Política de Segurança da Informação

Sumário

1. Objetivo

O documento tem como objetivo definir as diretrizes e regras que irão nortear a organização com relação aos padrões de tratamento de dados, geração, utilização, distribuição, armazenamento, boas práticas de uso e métodos para garantir que a disponibilidade, confidencialidade, integridade, autenticidade e confiabilidade sejam atendidas.

2. Público alvo

A presente política destina-se a todos os colaboradores do Grupo Tuberfil, extendendo-se a terceiros, fornecedores e prestadores de serviços temporários.

3. Regra Geral

Grupo Tuberfil serão tratadas neste e em outros documentos como Organização. Funcionários, estagiários, contratados e terceirizados serão tratados como colaboradores.
Todas as políticas relacionadas à de segurança da informação precisam estar disponíveis em local de acesso facilitado aos colaboradores, com versões controladas, protegidas contra alterações e devidamente classificadas quanto ao seu acesso e uso. Esta política é revisada e divulgada aos colaboradores anualmente ou havendo necessidade.

4. Princípios de Segurança da Informação

O compromisso da Organização, com o tratamento adequado das informações, está fundamentado nos seguintes princípios:

- **Confidencialidade**: garantimos que o acesso à informação seja obtido somente por pessoas autorizadas e quando for necessário;
- **Disponibilidade**: garantimos que as pessoas autorizadas tenham acesso à informação sempre que necessário;
- **Integridade**: garantimos a exatidão e a completude da informação e dos métodos de seu processamento. A informação será alterada apenas por pessoas autorizadas, tendo registro do procedimento realizado.
- **Confiabilidade**: garantimos a transparência no trato com os públicos envolvidos, bem como, a informação só pode ser acessada por pessoas autorizadas.
- **Autenticidade:** Garante a veracidade da informação. Verifica se alguém de fato é quem diz ser.
- **Irretratabilidade:** Não revogação da titularidade de uma ação.

5. Diretrizes Gerais

Aplica-se esta Política a todas as informações presentes na Organização, que podem existir de diversas maneiras:

- Escrita em papel;
- Armazenada e/ou transmitida por meios eletrônicos;
- Exibida em filmes ou na mídia;
- Falada em conversas formais e informais.

Independente da forma ou o meio pelo qual a informação for apresentada/compartilhada, ela sempre deverá estar protegida adequadamente, de acordo com controles definidos neste documento.

Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas pelos usuários na utilização dos sistemas de informação na Organização.

As informações, inclusive as de propriedade intelectual, devem ser utilizadas apenas para os propósitos da Organização. Os usuários não podem, em qualquer hipótese, apropriar-se dessas informações, seja em CDs, pendrives, dispositivos móveis ou qualquer outra mídia de armazenamento de dados, ou realizar transmissões não autorizadas. Todos os documentos produzidos, por qualquer sistema de informação, na Organização são de propriedade exclusiva da

Organização.

A identificação do usuário (por meio de seu usuário de rede, senha, crachá ou qualquer outro meio) é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas utilizando tal identificação. A liberação de seu uso será dada a partir do aceite e do preenchimento correto do Termo de Responsabilidade para Segurança da Informação (Anexo 1).

Todo processo de negócio ou de suporte, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador ou equipe de colaboradores, para que a atividade não seja executada e controlada pelo mesmo colaborador ou equipe.

A Organização, por meio de suas áreas ou representantes de Compliance legal e Tecnologia da Informação, se reserva o direito de monitorar e realizar auditorias, automaticamente, sobre o tráfego efetuado através das suas redes de comunicação, acesso à Internet, uso do correio eletrônico, pastas locais de rede, entre outros, em obediência às normas e procedimentos escritos neste e em outros documentos.

Periodicamente são realizados treinamentos sobre a política atual de segurança da informação, ou sempre que alterações significativas sejam inseridas. Nestes treinamentos também são passadas boas práticas e proteção de segurança de dados como políticas de Mesa limpa e Tela limpa.

6. Tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes de Segurança da Informação da Organização em todo o seu ciclo de vida, que compreende:

- Geração;
- Manuseio;
- Armazenamento;
- Transferência;
- Transporte; e
- Descarte

Maiores detalhes sobre o ciclo de vida da informação, pode ser obtida na Política de Classificação da Informação.

7. Processo de Segurança da Informação

Para assegurar que as informações tratadas estejam adequadamente protegidas, a Organização adota os seguintes processos:

• Gestão de Ativos da Informação

Entende-se por ativos da informação tudo o que pode criar, processar, armazenar, transmitir e até excluir informação, podendo ser tecnológicos (software e hardware) e não tecnológicos (pessoas, processos e dependências físicas). Considera-se ativo ou recurso de processamento da informação, além de computadores, notebooks, servidores de dados, de aplicação, Web e de Correio eletrônico, sua infraestrutura de comunicações e processamento, assim como os chamados dispositivos móveis (smartphones, câmeras, gravadores e equivalentes) ou mídias removíveis (pen-drives, cartões de memória, HD externo, Cloud-drives ou equivalentes).

Os ativos da informação são identificados de forma individual, inventariados e protegidos de acessos indevidos, fisicamente e logicamente, e tem documentação e planos de manutenção atualizados anualmente ou quando necessário. Sua nomenclatura é composta por 2 partes:

- Tipo do equipamento:

- TUB - Estações ou Notebook.

- Número sequencial de identificação:
  - 0000

Métodos de proteção e segurança são aplicados aos ativos da informação para proteger acessos indevidos ou não autorizados, vindos de meio externo ou interno, como dispositivos móveis ou mídias removíveis. Estes dispositivos estão sob atenção especial e restrições para evitar infiltração de fragilidades ou facilitar vazamento de informações.

Não é permitido aos colaboradores ou outras partes alterarem a configuração entregue para utilização, ficando esta atividade restrita aos colaboradores da área de Tecnologia da Informação.

Os equipamentos pertencentes à Organização de uso pessoal/coletivo, servidores de dados e aplicativos, de qualquer porte, estão dotados de mecanismos de proteção contra vírus e malwares, com atualizações automáticas e na frequência determinada pela área de TI.

A utilização de softwares, programas, aplicativos e ferramentas de produtividade ou de suporte são definidas pela área de Tecnologia da Informação, não sendo permitido aos colaboradores, realizar instalação ou alterações significativas nos recursos de processamento da informação existentes.

Havendo a necessidade de uso/aquisição de software, sistema, programa, aplicativo ou ferramenta específica, o colaborador deverá obter aprovação da área de Tecnologia da Informação, que após análise técnica, de performance e de segurança necessárias, poderá autorizar sua aquisição ou utilização. Toda e qualquer instalação destas será realizada pela área de Tecnologia da informação ou pelo seu fornecedor, sob supervisão da área de TI.

Cada área da Organização possui pastas de arquivos exclusivas, com acesso restrito a seus colaboradores, devendo ser utilizada de forma ética e responsável.

O uso de impressoras é uma concessão feita aos usuários, assim como correio eletrônico, acesso à Internet, entre outros, e não um direito. Disto decorre que se deve utilizá-la prioritariamente para atividades ligadas ao trabalho, quando em horário comercial ou de trabalho, contribuindo e controlando sua utilização para a segurança da Organização no tocante a vazamento ou acesso indevido a informações desta. Material impresso defeituoso ou inservível pode ser utilizado como rascunho, contanto que não apresente dados de uso restrito, confidencial ou que represente risco à Organização. Material impresso inservível de uso restrito, confidencial ou com conteúdo sensível deve ser destruído através de fragmentação e/ou incineração.

O transporte de mídias de armazenamento, que não seja por meios eletrônicos, deve considerar controles de entrada e saída destas mídias dos locais de armazenamento primário para os de recuperação/guarda. Os controles de entrada e saída devem considerar a solicitação e autorização de transporte/transferência da mídia, o registro do tipo de mídia física, o receptor/remetente autorizado, a data e o horário, e o número da mídia física. Tais recursos devem ser aplicados para assegurar que os dados somente possam ser acessados no ponto de destino e não durante o transporte.

Procedimentos de criptografia a mídias físicas que contenham Dados Pessoais devem ser aplicados nos recursos de processamento da informação, em dispositivos móveis de armazenamento de dados e durante o transporte destes dados.

O descarte de recursos de processamento da informação considera:

a) Substituição de dispositivos de armazenamento de dados – a mídia substituída deve ser formatada utilizando recursos do sistema operacional e, se possível, métodos extras de destruição do seu conteúdo.Caso tenha que

ser mantida por um tempo, antes do descarte de seu conteúdo, recomenda-se o uso de envelopes lacrados para sua guarda;

b) Destruição de dispositivos de armazenamento de dados – o processo de destruição da mídia deve considerar a adoção da legislação de proteção ao meio ambiente, uso de mecanismos físicos como furadeiras, martelo ou prensa mecânica/hidráulica, com objetivo de impedir totalmente o acesso indevido à mídia de armazenamento, ou seja, furar várias vezes os discos, esmagar as placas de dados e/ou os discos, entre outros;

c) Fragmentar ou incinerar documentos ou mídias não óptico/magnéticas.

• Procedimentos de backup

Estabelece diretrizes e padrões para os procedimentos de backup, testes e recuperação de dados como atividades periódicas ou realizados em caso de crise. Serão executados de forma automática e abrangem os dados gravados em sistemas, aplicativos, ferramentas, diretórios de rede privativos de cada equipe, nos servidores de dados e aplicativos.

Os dados armazenados em discos rígidos locais não serão copiados e não será garantida sua recuperação em caso de erro físico nas mídias de gravação ou instabilidade no sistema operacional instalado no equipamento.

Dados armazenados em pastas locais da rede terão suas cópias realizadas, segundo as diretrizes específicas da área de Tecnologia da informação.

A periodicidade, o tempo de retenção, o RPO (Recovery Point Objective) e o RTO (Recovery Time Objective) dos backups observam as regras especificadas nos contratos de prestação de serviços com fornecedores.

RPO (Recovery Point Objective): Tempo máximo suportado de perda de dados de um determinado serviço ou processo de negócio após aocorrência de um desastre.
RTO (Recovery Time Objective): Tempo máximo para retorno operacional de um serviço ou processo de negócio após a ocorrência de um desastre.

Para o plano de backup, devem ser considerados os backups operacionais e contingenciais, onde:

Operacional: é a cópia das informações estratégicas que fazem parte do dia a dia do usuário e que são essenciais para a continuidade do negócio. A restauração deve ser imediata.

Contingencial: cópia das informações sensíveis, vitais para a continuidade do negócio, tem como objetivo permitir a recuperação em casos de catástrofe.

As informações consideradas imprescindíveis, devem estar presentes tanto na rotina do backup operacional quanto contingencial.

Deve-se realizar testes de restore periódicamente (máximo espaçamento de um mês), mantendo evidência da operação, seja sucesso ou não.

A realização do backup é de responsabilidade do setor de tecnologia da informação. O usuário deve seguir o procedimento de armazenamento informado pela TI, que consiste em não armazenar os arquivos localmente, mas sim, no servidor/fileserver, que possui atividades de backup diárias.

Deve ser mantido um backup local e um backup fora das dependências da empresa (mídia física ou nuvem).

• Transferência de informações/dados

Estabelece diretrizes e padrões para os procedimentos de transferência de dados interna e externamente, com proteção

e segurança, através de análises e investigação de vulnerabilidades prévias, nos recursos de processamento da informação, permitindo correções/adequações a tempo, minimizando a violação de dados e impedindo o vazamento dos dados tratados.

Os recursos adotados constam de itens técnicos dos contratos com fornecedores.

• Gestão de Acessos

As concessões, revisões e revogações de acesso devem utilizar ferramentas e os processos da Organização.

Os acessos devem ser rastreáveis, a fim de garantir que todas as ações passíveis de auditoria possam identificar individualmente o colaborador, suas ações e permissões, para sua devida responsabilização.

Devem estar habilitados logs de acesso a recursos de processamento da informação, como:

- Estações de trabalho (desktop e notebook)
  - Log-in e log-off;
- Servidores de dados, aplicativos, WEB e de comunicações
  - ID usuário,
  - data e hora de acesso,
  - identificação do recurso de processamento da informação,
  - operação realizada,
  - resultado da operação (sucesso ou não);
- Sistemas, ferramentas e aplicativos
  - ID usuário,
  - data e hora de acesso,
  - identificação do sistema, ferramenta, aplicativo,
  - módulo, funcionalidade, opção utilizada,
  - operação realizada (inclusão, alteração, exclusão, consulta, emissão de relatório, cópia etc.),
  - Se alteração - informação anterior e informação resultante,
  - Se exclusão – informação eliminada,
  - Se consulta, impressão ou cópia – informações apresentadas para a operação,
  - resultado da operação (sucesso ou não);
- Configuração de sistema operacional, antivírus, malware, Endpoint, ERP, outros
  - ID usuário,
  - data e hora de acesso,
  - identificação do recurso acessado,
  - parâmetro acessado/alterado,
  - operação realizada (inclusão, alteração, exclusão, consulta, emissão de relatório, cópia etc.),
  - informação resultante da operação

As trilhas de auditoria de sistemas devem ser definidas pelos Donos da Informação, seu tempo de retenção e método de eliminação. A equipe de TI ou de Segurança da Informação deve definir o espaço máximo de armazenamento para estas trilhas de auditoria, local de armazenamento, acesso apenas de leitura sob demanda e aprovação, mecanismos de backup distintos, gestão das trilhas de auditoria.

Periodicamente devem ser realizadas revisões de acessos sobre os recursos de processamento da informação, que consideram, recurso de processamento da informação, módulos, funcionalidades, usuários, permissões concedidas e capturar dos gestores destes recursos novas concessões, revogações ou manutenção das permissões existentes.

• Gestão de Riscos

Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidades, ameaças e impactos sobre os ativos de informação da Organização, para que sejam recomendadas as proteções adequadas.

A identificação dos cenários de riscos de segurança da informação e as ações a serem tomadas serão discutidas nos comitês específicos da Organização.

Os testes de identificação de vulnerabilidades e fragilidades na infraestrutura interna e externa da Organização são realizados anualmente e seus resultados são avaliados pela alta direção, tendo seus planos de ação considerados e adotados conforme deliberação destes comitês.

Deve-se manter, junto à equipe de Compliance da Organização, uma Matriz de Riscos, identificando os riscos, suas causas, controles de identificação de materialização e planos de ação, juntamente com a gestão compartilhada sobre a execução e eficácia dos planos de ação identificados, junto aos seus responsáveis, sua data de conclusão, grau de efetividade e risco residual.

• Tratamento de Incidentes de Segurança da Informação e Segurança Cibernética

Os incidentes de segurança da informação e cibernéticos da Organização devem ser reportados à área de Tecnologia da Informação, seja pessoalmente, por e-mail ou qualquer outra forma existente, imediatamente e sem restrições ou receio de penalidades. O tratamento destes incidentes está mapeado em um processo exclusivo de gestão de incidentes de segurança da informação, sob responsabilidade de TI ou de Segurança da Informação. Sua gestão será realizada em processo específico de Gestão de incidentes.

Eventos identificados e classificados como de vazamento ou violação de dados, serão tratados como um subprocesso da gestão de incidentes e segurança da informação, devendo ser reportados ao Encarregado de Proteção de Dados da Organização (DPO), imediatamente pessoalmente, por e-mail ou qualquer outro meio disponível, para que este realize a gestão deste processo, tome as providências necessárias, comunique as partes interessadas e realize as análises, tome as ações adequadas, documente o evento e o finalize como um processo de melhoria contínua do processo.

• Governança com as Áreas de Negócio e Tecnologia

As iniciativas e projetos das áreas de negócios e tecnologia devem estar alinhadas com as diretrizes e arquiteturas de segurança da informação, garantindo a confidencialidade, integridade, disponibilidade e confiabilidade das informações. São tratadas em processo específico de Gestão de Demandas e projetos.

• Segurança Física do Ambiente

O processo de segurança física estabelece controles relacionados à proteção física do perímetro da Organização, à concessão de acesso físico aos ambientes somente a pessoas autorizadas, de acordo com a criticidade das informações previamente mapeadas e declaradas. Estabelece critérios e controles de monitoração do ambiente físico, métodos de comunicação e restrição de colaboradores e terceiros aos ambientes seguros da Organização.

• Segurança Cibernética

A segurança cibernética da Organização é norteada pelos seguintes fatores:

a) Regulamentações vigentes;
b) Melhores práticas; e
c) Cenário mundial.

Conforme sua criticidade, o programa divide-se em:

a) **Ações críticas:** Consiste em correções emergenciais e imediatas para mitigar riscos iminentes;
b) **Ações de Sustentação:** Iniciativas de curto/médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro, respeitando o apetite de risco da Organização e permitindo que ações de longo prazo ou estruturantes possam ser realizadas;
c) **Ações Estruturantes:** Iniciativas de médio/longo prazo que tratam a causa raiz dos riscos e que preparam a Organização para o futuro.

Ações de suporte da equipe de colaboradores da área de Tecnologia da Informação através de ferramentas de acesso remoto às estações somente poderão ser realizadas através da aprovação do usuário ou seu gestor imediato.

Medidas protetivas ao acesso remoto às redes da Organização, seja por conexão direta, através de VPN ou ferramenta de acesso remoto, devem ser mantidas atualizadas e validadas periodicamente, alinhadas às diretrizes do Plano de Continuidade de Negócios.

8. Normas de Utilização da Internet

O acesso à Internet na Organização é uma concessão feita aos usuários, e não um direito. Disto decorre que se deve utilizá-la prioritariamente para atividades ligadas ao trabalho, quando em horário comercial ou de trabalho.

Os usuários devem utilizar a Internet de forma adequada e diligente, em conformidade com a lei, a moral e a ordem pública, abstendo-se de objetivos ou meio para a prática de atos ilícitos, lesivos aos direitos e interesses da Organização ou que, de qualquer forma, possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos e documentos de qualquer tipo.

É proibida a divulgação e/ou compartilhamento indevido de informações sigilosas em listas de discussão, bate-papo ou softwares de mensagens eletrônicas.

A concessão de uso será realizada a partir de uma solicitação registrada na ferramenta de chamados, pelo gestor da área do colaborador e validação/aprovação pela equipe de TI.

Usuários com acesso à Internet não podem efetuar upload de qualquer software cuja licença pertence à Organização, o mesmo ocorrendo para dados/processos/informações de propriedade da Organização. Exceção feita a casos especiais, mediante solicitação ao responsável pelo software e/ou dados, e sua posterior autorização.

Downloads serão autorizados, mediante solicitação, justificativa e aprovação prévias, conforme processo de solicitações/chamados estabelecido, desde que a fonte seja confiável. Para instalação de softwares oriundos da Internet, será necessária autorização da área de Tecnologia da Informação.

Cada usuário é responsável por zelar pelo cumprimento ao estabelecido pela presente norma e por todas as atividades realizadas por intermédio de seu usuário de rede. As contas de serviço (grupo) têm acesso restrito a determinadas pastas de rede na Organização.

Não é permitida a utilização de Webmail externo, salvo autorização pela área de TI, software peer-to-peer (ponto-a- ponto ou torrent), acesso a sites de relacionamento (como Facebook, Twiter, Instagram e afins), jogos, sites que incitem ao ódio, racismo, pornografia, pedofilia e outros contrários à lei. Também, fica vetado a utilização de hotspot para roteamento de internet para outros dispositivos pessoais.

O Grupo Tuberfil retém o direito de monitoramento de tráfego em sua rede interna, caso identificada alguma violação, os responsáveis serão notificados e as ações cabíveis tomadas.

9. Normas de Utilização da Telefonia

De acordo com a regulamentação interna, as ligações telefônicas realizadas não são monitoradas e gravadas. O que não exime cada colaborador ou prestador de serviços, usuário deste serviço de seguir as regras de comportamento público do Código de Ética e Compliance, sendo constatada alguma violação, as medidas cabíveis serão aplicadas.

10. Normas de Utilização do Correio Eletrônico

As contas de correio-eletrônico têm titularidade única e exclusiva, sendo considerada como uma ferramenta de trabalho, e seu bom ou mal uso determina a responsabilidade direta do usuário. As contas de serviço (grupo), por sua vez, possuem um ou mais responsáveis pelo seu uso.

A utilização do correio deve ser feita de forma adequada e diligente exclusivamente para atender aos fins da Organização. A concessão de uso será realizada a partir de uma solicitação registrada na ferramenta de chamados,realizada pelo gestor da área solicitante, com análise e aprovação pela equipe de TI.

O tamanho das caixas postais é de 50GB para todos os usuários. Já em relação ao tamanho de cada mensagem enviada/recebida, o limite é de 10MB. Necessidades acima destes limites devem ser solicitados à área de Tecnologia da Informação.

É vedada a qualquer usuário a utilização do correio eletrônico para quaisquer das seguintes atividades:

- Envio de mensagens não autorizadas, divulgando informações sigilosas;
- Acesso não autorizado à caixa postal de outro usuário ou de serviços, caso esta não esteja sob sua responsabilidade;
- Envio, manuseio e armazenamento de material que caracterize a divulgação, incentivo ou prática de atos ilícitos, proibidos (seja pela lei, seja pela presente norma), lesivos aos direitos e interesses da Organização, que possam danificar, inutilizar, sobrecarregar ou deteriorar hardware e/ou software, documentos e arquivos de qualquer tipo,ou que contrariem a moral, os bons costumes e a ordem pública;
- Envio intencional de mensagens do tipo “corrente”, “spam” ou que contenham vírus eletrônico ou qualquer forma de programação (arquivos executáveis ou do tipo script) que sejam prejudiciais ou danosas aos destinatários das mensagens;
- Utilização de listas e/ou caderno de endereços para distribuição de mensagens que não tenham relação com o interesse funcional da Organização ou a devida permissão do responsável pelas listas e/ou caderno de endereços em questão;
- Uso de contas particulares, através da configuração dos serviços Post Office Protocol – POP, Internet Message Access Protocol – IMAP e Simple Mail Transfer Protocol – SMTP de provedores não pertinentes aos domínios Tuberfil.com.br.
- Envio de mensagens que contenham 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 da rede;
- Todo e qualquer uso do correio eletrônico não previsto nesta política que afete a Organização de forma negativa.

11. Normas de Utilização de Contas e Senhas para Usuários

Com o intuito de controlar a distribuição de direitos de acesso a sistemas de informação e serviços, a Organização estabelece estas normas para evitar o uso inapropriado de usuários e senhas e, consequentemente, diminuir o risco de falhas e violações de sistemas.

- Os acessos a computadores e redes deve ser protegido por senha.
- As senhas poderão ser alterdadas pelos usuários no ambiente utilizado (Windows, Sap, Totvs etc).
- Caso algum sistema defina uma senha inicial, essa deve ser trocada no primeiro acesso.
- As senhas trocadas ou expiradas devem ser cadastradas para efeito de bloqueio de utilização, por no mínimo, cinco vezes.
- Os arquivos com informações restritas, sigilosas ou senhas, devem ser criptografados no seu armazenamento.
- Todas os usuários e senhas de rede são pessoais e intransferíveis, devendo ser mantidas em sigilo. Cada usuário é responsável por manter em segredo seu usuário e sua senha, e será responsabilizado pelo mau uso desses.
- As senhas de rede para usuários finais têm, no mínimo, 8 caracteres, sendo obrigatório o uso de letras maiúsculas e minúsculas, números e caracteres especiais (@ % ^; .), na ocorrência de 5 tentativas de ingresso erradas, a senha de acesso à rede da Organização é bloqueada. Para desbloqueio, somente com solicitação formal à área de TI. O tempo de expiração da senha será de 90 dias no máximo, podendo ser trocada a qualquer momento pelo colaborador. O desbloqueio de usuários e senhas somente ocorrerá através de solicitação formal pelo gestor imediato do colaborador.
- As senhas não devem ser triviais ou previsíveis.
- Eventos de incidente de segurança da informação ou de vazamento/violação de dados, poderão iniciar um processo de expiração de senhas, conforme procedimento específico.
- Todos os sistemas e aplicações instalados na Organização devem ter algum mecanismo que oculte a visualização das senhas para utilização desses sistemas/aplicações.
- Os usuários de rede terão privilégios administrativos que se enquadrem às suas atividades, o mesmo ocorrendo nas permissões aos diretórios de rede e seus conteúdos.
- Instalações de softwares de qualquer natureza devem ser solicitadas à área de TI, que irá analisar o impacto dessa instalação, executando-a ou não, de acordo com o resultado dessa avaliação.
- Quaisquer desligamentos ou novas contratações deverão ser informados com antecedência às áreas de TI e representantes de Compliance/Controles Internos, para que os acessos à Organização sejam bloqueados ou concedidos adequadamente.
- A criação ou alteração de usuários e atribuição de senhas será realizada a partir de uma solicitação registrada na ferramenta de chamados, pelo gestor da área solicitante. A primeira senha será criada já como expirada, exigindo que na primeira conexão do usuário essa seja trocada.

A identificação de usuário segue as seguintes regras:

- Primeiro nome, seguido de um ponto, seguido pela última parte do nome do colaborador
- Casos de duplicidade de identificação de usuário será utilizada outra parte do nome do colaborador

12. Normas de Controle de Acesso

O acesso físico às dependências da Organização e a segregação física das atividades está contemplado na Política de Segregação de Atividades.

13. Aprovação desta Política

A presente política foi revisada e aprovada pelo Comitê de Risco e Compliance.

Versão	Responsável	Aprovador	Data publicação
2.0	Jefferson Nogueira	Fábio Marcon	18/01/2023

ANEXO 1 - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

TERMO DE ADESÃO

Atesto ter recebido, lido e compreendido as diretrizes, normas, instruções e procedimentos contidos na Política de Segurança da Informação da Tuberfil Indústria e Comércio de Tubos LTDA, comprometendo-me a observá-la em sua íntegra e comunicar, imediatamente qualquer inconformidade com a Política que venha a ser de meu conhecimento, seja diretamente, seja por terceiros.

Declaro ter pleno conhecimento que o descumprimento deste Termo de Adesão pode implicar no meu afastamento imediato da empresa, sem prejuízo da apuração dos danos que tal descumprimento possa ter causado.

Declaro ainda que, quando cabível, o descumprimento deste termo pode sujeitar-me às responsabilidades legais associadas a meus atos.

_____,_____de_____de _____

_____

Assinatura e Nome Completo

ANEXO 2 - Glossário

Usuário - Colaboradores do Grupo Tuberfil, que estão autorizados a utilizar a rede e os equipamentos de informática. Pode também, ser referenciado como uma identificação de usuário.

TI - Tecnologia da Informação (informática).

Recurso de processamento da informação - São os equipamentos utilizados pelos colaboradores tais como: computadores, impressoras, e-mails, Internet e afins.

Identificação de Usuário – Identidade atribuída a um colaborador para realizar acesso aos recursos de processamento da informação da organização.

Site ou Website – Endereço na internet (WWW) composta por páginas que contém informações, imagens, vídeos, sons etc., para serem acessados por qualquer pessoa que se conecte à rede mundial. Estão hospedadas em servidores Web, que armazenam conteúdo, dados e outros tipos de informação, administradas por provedores de acesso.

Software – Programas de Computador.

Download – Atividade de copiar conteúdo da internet para estação local de trabalho, dispositivos móveis (smartphones, câmeras, gravadores e equivalentes) ou mídias removíveis (pen-drives, cartões de memória, HD externo ou equivalentes), ou recurso de processamento da informação, através da Internet.

Upload – Envio de um arquivo de um recurso de processamento da informação para outro, através da Internet.

Peer-to-Peer (P2P) – É um tipo de programa que permite a distribuição de arquivos a outros usuários através da Internet (exemplo Torrent).

Internet – Associação mundial de redes de computadores interligados, que utilizam protocolos de comunicação de dados. A Internet provê um meio abrangente de comunicação através de: transferência de arquivos, conexões à distância, serviços de correio eletrônico etc.

Intranet – Rede interna, restrita, de uso pessoal ou corporativo, que utiliza a mesma tecnologia da Internet, para que os usuários possam acessar as informações dos seus respectivos departamentos.

Caixa Postal – Recurso de armazenamento de dados de mensagens de correio eletrônico, onde são armazenadas as mensagens de e-mail e seus anexos.

Correio eletrônico – Meio de envio e recebimento de informações entre 2 ou mais partes, baseado em protocolos de comunicação da Internet, que se utiliza de uma rede de comunicação de computadores.

FTP (File Transfer Protocol) – Protocolo padrão da Internet, usado para transferência de arquivos entre recursos de processamento de informação.

IMAP (Internet Message Access Protocol) – Protocolo de acesso a mensagens eletrônicas.

POP (Post Office Protocol) – Protocolo usado por clientes de correio eletrônico para manipulação de arquivos de mensagens em servidores de correio eletrônico.

SMTP (Simple Mail Transfer Protocol) – Protocolo de comunicação usados para troca de mensagens na Internet.

ANEXO 3 - Termo de compromisso para uso de dispositivo e equipamento eletrônico corporativo

TERMO DE COMPROMISSO PARA AO USO DE DISPOSITIVO E EQUIPAMENTO ELETRÔNICO CORPORATIVO

A empresa TUBERFIL INDUSTRIA E COMERCIO DE TUBOS LTDA, situada na Rua Dalízio Silveira Barros, nº 290, Distrito Industrial, inscrita no CNPJ sob o nº 59.300.962/0001-09, entrega neste ato, em comodato ao colaborador/contratado _____, portador (a) da cédula de identidade RG sob o nº_____, doravante denominados simplesmente "USUÁRIO", o(s) dispositivo(s) e equipamento(s) descrito(s) abaixo:

Equipamento	Marca	Modelo	Service Tag/IMEI	Identificação/Linha

Acessórios Inclusos:

Acessório	Marca	Modelo	Service Tag	Identificação

O " USUÁRIO " utilizará o dispositivo / equipamento sob as seguintes condições:

1. O equipamento deverá ser utilizado ÚNICA e EXCLUSIVAMENTE a serviço da empresa e em benefício da atividade a ser exercida pelo USUÁRIO;

2. O USUÁRIO ficará responsável pelo uso e conservação do dispositivo / equipamento, doravante referido também como ferramenta de trabalho;

3. O USUÁRIO tem somente a posse em comodato desse equipamento, tendo em vista o uso exclusivo para prestação de serviços profissionais, sem qualquer direito a propriedade do equipamento, sendo terminantemente proibido o seu empréstimo, locação ou cessão à terceiros a qualquer título;

4. Ao término da prestação de serviço ou do contrato individual de trabalho, o USUÁRIO se compromete na devolução desse equipamento, nas mesmas condições em que o recebeu, no mesmo dia em que ocorrer a comunicação do encerramento de seu contrato;

5. Quando o equipamento for um dispositivo móvel ou smartphone, fica proibido o uso do aparelho para navegação em internet e redes sociais, ligações que não sejam entre números da empresa e em prol de suas atividades ou para

seus demais contratos. Ligações externas ou para outros números devem ser feitas de forma a cobrar. Caso contrário,o valor das chamadas ou dos serviços desautorizados será cobrado do USUÁRIO, ficando desde já autorizado o desconto desse valor da remuneração do USUÁRIO;

6. Fica proibida a instalação de aplicativos ou programas que não aqueles já instalados no dispositivo/ equipamento quando de sua entrega;

7. Caso o equipamento seja danificado ou inutilizado por emprego inadequado, mau uso, negligência ou extravio, a empresa poderá cobrar o seu conserto ou reposição do USUÁRIO, ficando desde já autorizado o desconto desse valor da remuneração do USUÁRIO;

8. O USUÁRIO abaixo identificado declara estar ciente e de acordo com os termos e as condições para o recebimento e uso desse dispositivo / equipamento.

Indaiatuba,_____de_____de_____.

_____

Nome:

CPF: