta política está baseada nas recomendações propostas de gestão da segurança da informação pela norma ABNT NBR ISO/IEC 27002:2013, assim como cumpre com os requisitos legais em território nacional.
É também responsabilidade de cada colaborador buscar orientação com seu gestor ou com o serviço de Tecnologia da Informação (TI) sempre que não estiver absolutamente seguro.

OBJETIVO

Esta política tem como fim estabelecer diretrizes que permitam aos colaboradores e clientes da Teknofil seguirem padrões de comportamento adequados, relacionados à segurança da informação, visando a proteção legal da empresa e do indivíduo, bem como, orientar a implementação de controles e processos para atingir seu propósito.

A Teknofil tem como objetivo preservar as informações quanto à:

- Integridade
- Confidencialidade
- Disponibilidade

PRINCÍPIOS

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional pertence à referida instituição. As exceções devem ser explícitas e formalizadas em contrato entre as partes.
Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.
Deverá constar em todos os contratos da TEKNOFIL, seja com colaboradores ou parceiros, o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.
Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos. Todos devem se comprometer assinando o Termo de Compromisso de Sigilo e Confidencialidade.
Todo incidente que afete a segurança da informação deverá ser comunicado imediatamente à Direção Executiva para análise.
Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

RESPONSABILIDADES

1 - Dos Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

O colaborador será responsabilizado por todo prejuízo ou dano que vier a sofrer ou causar à Teknofil e/ou a terceiros, em decorrência do descumprimento às diretrizes estabelecidas.

2 - Dos Gestores de Pessoas

Ser modelo de referência para os colaboradores sob a sua gestão.

Assegurar nos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento desta política, através da assinatura do Termo de Compromisso de Sigilo e Confidencialidade.

3 - Dos Custodiantes da Informação: Tecnologia da Informação/ Segurança da Informação

Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes.

Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente da rede/ servidor após estarem livres de código malicioso e/ou indesejado.

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

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta política.

O administrador dos sistemas computacionais pode acessar os arquivos e dados de outros usuários, somente em situações especiais e necessárias para a execução de atividades operacionais sob sua responsabilidade.

Segregar as funções por nível hierárquico a fim de restringir ao mínimo necessário os poderes de cada indivíduo dentro do sistema.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para TEKNOFIL.

Implantar controles que gerem registros auditáveis de mídias das informações custodiadas pelo serviço de TI, nos ambientes totalmente controlados por ela.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pela empresa.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.
- os usuários (logins) de terceiros serão de responsabilidade do Diretor Executivo.

Propor as metodologias e os processos específicos para a segurança da informação.

Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.

Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.

Monitorar o ambiente de TI, gerando indicadores e históricos de incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante).

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
Analisar criticamente incidentes em conjunto com o Diretor Executivo. Manter atas das reuniões que exijam ações de Segurança da Informação.

4 - Diretor Executivo, ou seu preposto
É responsabilidade do Diretor Executivo:

- Promover a conscientização dos colaboradores em relação à relevância da segurança da informação para o negócio da TEKNOFIL, mediante treinamentos e outros meios de endomarketing.
- Propor investimentos relacionados à segurança da informação com o objetivo de reduzir mais os riscos;
- avaliar os incidentes de segurança e propor ações corretivas;
- definir as medidas cabíveis nos casos de descumprimento da Política de Segurança da Informação.

MONITORAMENTO/ AUDITORIA
A fim de certificar-se que os controles estão adequados, a empresa poderá:

- Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- 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 sua propriedade;
- Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

CORREIO ELETRÔNICO
O uso do correio eletrônico da TEKNOFIL é para fins corporativos e relacionados às atividades do colaborador dentro do seu escopo de responsabilidades. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique a empresa.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico da Teknofil para:

- Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Enviar mensagem por correio eletrônico usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;
- Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da TEKNOFIL estiver sujeita a algum tipo de investigação.
- Produzir, transmitir ou divulgar mensagem que:
    - Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses da TEKNOFIL;
    - Contenha ameaças eletrônicas, como: *spam*, *mail bombing*, vírus de computador;

- Contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
- Vise obter acesso não autorizado a outro computador, servidor ou rede;
- Vise interromper um serviço, servidor 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;
- Vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- Inclua imagens criptografadas ou de qualquer forma mascaradas;
- Tenha conteúdo considerado impróprio, obsceno ou ilegal, ou que seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- Tenha fins políticos ou propaganda política;
- Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador
- Telefone(s)
- Correio eletrônico

INTERNET

A TEKNOFIL determina diretrizes para que o uso da internet seja condizente com comportamento ético e profissional.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da empresa, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique a realização das atividades profissionais.

Somente os colaboradores que estão devidamente autorizados a falar em nome da Teknofil para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pela empresa poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender às normas internas, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal, à Lei de Proteção de Dados Pessoais e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da empresa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores não tem autorização para utilizar os recursos da TEKNOFIL para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.
Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado TEKNOFIL ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização da Diretoria Executiva.
Os colaboradores não poderão utilizar os recursos da Teknofil para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante a empresa e/ou terceiros.
Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.
Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a Teknofil, a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.
É proibido o compartilhamento de login para funções de administração de sistemas.
A Direção da TEKNOFIL é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.
O Serviço de TI responde pela criação da identidade lógica dos colaboradores, através do gerenciamento de contas dos usuários.
Devem ser distintamente identificados os visitantes, colaboradores e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas.
É de responsabilidade de cada usuário a confidencialidade de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.
Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade).
Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas com maior frequência e sempre que existir um risco eminente.
Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade da TEKNOFIL, cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da empresa, bem como cumprir as recomendações constantes nos procedimentos internos.
É proibido qualquer procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento do suporte de TI da TEKNOFIL.
Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o suporte de TI mediante registro de chamado por email.

Arquivos pessoais e/ou não pertinentes ao negócio (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para os drives de rede.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede, para não correr o risco de serem perdidos caso ocorra uma falha no computador.
No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas.

- Os colaboradores devem informar ao suporte de TI qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico autorizado.
- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador quando não estiverem sendo utilizados.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos algumas situações em que é proibido o uso de computadores e recursos tecnológicos da TEKNOFIL:

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.
- Usar qualquer tipo de recurso tecnológico para 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;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.
- Utilizar software pirata.

DISPOSITIVOS MÓVEIS

O colaborador que deseje utilizar equipamentos portáteis particulares ou acessórios e posteriormente conectá-los à rede da Teknofil, deverá submeter previamente tais equipamentos ao processo de autorização do seu gestor hierárquico.
Equipamentos portáteis, como smartphones, palmtops, pen drives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão previamente validados para uso e conexão em sua rede corporativa.

BACKUP

As mídias de backup (como DVD, CD e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em outro endereço).
Os arquivos de backup devem ser devidamente identificados, inclusive quando for necessário efetuar alterações de nome.
Quaisquer atrasos na execução de backup deverão ser justificados formalmente pelos responsáveis.
Testes aprovação das mídias são realizados automaticamente pelo sistema no momento da criação do backup.
Para formalizar o controle de execução de backups e restores, é gerado um protocolo pelo sistema que deverá ser mantido e arquivado como registro no drive da Teknofil.

DAS DISPOSIÇÕES FINAIS

A segurança deve ser entendida como obrigação de todos dentro da TEKNOFIL. Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela instituição.

A Teknofil exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento dos requisitos previstos nesta Política de Segurança da Informação acarretará violação às regras internas da empresa e sujeitará o usuário às medidas administrativas e legais cabíveis.

Marcello Duarte Santos

Diretor Executivo

TEKNOFIL COMERCIAL LTDA.