SUMÁRIO

1. INTRODUÇÃO 3
2. OBJETIVO 3
3. PARTES INTERESSADAS E CAMPO DE APLICAÇÃO 3
4. LEGENDA 4
5. CONCEITOS IMPORTANTES 5
6. PROPRIEDADE, MANUTENÇÃO DA CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE DAS INFORMAÇÕES 5
7. DOS RECURSOS TECNOLÓGICOS 6
7.1. EQUIPAMENTOS DOS USUÁRIOS (ESTAÇÃO DE TRABALHO), EMPRÉSTIMO E RETIRADA DE ATIVOS (NOTEBOOKS E CELULARES) 6
7.2. EQUIPAMENTOS DE TERCEIROS 8
7.3. UTILIZAÇÃO DA REDE 9
7.4. AUTENTICAÇÃO E CREDENCIAIS DE ACESSO 9
7.5. POLÍTICA DE SENHAS 9
7.6. ACESSO - PERÍODOS DA SEMANA 10
7.7. REMOÇÃO, DEVOLUÇÃO E DESCARTE DAS INFORMAÇÕES 11
7.8. ACESSOS A SISTEMAS DE INFORMAÇÃO E SEGREGAÇÃO DE ATIVIDADES/FUNÇÕES 11
7.9. MÍDIAS SOCIAIS - ACESSO CORPORATIVO E PARTICULAR 11
7.10 ACESSO REMOTO (VPN) 12
7.11 ACESSO AO BANCO DE DADOS 12
7.12 CONCESSÃO DE ACESSO A SERVIÇOS ESPECÍFICOS 13
7.13 USO DE MÍDIAS REMOVÍVEIS 13
7.14 INTERNET, SOFTWARES DE COMUNICAÇÃO E MENSAGERIA: 14
7.15 CORREIO ELETRÔNICO E ASSINATURA: 15
7.16 WHATSAPP 18
7.17 EXCEÇÃO 18
7.18 SERVIDOR DE ARQUIVOS 18
7.19 IMPRESSORAS 18
7.20 ARQUIVOS E PROGRAMAS 19
7.21 BACKUP 19
7.22 USO WIFI 20
7.23 MONITORAMENTO - RASTREABILIDADE E CÂMERAS DE SEGURANÇA 20
8. MESA E TELA LIMPA EXPOSIÇÃO DE INFORMAÇÕES 21
9. GESTÃO DOS ATIVOS DE INFORMAÇÃO E CLASSIFICAÇÃO 22
10. IDENTIFICAÇÃO DAS INFORMAÇÕES DOCUMENTADAS 23
11. PARTES EXTERNAS E CONTRATOS 23

12. CONTINUIDADE DO NEGÓCIO, CONSCIENTIZAÇÃO, TREINAMENTO E PRIORIZAÇÃO DAS AÇÕES VOLTADAS A SEGURANÇA DA INFORMAÇÃO 24
13. MONITORAMENTO E RASTREABILIDADE 25
14. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS 25
15. INCIDENTES DE SEGURANÇA DE INFORMAÇÃO 26
15.1 EVENTOS VERSUS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 27
15.1.1 EVENTOS 27
15.1.2 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 28
15.2 OBJETIVOS DO PROCESSO 28
15.3 CLASSIFICAÇÃO DOS INCIDENTES DE SEGURANÇA 29
15.4 RESPONSABILIDADE SOBRE A NOTIFICAÇÃO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO 30
15.5 GESTÃO PARA INCIDENTES E SEGURANÇA DA INFORMAÇÃO 30
16. DOS DEVERES E RESPONSABILIDADES 31
16.1 DEVERES E RESPONSABILIDADES DOS COLABORADORES 31
16.2 DEVERES E RESPONSABILIDADES DOS DIRETORES E GESTORES 31
16.3 DEVERES E RESPONSABILIDADES DOS PRESTADORES DE SERVIÇOS 32
16.4 DEVERES E RESPONSABILIDADES DOS VISITANTES 32
17. DAS PENALIDADES 32
18. CRIPTOGRAFIA 34
19. CONSIDERAÇÕES FINAIS 35
20. TERMO DE RESPONSABILIDADE 36

1. INTRODUÇÃO

Para a empresa **WTECH INDÚSTRIA E COMÉRCIO LTDA**, toda informação é um recurso fundamental e estratégico para o desenvolvimento e manutenção das atividades profissionais.

A presente **Política de Segurança da Informação (PSI)** está baseada nos requisitos da norma ABNT NBR ISO/IEC 27001:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação.

O termo "política" refere-se às regras, procedimentos e condutas que visam estabelecer responsabilidades e limites de atuação em relação à segurança da informação e comunicação, reforçando uma cultura interna baseada em integridade.

2. OBJETIVO

A **Política de Segurança da Informação (PSI)** visa definir as diretrizes que nortearão as normas e práticas que tratam acerca da **proteção da informação**, principalmente aspectos que envolvem a utilização, armazenamento e distribuição de tais dados.

Torna-se indispensável a **confidencialidade, integridade e disponibilidade** das informações utilizadas pelos envolvidos, independentemente do meio e local em que estejam inseridas.

Todas as instruções e práticas realizadas pela empresa **WTECH** baseiam-se na legislação vigente, órgãos reguladores, autorreguladores, nas boas práticas que envolvem a segurança da informação e normas complementares.

3. RESPONSABILIDADE

A presente Política foi desenvolvida pela advogada e DPO *(Data Protection Officer)* **Jéssica Maria Machado**, responsável pelo setor Jurídico da empresa **WTECH, e aprovada pela Diretoria**.

A administração da empresa acredita e compromete-se com a melhoria contínua dos procedimentos internos, além da segurança das informações e cibernética que a envolvem, portanto, havendo a necessidade de quaisquer mudanças, tais alterações deverão ser aprovadas pela Diretoria.

4. PARTES INTERESSADAS, PÚBLICO ALVO E CAMPO DE APLICAÇÃO

Esta política abrange todos os colaboradores, prestadores de serviço, profissionais de empresas contratadas e visitantes que possuem acesso à rede de comunicações, às informações confidenciais, aos equipamentos computacionais e/ou ambientes controlados.

Terão acesso às informações confidenciais e ambientes controlados da empresa **WTECH**, dentro dos limites definidos, os colaboradores e prestadores de serviço, profissionais de empresas contratadas e visitantes, que concordarem com a política, registrando o aceite através da assinatura no **Termo de Aceite,** seja ele virtual quando for acessado online, quanto presencialmente, caso seja uma visita física.

Sempre que for realizado o primeiro contato com a empresa **WTECH,** o profissional participará de uma integração com o **setor de Compliance**, a fim de estar ciente das disposições internas.

É obrigação de cada colaborador e profissional, manter-se atualizado em relação a esta Política de Segurança da Informação (PSI) e aos procedimentos e normas relacionadas, buscando orientação do setor jurídico ou de TI da empresa **WTECH,** sempre que não estiver absolutamente seguro quanto às suas ações.

5. LEGENDA

a) **Rede de Comunicações:** Abrange todos os sistemas, diretórios e Intranet disponibilizados aos colaboradores, conforme perfil de acesso definido.

b) **Papel**: diz respeito às atividades exercidas por um os mais colaboradores na empresa;

c) **Software:** São todos os programas instalados nos computadores, os quais são disponibilizados pela equipe de TI para o exercício de sua função.

d) **Ambiente Lógico:** Ambiente controlado, eletrônico, onde circulam e são armazenadas informações confidenciais, softwares e sistemas.

e) **Ambiente físico:** Dependências físicas da empresa.

f) **TI:** Setor de Tecnologia da Informação.

g) **Usuário:** Colaborador ou colaboradores que detenham acesso aos ambientes físico e lógico para o desempenho de suas atividades.

h) **Equipamentos Computacionais:** São todos os equipamentos de propriedade da empresa, disponibilizados ao uso dos colaboradores, incluindo desktops, notebooks, impressoras, scanners, celulares, tablets, equipamentos de vídeo conferências, etc.

i) **Colaboradores:** Todas as pessoas com vínculo empregatício com a empresa.

j) **Prestadores de serviços:** Pessoa jurídica ou física que mantenha contrato de prestação de serviço.

k) **Visitante:** Todo indivíduo que não mantenha qualquer sorte de vínculo formal com a empresa, todos aqueles que não se enquadram na definição de colaborador, conforme acima;

l) **Ativos:** Todo elemento que compõe os processos que manipulam e processam a informação, a contar a própria informação, o meio em que ela é armazenada, bem como os equipamentos, sistemas ou aplicativos em que ela é manuseada, transportada e descartada;

m) **Áreas Sensíveis:** São áreas ou setores que concentram uma quantidade considerável de informações sensíveis e estratégicas para o negócio;

n) **Ativos de informação:** Qualquer informação que tenha valor para a organização.

o) **Custodiante:** Usuário com atribuição fornecida pelo proprietário da informação para protegê-la adequadamente;

p) **Confidencialidade:** Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando à limitação de seu acesso e uso apenas às pessoas para quem elas são destinadas;

q) **Disponibilidade:** Toda informação gerada ou adquirida por um indivíduo ou instituição deve estar disponível aos seus usuários quando os mesmos necessitem para executar suas atividades.

6. DIRETRIZES GERAIS

A empresa **WTECH** possui o domínio de todo e qualquer material presente em sua rede e ativos de sua propriedade, e, portanto, se reserva ao direito de controlar, através de ferramentas de gerenciamento, procedimentos e auditorias, qualquer informação encontrada em qualquer um de seus ativos, com ou sem a ciência do seu colaborador, funcionário ou terceiros, de modo a garantir a boa utilização e a integridade de seu sistema de informação.

A informação sob custódia da matriz e filiais da empresa **WTECH**, mesmo que pertencente a clientes, colaboradores ou fornecedores, serão protegidas contra o acesso de pessoas não autorizadas.

A informação deve ser armazenada, pelo tempo determinado pela instituição, legislação ou regulação vigente, o que for maior, e recuperável quando necessário. O local de armazenamento das informações deve ser apropriado e protegido contra sinistros e acessos de pessoas não autorizadas.

7. PROPRIEDADE, MANUTENÇÃO DA CONFIDENCIALIDADE, INTEGRIDADE E DISPONIBILIDADE DAS INFORMAÇÕES

As informações pertencentes à empresa **WTECH** devem ser preservadas em relação a sua confidencialidade, integridade e disponibilidade. Toda informação manuseada, transportada, armazenada ou descartada deve observar os seguintes princípios e diretrizes:

- Todas as informações geradas pelos usuários e autorizadores, que sejam utilizadas através de algum recurso disponibilizado pela empresa, é de propriedade exclusiva desta;
- As ideias, os métodos, fórmulas e as criações aplicadas e desenvolvidas pela empresa **WTECH,** não serão cedidas a nenhum profissional, seja ele colaborador ou terceirizado;
- Todas as partes que obtiverem informações deverão prevenir-se quanto à possibilidade da ocorrência de vazamento da informação, por meio de controles específicos descritos na presente Política e correlatos;

• Todos os colaboradores, terceiros e envolvidos em negociações, devem utilizar os recursos da empresa seguindo os princípios de segurança da informação, sem afetar ou causar prejuízo a outrem;

• Qualquer descumprimento da política por qualquer usuário deve ser imediatamente comunicado ao setor jurídico da empresa **WTECH;**

• A empresa de tecnologia deverá manter um Sistema de Gestão de Riscos sobre o aspecto da segurança da informação. O Gerenciamento de Riscos deve ser identificado por tipo de exposição, avaliado quanto a probabilidade de incidência e o impacto no negócio. O resultado desta análise poderá ser classificado como baixo, médio ou alto. Identificado o risco alto, será aplicado o plano de ação para mitigação do risco;

• Os processos e controles internos devem ser revisados, controlados e sempre que possível, mapeados;

• Todos os dados pessoais eventualmente coletados observarão as hipóteses de tratamento previstas na legislação, em especial à Lei Geral de Proteção de Dados Pessoais (LGPD). Nestes casos, os titulares de dados serão devidamente informados sobre a finalidade dos tratamentos que serão realizados e o armazenamento respeitará padrões rígidos de segurança e confidencialidade, sendo providas todas as medidas técnicas, administrativas e institucionais cabíveis;

• A empresa **WTECH** preocupa-se com todas as informações cedidas, sendo assim, os dados dos titulares serão devidamente observados, sendo possível que acessem, retifiquem e solicitem a exclusão de dados, caso achem pertinente. O mesmo ocorre com a limitação e oposição quanto ao tratamento de dados, qualquer pessoa poderá retirar eventual consentimento concedido.

8. DOS RECURSOS TECNOLÓGICOS

Caberá ao setor de T.I, ou, na falta deste, a empresa terceirizada de tecnologia, definir procedimentos sistêmicos e/ou instruções de trabalho específicas quando cabíveis.

8.1. EQUIPAMENTOS DOS USUÁRIOS (ESTAÇÃO DE TRABALHO), EMPRÉSTIMO E RETIRADA DE ATIVOS (NOTEBOOKS E CELULARES)

Os equipamentos (desktops, notebooks, celulares, etc.) necessários para execução das atividades profissionais serão disponibilizados pela empresa **WTECH**, desde que solicitado pelo profissional e autorizado pelo gestor competente.

Cada colaborador e/ou terceiro deverá zelar pelo bom uso dos equipamentos recebidos, e, sendo constatado algum dano por imprudência ou imperícia no uso dos equipamentos, a empresa reserva-se o direito de solicitar reembolso.

A empresa **WTECH** escolherá o modelo, fabricante, configuração, tamanho e demais características do equipamento a ser adquirido. Inclusive, a manutenção física ou lógica, a instalação, desinstalação, correções de segurança, aplicativos, alterações diversas, configuração ou modificação, deverá ser realizada pelo setor de T.I interno e/ou terceirizado, sendo proibido quaisquer outros usuários realizarem tais atos.

Todos os computadores serão entregues com as versões de software antivírus instaladas, ativas e atualizadas permanentemente, sendo terminantemente proibido que sejam deletadas.

Além do mencionado, é vetado aos usuários conectarem dispositivos não autorizados no sistema de rede interna da empresa, intervir nos servidores e sistemas, conectar redes móveis sem autorização, e, por fim, manter dados e informações pessoais nos computadores.

8.2. EQUIPAMENTOS DE TERCEIROS

É permitido ao terceiro conectar-se à rede de computadores através da rede de visitantes e tal acesso é solicitado ao setor administrativo da empresa.

A rede de visitantes poderá ser acessada através de um "voucher" com senha e terá duração de 8 horas contínuas.

8.3. UTILIZAÇÃO DA REDE

O ingresso à rede interna deve ser devidamente controlado pela empresa de tecnologia, para que a empresa não corra riscos envolvendo a segurança das informações e, caso ocorram, sejam minimizados.

8.4. AUTENTICAÇÃO E CREDENCIAIS DE ACESSO

A senha é a chave de acesso pessoal que garante que somente pessoas autorizadas utilizem determinados dispositivos ou recursos.

Cada usuário é responsável pela manutenção e guarda de sua senha, a qual não pode ser compartilhada e não deve ser anotada em arquivos físicos ou de fácil acesso, cabe aos usuários a memorização de suas senhas.

8.5. POLÍTICA DE SENHAS

Para que os usuários acessem o ambiente tecnológico da empresa **WTECH,** é necessário que possua um login e senha. A sua propriedade é única, intransferível e nominal.

Qualquer ação realizada pelo usuário é de sua inteira responsabilidade, portanto, é proibido que as informações de login sejam compartilhadas com terceiros.

As senhas, quando possíveis de serem configuradas, deverão seguir o conceito de "senha forte", que inclui letras (A-Z, a-z), números (0-9) e caracteres especiais (@#$#, entre outros). Quando não possíveis de serem configuradas, a utilização de datas de aniversário, datas comemorativas, datas especiais, nomes, apelidos, endereços de residência, telefones e placas de veículos devem ser evitadas.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade).

Cada login possui um acesso e é vinculado à função que o usuário exerce na empresa **WTECH,** portanto, não é permitido que um usuário acesse outras áreas que não sejam as necessárias para a execução de suas atividades.

Para preservar a confidencialidade e a integridade das informações, é obrigatório ao usuário manter o bloqueio da tela da sua estação de trabalho sempre que não estiver no local.

8.6. ACESSO - PERÍODOS DA SEMANA

Os acessos, quando possíveis de serem configurados nos sistemas, respeitarão 2 (dois) períodos de acesso, sendo esses definidos pelo Gestor da área em cada "papel", da forma abaixo:

a) Acesso Total – acesso 24 horas por dia, 7 dias por semana;
b) Acesso Expediente – acesso de segunda a sexta feira das 08:00h às 18:00h.

A gerência, diretoria e os colaboradores que forem devidamente autorizados, terão acesso total ao sistema. Os demais, apenas o horário de expediente, conforme mencionado acima.

8.7. REMOÇÃO, DEVOLUÇÃO E DESCARTE DAS INFORMAÇÕES

Sempre que um colaborador for desligado, as informações armazenadas serão verificadas pelo gestor, e, serão repassadas ao próximo usuário a utilizar o login em questão.

O acesso será bloqueado pelo setor de T.I competente, para que o usuário desligado não possa mais acessá-lo e todas as informações serão avaliadas de forma técnica.

8.8. ACESSOS A SISTEMAS DE INFORMAÇÃO E SEGREGAÇÃO DE ATIVIDADES/FUNÇÕES

Os responsáveis pelos processos internos da empresa **WTECH** controlarão e cuidarão das informações baseando-se na confidencialidade, integridade e disponibilidade dos dados.

Todos os acessos serão divididos por autorizações, ou seja, cada profissional terá acesso apenas ao que lhe compete.

8.9. MÍDIAS SOCIAIS - ACESSO CORPORATIVO E PARTICULAR

O acesso e uso de mídias sociais a partir da rede da empresa é passível de restrição em caso de uso indevido ou fora dos critérios de razoabilidade que norteiam o trabalho de cada setor.

A liberação de acesso às mídias sociais para fins profissionais deve estar definida de acordo com a função que o colaborador exerce. Caso o usuário detecte algum conteúdo publicado que afete diretamente a imagem da empresa, deve comunicar imediatamente o Comitê de Segurança da Informação e Privacidade de Dados, conforme descrito na presente Política. Todo usuário é responsável pela proteção das informações da empresa.

As áreas ou usuários que possuem o acesso corporativo autorizado às mídias sociais, devem fazer o seu uso apenas no âmbito de suas competências e atividades profissionais.

8.10 ACESSO REMOTO (VPN)

A concessão de acesso remoto VPN será feito apenas em notebooks de colaboradores ou em casos especiais por solicitação do Gestor e com aprovação da Diretoria da área, podendo ser revogada a qualquer tempo, sem aviso prévio.

Acesso remoto VPN para fornecedores serão criadas via solicitação das áreas, com aprovação do Gestor e informação do tempo necessário que deverá ficar disponível. Preferencialmente, de 6 em 6 meses, todos os usuários de acesso remoto VPN serão inativados e suas senhas alteradas, aguardando o contato de cada usuário/fornecedor para nova criação, essa medida visa garantir que os acessos remotos estão sendo feitos por colaboradores e fornecedores autorizados.

A concessão de uso de acesso remoto deve ser realizada de modo a atender aos objetivos de negócio, limitada às atribuições, cargo e/ou funções do usuário e/ou fornecedor.

O usuário/fornecedor que utiliza os recursos de acesso remoto ao ambiente corporativo, deve proteger suas credenciais de acessos e realizar o encerramento da sessão ao término de suas atividades.

O usuário deve utilizar os serviços de acesso remoto em ambientes seguros de conexão, especialmente quando estiver em deslocamento.

8.11 ACESSO AO BANCO DE DADOS

O acesso e o uso aos bancos de dados devem ser restritos às pessoas autorizadas e de acordo com a necessidade para o cumprimento de suas funções. A concessão de acesso às informações contidas nos bancos de dados devem ser autorizadas com base na regra de mínimo acesso necessário para o desempenho da função.

Os acessos devem ser nominados (pessoal) e com "senha forte", observando-se o item 6.5 desta política. Quando possível, é necessário que sejam criados logs nas intervenções para consulta ou manipulação de dados realizados nos bancos de dados, principalmente se o nível de privilégio concedido ao usuário em questão for alto.

8.12 CONCESSÃO DE ACESSO A SERVIÇOS ESPECÍFICOS

Compreende-se como acesso a serviços específicos aqueles que não fazem parte do dia a dia do colaborador, tais como VPN, Terminal remoto, administrador local da máquina, entre outros. São serviços que precisam ser liberados, de forma exclusiva e específica, para que o colaborador possa exercer a sua atividade de forma habitual ou esporádica.

A autorização para a liberação é feita pelo gestor do colaborador, mediante abertura de chamada junto ao setor de T.I. Quando este tipo de acesso for liberado, tanto o colaborador como gestor passam a ser diretamente responsáveis (custodiante) pelas informações produzidas ou manipuladas, independente de onde o colaborador se encontre fisicamente. Aplica-se integralmente às regras de segurança da informação descritas neste documento.

Em se tratando de acesso ao administrador local da máquina, o simples fato de ter sido liberado este nível de privilégio, não autoriza o colaborador a instalar softwares não autorizados ou ilegais, realizar varredura na rede corporativa, utilizar o equipamento para fins diferentes para, alterar a configuração do equipamento ou realizar intervenções que estejam fora das regras descritas nessa Política de Segurança da Informação (PSI).

8.13 USO DE MÍDIAS REMOVÍVEIS

É terminantemente proibido que os usuários utilizem e conectem dispositivos de armazenamento nos equipamentos em que realizam as atividades profissionais, exceto os usuários que necessitem de tais dispositivos por força da função.

Para a utilização de Pen-Drives, CD/DVD, HD externo e outros dispositivos similares, o(a) funcionário(a) que necessitar utilizar, deverá requerer a permissão ao(a) seu(a) gestor(a) direto. Sendo autorizado, tanto o(a) gestor(a), quanto o(a) colaborador(a), serão, em conjunto, responsáveis pela segurança da informação.

8.14 INTERNET, SOFTWARES DE COMUNICAÇÃO E MENSAGERIA:

A empresa **WTECH** disponibiliza o acesso à internet para que os colaboradores e terceiros possam desempenhar as atividades profissionais, no entanto, a fim de proteger os dados armazenados nos sistemas e portais internos, poderá monitorar todos os acessos.

O uso de sites de notícias e similares serão autorizados desde que para fins profissionais. Mas, a empresa **WTECH** salienta que os colaboradores e terceiros devem atentar-se ao direito de imagem, à Lei de Direitos Autorais, o disposto na Constituição Federal e demais dispositivos legais.

Inclusive, todas as informações da empresa **WTECH** não poderão ser divulgadas e/ou compartilhadas sem a devida autorização por escrito e assinada pela Diretoria.

É expressamente proibido:

a) Acessar sites de entretenimento;
b) Materiais de cunho sexual;
c) Baixar programas que não sejam da área profissional;
d) Acessar jogos de azar.

Por fim, todos que infringirem o disposto na presente Política, sofrerão as sanções disciplinares cabíveis, conforme a legislação pertinente.

8.15 CORREIO ELETRÔNICO E ASSINATURA:

Informações de cunho confidencial (informações sensíveis) não devem ser enviadas via e-mail para fora da organização ou até mesmo para outros colaboradores dentro da empresa, a menos que o destinatário da mensagem esteja autorizado a receber tais informações. Todos devem reconhecer que as informações transmitidas via e-mail podem conter segredos técnicos, comerciais ou informações confidenciais, e que devem ser tomadas as providências cabíveis para proteger a segurança de tais informações.

Não é permitido a utilização de e-mail particular dentro da rede corporativa (exemplo: gmail, hotmail, outlook entre outros). Exceções deverão ser tratadas à parte, para fins específicos e profissionais de interesse, e com a devida autorização do gestor responsável pelo colaborador ou terceiro, desde que não contraponha a esta política.

O correio eletrônico (e-mail) deverá conter a assinatura padrão. A empresa disponibiliza cotas específicas de e-mail, podendo sofrer revisões a qualquer instante. O uso do correio eletrônico é destinado única e exclusivamente para fins profissionais e assuntos inerentes aos negócios. A organização, o sigilo, o manuseio e o descarte são de inteira responsabilidade do usuário.

Toda conta de e-mail criada deverá ser utilizada única e exclusivamente por 1 colaborador, este responderá pelo seu correio eletrônico sempre que necessário e deverá seguir as condutas descritas nessa Política. Cada e-mail poderá ter apenas 1 zorro (apelido) ligado a ele, isso é

utilizado em casos onde algum colaborador é desligado e ainda recebe e-mails e esses devem ser direcionados para o novo colaborador.

Reserva-se o direito de monitorar qualquer conta de e-mail, a qualquer instante, com ou sem comunicação prévia, por razões legítimas de negócio, e inclusive em razão desta própria Política de Segurança da Informação (PSI) para identificar situações em que haja suspeita de atividades que violam essa política. O conteúdo da mensagem de e-mail corporativo pode ser revelado sem a permissão do usuário.

As mensagens transmitidas por este meio não devem ser profanas, vulgares, difamatórias ou embaraçosas, racial ou sexual em sua natureza.

Restrições no uso do e-mail para o uso dos serviços de e-mail, são vetados:

a) Uso de programas de computador que enviem sistematicamente uma grande quantidade de mensagens através do servidor de e-mail corporativo;
b) Forjar quaisquer informações do cabeçalho do remetente ou enviá-las anonimamente. A identificação do usuário remetente é sempre obrigatória;
c) Enviar mensagem de e-mail pelo endereço eletrônico de seu departamento para fins diferentes daquele pela qual foi criada, ou usando o nome de usuário de outra pessoa;
d) Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou suas unidades vulneráveis a ações civis ou criminais;
e) Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa concedida pelo proprietário desse ativo de informação;
f) Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas nesta política;
g) Apagar mensagens de e-mail quando qualquer uma das unidades estiver sujeita a algum tipo de investigação interna.

Ainda, são vetados:

Produzir, transmitir, baixar ou divulgar mensagem que:

h) Contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do Grupo Wtech;

i) Contenha arquivos com extensão: .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl,.reg, .dll, .inf; ou qualquer outra extensão que represente um risco à segurança da informação;

j) Contenham ameaças eletrônicas a segurança da informação, como: spam, mail bombing, vírus de computador;

k) Vise vigiar secretamente ou assediar outro usuário, colaborador, terceiros ou qualquer pessoal de forma geral;

l) Inclua imagens criptografadas ou de qualquer forma mascaradas que não façam parte do negócio ou atividade do usuário;

m) Tenha conteúdo ou caráter considerado impróprio, ilícito ou obsceno, calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;

n) Contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas pela lei;

o) Tenha fins políticos locais ou do país (propaganda política);

p) Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

Recomenda-se a utilização do chat, como ferramenta de comunicação e aumento de produtividade, devendo ser usado prioritariamente para atividades de negócio e podendo ser monitorado pela empresa e até mesmo vistoriado por direitos de verificação e auditoria.

A instalação de software de mensageria e a liberação do acesso são restritas e sua utilização deve ser justificada à área de TI. O uso de sistemas de mensageria é aceitável apenas quando for utilizado como ferramenta de produtividade para comunicação on-line, no exercício de sua função. Enquanto o uso responsável dos sistemas de mensageria é estimulado, o seu abuso deve ser evitado.

8.16 WHATSAPP

Em seu lugar, o MS Teams é a ferramenta padrão de Comunicação e Mensageria. O uso do Whatsapp é autorizado, desde que a troca de mensagens seja realizada de forma consciente, sem transmitir dados pessoais confidenciais.

8.17 EXCEÇÃO

Nos casos omissos ou divergentes do exposto na presente Política, ou seja, tratando-se de uma exceção, a solicitação deverá ser requerida junto ao setor de tecnologia e/ou setor Jurídico e só poderão ser colocados em prática após a autorização da Diretoria.

8.18 SERVIDOR DE ARQUIVOS

A empresa **WTECH** disponibiliza uma área específica para armazenamento seguro de dados e informações relativas ao negócio da empresa, com o perfil de acesso conforme a função exercida pelo usuário. Somente informações referentes às atividades profissionais do usuário deverão ser armazenadas nesta área.

A restrição de acesso é feita a nível de pastas e qualquer tentativa de acesso a uma pasta ou arquivo armazenado em outras áreas, que não sejam de interesse profissional do usuário é passível de medidas disciplinares.

Não é permitido ao usuário o armazenamento de informações de domínio da empresa em locais ou dispositivos particulares do(a) colaborador(a).

8.19 IMPRESSORAS

O uso das impressoras deve seguir algumas regras:

a) É proibida a impressão de documentos de cunho pessoal (exceto se houver autorização do gestor) e/ou ilegal;
b) A configuração e manutenção das impressoras só podem ser realizadas pela equipe de T.I ou empresa terceirizada que cuida da locação dos equipamentos;
c) A instalação das impressoras deverá ser realizada preferencialmente através do servidor de impressão;

d) O gestor de cada departamento será o responsável pela impressora localizada na sala, inclusive poderá responder a questionamentos como impressões excessivas.

8.20 ARQUIVOS E PROGRAMAS

Todos os sistemas e programas utilizados pela empresa **WTECH** são licenciados conforme a versão adequada para o desempenho das atividades de seus colaboradores, sendo, portanto, proibido que os colaboradores baixem, gravem ou instalem qualquer tipo de arquivo ou programa falsificado.

Sobre hipótese alguma é permitido ao usuário instalar programas de computador de origem desconhecida ou não devidamente licenciada, tornando-se crime de violação das leis de Copyright (fere os direitos autorais do autor do software).

Caso o(a) colaborador(a) descumpra a norma interna, estará sujeito(a) às medidas disciplinares previstas na presente Política.

8.21 BACKUP

Visando a segurança e recuperação dos dados, a empresa **WTECH** possui uma Política específica acerca do BACKUP (cópia de segurança), estando preparada para recuperar quaisquer dados de forma íntegra caso ocorra algum incidente.

As normas, procedimentos e rotinas de backup estão descritos no **POP 017 Backup.**

8.22 USO WIFI

O uso do Wifi nos celulares cedidos pela empresa será configurado pelo setor de T.I, somente após devidamente configurado o usuário terá acesso à internet.

No caso de terceiro visitante, somente terá acesso ao Wifi da empresa mediante utilização de "voucher" com prazo determinado para sua utilização.

Por fim, todas as medidas de segurança necessárias à proteção de seus equipamentos (antivírus, firewalls e afins), sistemas e arquivos contra atuação indevida e invasões não autorizadas de outros usuários de internet serão realizadas previamente.

8.23 MONITORAMENTO - RASTREABILIDADE E CÂMERAS DE SEGURANÇA

A empresa **WTECH** poderá implantar sistemas de monitoramento e rastreamento para que as respostas frente aos incidentes de segurança sejam rápidos e precisos, além disso, visando a segurança, monitoramento e rastreabilidade das informações, a empresa poderá:

a) Implantar sistemas de monitoramento nas estações de trabalho, servidores, e-mails, dispositivos móveis cedidos pela empresa, a fim de que possa identificar os usuários e os acessos efetuados;
b) Tornar acessível as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior) ou por determinação do Comitê de Segurança da Informação e Privacidade de Dados;
c) Realizar, a qualquer tempo, inspeção física e lógica nas máquinas de sua propriedade, bem como instalar sistemas de proteção para garantir a proteção dos dados.

Alguns procedimentos são indispensáveis e a empresa WTECH realizará sempre que possível:

i. Todos os registros de login deverão ser guardados, quando possível, de modo a auxiliar na identificação de não conformidade de segurança para caráter corretivo, legal e de auditoria para períodos de análise sempre o menor possível;
ii. O ambiente poderá ser monitorado, manual ou sistemicamente afim de detectar ou antever incidentes ou problemas que gerem riscos para o negócio;
iii. Os sistemas corporativos, quando possível, devem conter rotinas que permitam a rastreabilidade das informações incluídas, alteradas ou excluídas.

9. MESA E TELA LIMPA EXPOSIÇÃO DE INFORMAÇÕES

Para reduzir o risco de acesso não autorizado, perda, furto e dano da informação durante e fora do horário normal de trabalho, é responsabilidade de cada colaborador prezar pela guarda dos dados que utiliza, seguindo as regras impostas.

É proibido deixar qualquer informação impressa sobre as mesas ou a tela ligada enquanto está ausente do local.

Portanto, deve-se seguir as regras abaixo:

a) Todos os documentos em formato físicos ou armazenados em dispositivos eletrônicos, não podem permanecer sobre a mesa sem necessidade. Caso estas informações não estejam em uso é recomendável que sejam armazenados em armários ou gavetas com chave;
b) Informações classificadas como confidenciais e sensíveis ao negócio da organização devem ser trancadas em local separado e seguro (Exemplo: armário com chave ou cofre à prova de fogo);
c) Anotações, como recados ou lembretes de assuntos confidenciais não devem ser deixados amostra, em cima da mesa, colados em paredes ou monitor do computador;
e) O armazenamento de documentos classificados como confidenciais deve ser feito em armários com fechadura;
f) O descarte de documentos impressos, deve contemplar a destruição dos mesmos, sempre que possível através de máquina fragmentadora;
g) É recomendável a leitura de documentos diretamente pela tela do computador, sempre que possível, evitando impressões desnecessárias;
h) Documento classificado como confidencial, quando impresso, deve ser retirado da impressora imediatamente;
i) Sempre que for necessário a solicitação de documentos de outro departamento, realizar a devolução assim que possível;
j) Todas as estações de trabalho de uso individual ou comum, devem ser bloqueadas durante a ausência do usuário;
k) Em todos computadores e notebooks utilizar a proteção de tela com login e senha para acesso;
l) Todos cadernos/agendas para anotações devem ser mantidos em gaveta trancada;

m) Mídias (ex.: CDs, pen-drives) devem ser desconectados do computador imediatamente após o uso;

n) Deve-se manter sempre armários e gavetas fechadas e retirar as chaves da fechadura;

o) Não se deve colocar copos abertos de água, suco, refrigerante ou café sobre a mesa de trabalho;

p) As salas devem ser mantidas fechadas sempre que terminar o expediente;

q) A área de trabalho deve ser mantida sempre organizada;

r) Todos os documentos eletrônicos devem ser mantidos na rede. Para tentar evitar a exposição de informações, as máquinas que se encontram no domínio, (Active Directory) terão seu bloqueio de tela após 10 minutos de inatividade, tendo que o usuário informar sem login e senha para desbloqueio.

10. GESTÃO DOS ATIVOS DE INFORMAÇÃO E CLASSIFICAÇÃO

Para que o controle interno seja adequado e organizado, a empresa **WTECH** classificou as informações e a gestão de seus ativos, para que se torne mais fácil a implementação dos controles.

Os controles baseiam-se em alguns pilares, tais como:

• Identificação dos ativos e sua atualização mensal;

• Classificação das informações quanto a sua sensibilidade (confidencialidade), criticidade, valor (documental ou estratégico) e requisitos legais, identificando a forma adequada. Estas informações devem estar documentadas no Registro de Controle de Informações Documentadas, documento a ser criado e desenvolvido pelo setor de tecnologia;

• Aplicação de medidas de proteção dos ativos de forma compatível com o risco e com o valor (documental ou estratégico) da informação para os negócios da companhia. As informações devem ser classificadas sistematicamente.

11. IDENTIFICAÇÃO DAS INFORMAÇÕES DOCUMENTADAS

As informações armazenadas e movimentadas pela empresa WTECH serão classificadas em um documento denominado "**Registro de Controle de Informações Documentadas"**, e serão avaliados os níveis de criticidade, sensibilidade, valor e requisitos legais.

- **Criticidade:** Define o nível de impacto que pode advir da divulgação ou uso indevido da informação. Pode ser classificada como Alto, Média ou Baixa.
- **Sensibilidade:** Refere-se à informação de uso Restrito, Público ou Confidencial.
- **Valor:** Define se a informação é apenas Documental ou Estratégica.
- **Requisitos Legais:** Relaciona-se a uma lei ou normativa. Para efeito desta política, todas as informações classificadas com a Sensibilidade "Confidencial" devem ser identificadas no rodapé dos respectivos documentos ao serem manuseados e transportados.

12. PARTES EXTERNAS E CONTRATOS

Os contratos, Termos e quaisquer outros documentos burocráticos, devem preservar a segurança da informação considerando que:

a) As cláusulas contratuais devem ser avaliadas criteriosamente pelo Departamento Jurídico, tendo em vista que a aplicação da Lei Geral de Proteção de Dados (LGPD) deverá ser seguida integralmente em todas as negociações e fechamentos;
b) O setor jurídico deverá realizar o acordo de confidencialidade com todos os funcionários e terceiros envolvidos.

13. CONTINUIDADE DO NEGÓCIO, CONSCIENTIZAÇÃO, TREINAMENTO E PRIORIZAÇÃO DAS AÇÕES VOLTADAS A SEGURANÇA DA INFORMAÇÃO

Todas as informações que estão sob a posse da empresa WTECH serão analisadas e avaliadas através de um levantamento do grau de relevância entre os processos ou atividades para compor o escopo da contingência para a segurança da informação, com as seguintes características:

a) Disponibilidade dos sistemas, dispositivos redundantes e meios para garantir a continuidade da operação dos serviços críticos de maneira oportuna;

b) Elaboração de procedimentos de cópia de segurança (backup) e de recuperação (restore) documentados e mantidos atualizados, testados regularmente, garantindo a integridade e disponibilidade das informações;
c) Definir e executar a guarda de informações local seguro e segregado.

Por ser uma questão corporativa que envolve os aspectos físicos, tecnológicos e humanos que sustentam a operação do negócio, torna-se condição imprescindível o envolvimento e apoio da alta direção nos trabalhos voltados à gestão da segurança da informação. Entende-se por apoio não só a sensibilização e a percepção adequada dos riscos e os problemas associados, mas também a consequente priorização das ações voltadas a:

• Existência de evidências que demonstrem a conscientização dos usuários quanto a necessidade da segurança das informações e aspectos previstos na **WTECH;**
• A capacitação dos usuários em relação à correta e eficiente utilização dos recursos de acordo com as normas e políticas em vigor;
• A gestão da PSI **WTECH é** executada por profissional do setor Jurídico (terceirizado) e por colaboradores devidamente capacitados para esta função.

14. COMITÊ DE SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

Cabe ao Comitê de Segurança da Informação e Privacidade de Dados:

a) Propor melhorias, alterações e ajustes da Política de Segurança da Informação (PSI);
b) Propor investimentos relacionados à segurança da informação com o intuito de minimizar os riscos;
c) Classificar e reclassificar o nível de acesso às informações sempre que necessário;
d) Avaliar incidentes de segurança e propor ações corretivas;
e) Manter ações preventivas e educativas de segurança;
f) Definir estratégias para implantação dessa política e das demais que relacionadas a segurança da informação e privacidade de dados;
g) Promover a fiscalização da aplicação das normas e da política de segurança da informação (PSI);

h) Propor recursos necessários à implementação das ações de segurança da informação;

i) Propor a realização de análise de riscos e mapeamento de vulnerabilidades nos ativos;

j) Propor a abertura de sindicância para investigar e avaliar os danos decorrentes de quebra de segurança da informação;

k) Sugerir convite ou contratação de profissionais externos, de relevante importância na área de segurança da informação, para auxílio em questões que assim o exijam, sob a condição de confidencialidade;

l) Propor ações de treinamento e atualização necessárias;

m) Dar resposta a qualquer incidente de segurança relevante;

n) Manter comunicação com outros comitês da empresa;

O Comitê de Segurança da Informação e Privacidade de Dados deverá ser composto por, no mínimo, um colaborador das seguintes áreas: RH, Jurídico e TI. O Comitê reunir-se-á sempre que for necessário deliberar sobre algum incidente grave ou definição relevante.

15. INCIDENTES DE SEGURANÇA DE INFORMAÇÃO

Considera-se um incidente de segurança da informação qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação, aplicações ou redes de computadores.

Em geral, qualquer situação em que um ou mais ativos da informação estão sob risco, é considerado um incidente de segurança da informação.

Considera-se um incidente de segurança da informação qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança de sistemas de computação, aplicações ou redes de computadores. Em geral, qualquer situação em que um ou mais ativos da informação estão sob risco, é considerado um incidente de segurança da informação. Na **WTECH**, os incidentes devem ser documentados via **RNC (Registro de Não Conformidade)** para a retomada o mais breve possível do(s)serviço(s) prejudicado(s) e a posterior análise da causa raiz e ações para mitigação posterior. Para que os incidentes de segurança da informação possam ser notificados o mais rapidamente possível quando de sua ocorrência, a **WTECH** possui canais de comunicação formais,

acessíveis, de fácil utilização, sempre disponíveis e que, preferencialmente, preservam a identidade da pessoa que informou o incidente. Os canais disponíveis são:

O sistema de chamados service desk. A comunicação dos incidentes deve envolver, além do setor de tecnologia da informação, os proprietários (owners) da(s) informação(ões).

15.1 EVENTOS VERSUS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

A fim de distinguir a diferença entre "eventos" e "incidentes de segurança", nos itens abaixo, encontram-se as explicações detalhadas, para que o usuário tenha conhecimento e entenda a diferença entre os conceitos.

15.1.1 EVENTOS

Qualquer ocorrência dentro da área do T.I que tenha relevância para a gestão dos serviços entregues ao cliente, são considerados "eventos", além disso, qualquer mudança ou alteração em configurações ou sistemas são chamados de "eventos".

Exemplos de eventos (não exaustivo):

• Um usuário logou no sistema;
• Um backup agendado não ocorreu;
• Excesso de ligações por engano para o Service Desk, sem autorização;
• Qualquer outro que tenha relevância para quem está gerindo os serviços de TI;

O evento tem diversas naturezas, sendo categorizadas na seguinte ordem:

- Por nomenclaturas como normal, não usual, exceção, alerta;
- Por cores como vermelho, laranja, amarelo e verde;
- Por criticidade como sendo crítico, tendência de ser crítico, alerta e normal.

O T.I controla e acompanha os eventos para que esteja ciente do que está acontecendo e para que evite problemas maiores, como por exemplo os incidentes de segurança da informação.

15.1.2 INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Sempre que for detectada alguma quebra na segurança da informação, o problema é tratado como "incidente de segurança", diferentemente dos eventos mencionados anteriormente, que não chegam a gerar um rompimento na segurança dos dados, apenas informam as alterações e notificam.

Quando o setor de T.I detecta qualquer alteração nos sistemas, avalia-se a gravidade através das classificações e dependendo do que for constatado, poderá ser tratado como "evento" ou "incidente".

Após avaliado o dano, a gestão de incidentes da Segurança da Informação entra em ação, a fim de garantir o tratamento adequado, garantir a segurança dos dados identificados e minimizar quaisquer efeitos adversos.

15.2 DA GESTÃO DE INCIDENTES - SEGURANÇA DA INFORMAÇÃO

Conforme mencionado anteriormente, a gestão de incidentes realiza o tratamento adequado das informações, garante que tais incidentes sejam corretamente avaliados e por fim, minimiza os efeitos adversos.

Em caso de vulnerabilidades, o setor competente deverá reportar e ajudar a prevenir futuras ocorrências, através da manutenção contínua dos sistemas e softwares de segurança.

A gestão para os incidentes de segurança da informação será detalhada em documento próprio denominado: "Gestão de Incidentes de Segurança da Informação".

15.3 RESPONSABILIDADE SOBRE A NOTIFICAÇÃO DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todos os usuários são responsáveis pelos seus atos e principalmente em relação à notificações e como formalizá-las em caso de necessidade. Quaisquer fragilidades deverão ser informadas imediatamente ao setor de T.I da empresa **WTECH** e/ou setor Jurídico.

No entanto, as averiguações dos incidentes de segurança só poderão ser realizadas por pessoas autorizadas que possuem a competência para agir e que entendem o procedimento a ser seguido.

Qualquer parte que infringir as orientações descritas na presente Política, poderá sofrer as sanções legais.

16. DOS DEVERES E RESPONSABILIDADES

Todos os envolvidos com a empresa **WTECH,** sejam colaboradores, gestores, visitantes ou prestadores de serviços, possuem a responsabilidade de comunicar o setor Jurídico e/ou setor de T.I sobre quaisquer irregularidades ou desvios do descrito na presente Política.

16.1 DEVERES E RESPONSABILIDADES DOS COLABORADORES

Todos os colaboradores devem manter o sigilo absoluto sobre os dados que possuem acesso, principalmente informações de cunho confidencial, e, portanto, devem preservar a integridade de todas as informações, independentemente do setor em que elas estejam inseridas.

Ao descumprir as determinações deste Política, os colaboradores poderão sofrer as sanções disciplinares cabíveis, conforme a legislação vigente.

16.2 DEVERES E RESPONSABILIDADES DOS DIRETORES E GESTORES

Além dos colaboradores, todos os gestores e diretores devem manter sigilo referente às informações obtidas e principalmente devem gerenciar o cumprimento da presente Política, a fim de identificar a prática de desvios cometidos por seus subordinados. Ao identificar tais desvios, devem adotar medidas e ações corretivas adequadas.

Todas as ações tomadas pelos gestores e diretores devem ser informadas ao setor jurídico competente, a fim de que avalie a regularidade e adequação.

16.3 DEVERES E RESPONSABILIDADES DOS PRESTADORES DE SERVIÇOS

a) Torna-se indispensável a preservação e integridade dos dados, portanto, é necessário que haja o sigilo absoluto sobre as negociações, operações, dados, informações, materiais, documentos, arquivos, procedimentos internos, especificações técnicas e comerciais, inovações e aperfeiçoamento tecnológicos e comerciais, incluindo todos os recursos de processamento de informações manuais ou sistêmicos que tenha ciência, acesso o que lhe tenha sido confiado, mesmo que não tenha sido previsto no contrato entre as partes;

b) Prever nos contratos, cláusulas que contemplem a responsabilidade dos terceiros ou prestadores de serviço no cumprimento da Política de Segurança da Informação (PSI).

c) Aderir o cumprimento das atividades do dia a dia, as regras e normas da Política de Segurança da Informação (PSI), independente onde o recurso esteja alocado.

16.4 DEVERES E RESPONSABILIDADES DOS VISITANTES

a) Cumprir as orientações recebidas por parte dos colaboradores da empresa **WTECH,** quando da visita física;

b) Não divulgar, utilizar ou repassar nenhuma informação confidencial ou dado pessoal;

c) Não se apropriar de nenhum dado pessoal ou informação;

d) Informar a empresa **WTECH** em caso de necessidades relacionadas ao tema deste documento.

17. DAS PENALIDADES

O descumprimento total ou parcial da presente Política, impõe aos envolvidos medidas disciplinares e legais, conforme o nível de criticidade e dano causado.

Conforme já informado nos tópicos anteriores, os colaboradores são responsáveis pelo tratamento e sigilo das informações que possuem acesso, e, portanto, ao violar ou infringir tal integridade e confidencialidade, estão sujeitos a penalidades administrativas e/ou legais.

No caso dos colaboradores, ao agir em desacordo com o pactuado no presente Instrumento, poderão sofrer as seguintes sanções:

a) **ADVERTÊNCIA VERBAL:** Sendo a primeira vez em que o(a) colaborador(a) age em desacordo com o disposto na presente Política, este será comunicado verbalmente por seu gestor imediato e/ou setor jurídico, que está infringindo as normas da Política de Segurança da Informação (PSI) e será recomendado a leitura desta Norma; e o seu devido cumprimento.

Parágrafo único: A advertência verbal será para os casos considerados não críticos, ou seja, nos casos em que não foi constatado nenhum dano gravíssimo à empresa e envolvidos.

Situações tidas como graves poderão ensejar a aplicação de outras medidas na esfera da legislação trabalhista, a critério do Departamento de Compliance da empresa, e diante da mensuração do provável dano.

b) **ADVERTÊNCIA FORMAL E ESCRITA:** Após a advertência verbal, sendo reincidente, o(a) colaborador(a) receberá a primeira notificação escrita, informando o descumprimento da norma, com a indicação precisa da violação cometida, e ratificação da necessidade de cumprimento do disposto na Política.

Em caso de reincidência de descumprimento da Política de modo geral, sendo ou não a mesma falta/infração praticada; O gestor, diretor e/ou setor de Compliance, além de replicar a advertência

poderá tomar medidas na esfera da legislação trabalhista, de acordo com a gravidade da falta praticada pelo colaborador.

c) **INFRAÇÕES DE TERCEIROS**

As infrações cometidas por terceiros em relação à Política de Segurança da Informação (PSI), terão as suas medidas administrativas e/ou penalidades cabíveis aplicadas, conforme o contrato que rege as relações entre as partes.

18. CRIPTOGRAFIA

Os **controles criptográficos** são considerados indispensáveis e serão utilizados para assegurar, dentre outros: **a confidencialidade, a integridade e a autenticidade de informações sensíveis ou críticas que se encontrem armazenadas ou em transporte físico ou eletrônico.** Os controles criptográficos auxiliam a identificar os usuários e serviços, através de sistemas informatizados.

A escolha dos tipos de algoritmos, assim como a definição de que tipo de controle criptográfico é apropriado para cada propósito e processo de negócio, será realizado pela empresa de tecnologia contratada e tomará como base, sempre que possível, o resultado do processo de gerenciamento de riscos de segurança da informação.

Tais registros de controles, quando forem aplicáveis, seus parâmetros e sua aplicação na proteção de informações classificadas serão mantidos e comunicados aos proprietários e custodiantes de ativos. Os documentos de sensibilidade alta, quando armazenadas os dispositivos móveis (notebook, tablet, smartphone entre outros) ou mídias removíveis (cd, dvd, pen-drivers entre outros) deverão ser criptografados para evitar a sua divulgação indevida em caso de perda ou furto do equipamento ou da mídia.

É de responsabilidade dos proprietários e custodiantes de tais informações, aplicarem adequadamente os recursos criptográficos para a proteção da informação sobre sua custódia, em conformidade com as determinações legais mencionadas neste documento.

Indispensáveis que as partes verifiquem com o setor jurídico, antes de transferir informações cifradas ou controles de criptografia para além das fronteiras jurisdicionais, tendo em vista que deve-se analisar a conformidade com as legislações e regulamentações vigentes em outros países.

19. CONSIDERAÇÕES FINAIS

As dúvidas decorrentes de fatos não descritos nesta Política de Segurança da Informação (PSI) deverão ser encaminhadas ao setor Jurídico para avaliação e decisão junto ao Comitê Gestor de Segurança da Informação.

Esta Política de Segurança da Informação (PSI) entra em vigor a partir da data de publicação, e pode ser alterada a qualquer tempo, por decisão dos sócios, mediante o surgimento de fatos relevantes que apareçam ou não tenham sido contemplados neste documento.

A atualização da Política também ocorrerá nos casos em que houver modificação legislativa.

Nº REVISÃO	DATA	ALTERAÇÃO	ELABORADOR	APROVADOR
01	28/05/2021	Emissão da Política	Jéssica Maria Machado	Diretoria
02	25/05/2022	Atualização da Política	Jéssica Maria Machado	Diretoria
03	30/01/2023	Atualização da Política	Jéssica Maria Machado	Diretoria

TERMO DE RESPONSABILIDADE

Eu, _____, devidamente registrado(a) como colaborador(a) ou prestador(a) de serviço da WTECH, declaro ter conhecimento da Política de Segurança das Informações Wtech – PSI WTECH , comprometendo-me a cumpri-las de forma plena e integral, estando sujeito a ações disciplinares definidas pelo Depto. de Recursos Humanos.

_____ de _____ de _____.

(Data)

_____

Assinatura