PSI – Política de Segurança da Informação

Sumário

Controle do Documento

Histórico de Aprovações

Aprovadores	Data
Conselho Diretivo	05/09/2018
Conselho Diretivo	16/07/2019
Conselho Diretivo	11/09/2019

Histórico de Revisões

Versão	Data	Resumo das Alterações	Alterado Por
01	30/08/2018	Criação do documento	Adeilson Brito
02	10/07/2019	Incluído o item 5.8 Aplicativo de Comunicação	Adeilson Brito
03	11/09/2019	Revisão anual da PSI	Adeilson Brito

1. Introdução

A Política de Segurança da Informação, também referida como PSI, é o documento que orienta e estabelece as diretrizes corporativas da Trust Image para a proteção dos ativos de informação e a prevenção de responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da organização.

A presente PSI está baseada nas recomendações propostas pela norma ABNT NBR ISO/IEC 27002:2013, reconhecida mundialmente como um código de prática para a gestão da segurança da informação, bem como está de acordo com as leis vigentes em nosso país.

2. Objetivos

Estabelecer diretrizes e princípios que permitam aos colaboradores, clientes e fornecedores da Trust Image seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e de proteção legal da empresa e do indivíduo.

Preservar as informações da Trust Image ou que estejam sob sua responsabilidade quanto à:

- **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- **Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3. Responsabilidades

As diretrizes e princípios aqui estabelecidos deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte. Dessa forma, é missão e responsabilidade de cada colaborador e prestador de serviços observar e seguir as diretrizes, princípios e procedimentos estabelecidos para o cumprimento da presente Política de Segurança da Informação. É imprescindível que cada pessoa compreenda o papel da segurança da informação em suas atividades diárias.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, não devendo o colaborador ter expectativa de sigilo em sua utilização.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

4. Diretrizes Gerais

4.1 Proteção das Informações (Propriedade)

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela Trust Image pertence à referida empresa, devendo ser armazenada e protegida quanto ao seu acesso e uso.

Independentemente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada, a informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada. Dessa forma, o acesso às informações de propriedade da Trust Image ou que estejam sob sua responsabilidade deve ser direcionado exclusivamente ao desempenho das atividades e objetivos da empresa.

É diretriz que toda informação de propriedade do da Trust Image ou que estejam sob sua responsabilidade seja protegida de riscos e ameaças que possam comprometer a confidencialidade, integridade ou disponibilidade destas.

4.2 Informações Confidenciais

São consideradas informações confidenciais, para os fins desta Política, quaisquer informações consideradas não disponível ao público ou reservadas, dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas pela Trust Image e/ou obtidas em decorrência da execução das atividades prestação de serviços.

O colaborador ou prestador de serviços que receber as informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar quaisquer cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma. Nenhuma das informações confidenciais podem ser repassadas para terceiros sem consentimento da Trust Image. Qualquer revelação das informações confidenciais deverá estar de acordo com os termos e condições estabelecidos pela Trust Image. As informações confidenciais somente poderão ser utilizadas para fins de execução das atividades profissionais.

Todos os colabores e prestadores de serviços são responsáveis pela observância deste item.

4.3 Conversas em Locais Públicos

Todos os colabores e prestadores de serviços devem fazer adoção da prática de não abordagem e não discussão em ambientes públicos e áreas expostas de assuntos confidenciais relacionados ao trabalho.

4.4 Classificação da informação

Para que as informações sejam adequadamente protegidas, cabe ao colaborador realizar a classificação no momento em que for gerada a informação, para garantir a devida confidencialidade, conforme com a lista a seguir:

- **Informação pública:** informação que pode ou deve ser tornada disponível para distribuição pública. Sua divulgação não causa qualquer dano à empresa.

- **Informação interna:** informação que pode ser acessada apenas por colaboradores da empresa, enquanto estiverem desempenhando atividades profissionais. Sua divulgação não autorizada ou acesso indevido podem causar impactos à empresa.

- **Informação confidencial:** informação exclusiva a quem se destina. Requer tratamento especial. Contém dados pessoais, sensíveis e/ou sigilosos, que, se divulgados, pode causar grave impacto (financeiro, de imagem ou operacional) ao negócio da organização.

4.5 Contratação de Colaboradores e Prestadores de Serviço

A responsabilidade em relação à segurança da informação deve ser comunicada na fase de contratação dos colaboradores. Todos os colaboradores devem ser orientados sobre os procedimentos de segurança, bem como o uso correto dos ativos, a fim de reduzir possíveis riscos. Eles devem assinar um termo de responsabilidade concordando expressamente com esta PSI.

Deverá constar em todos os contratos da Trust Image o anexo de Acordo de Confidencialidade ou Cláusula de Confidencialidade, em consonância com a presente Política de Segurança da Informação, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela empresa. O Acordo de Confidencialidade ou Cláusula de Confidencialidade incluirá, obrigatoriamente, o compromisso de sigilosidade e confidencialidade mesmo após o desligamento ou rescisão contratual.

É diretriz promover a ciência e o conhecimento de todo material referente à segurança da informação, disponibilizado pela empresa.

Em casos de desligamento, rescisão contratual ou término do contrato, a área de TIS (Tecnologia de Infraestrutura e Segurança) deve desativar a conta de usuário (login) do colaborador ou prestador de serviço em todos os sistemas e ambientes da Trust Image, promovendo o bloqueio imediato dos acessos aos recursos tecnológicos.

É de responsabilidade dos profissionais de nível hierárquico superior pela supervisão da conduta e do comportamento de seus subordinados diretos e indiretos, identificando as ocorrências que possam comprometer a segurança da informação.

4.6 Comunicação, Conscientização e Treinamento em SI - Segurança da Informação

Para a uniformidade da informação, a PSI deverá ser comunicada a todos os colaboradores e prestadores de serviços da Trust Image a fim de que a política seja cumprida dentro e fora da empresa.

Com a intenção de aumentar a segurança da informação, de modo que tal ativo e os recursos tecnológicos sejam usados de maneira apropriada e segura, devem ser desenvolvidas campanhas e treinamentos periódicos para a conscientização e capacitação dos usuários quanto às ameaças (vírus, interceptação de mensagens e dados, grampos e fraudes e tentativas que ensejam o roubo de senhas, etc) que possam afetar ou ameaçar a segurança das informações da empresa.

4.7 Uso Aceitável dos Recursos de TI

O uso correto e responsável dos recursos de TI deve ser aplicado a todos os colaboradores e prestadores de serviços da Trust Image. Somente atividades lícitas, éticas e administrativamente admitidas devem ser realizadas, pelo usuário, no âmbito da infraestrutura de TI, ficando os transgressores sujeitos às medidas administrativas e legais cabíveis.

Os equipamentos de informática e comunicação e sistemas devem ser utilizados pelos colaboradores e prestadores de serviço apenas para a realização das atividades profissionais.

Apenas os equipamentos e software disponibilizados e/ou homologados pela área de TIS (Tecnologia de Infraestrutura e Segurança) podem ser instalados e conectados à rede corporativa. Dessa forma, equipamentos particulares/privados, como computadores ou qualquer dispositivo portátil que possa armazenar e/ou processar dados, não devem ser usados para armazenar ou processar informações relacionadas com o negócio, nem devem ser conectados às redes da empresa.

O armazenamento de informações deve acontecer nos servidores da rede corporativa, em áreas protegidas separadas especificamente para esse fim.

4.7.1 Atividades Não Permitidas

A listagem a seguir elenca as práticas e atividades NÃO permitidas por esta PSI quanto ao uso dos recursos de TI:

- Conectar, na rede da empresa, equipamentos não autorizados e não homologados pela área de TIS (Tecnologia de Infraestrutura e Segurança);
- Instalar e usar sistemas e aplicações não autorizados e não homologados pela área de TIS (Tecnologia de Infraestrutura e Segurança);
- Alterar nomes padronizados dos ativos;
- Abrir ou executar arquivos de origem desconhecida;
- Introduzir códigos maliciosos nos sistemas de TI;

- Revelar códigos de identificação, autenticação e autorização de uso pessoal (conta, senhas, chaves privadas etc) ou permitir o uso por terceiros de recursos autorizados por intermédio desses códigos;
- Tentar interferir desautorizadamente em um serviço, sobrecarregá-lo ou, ainda, desativá-lo, inclusive aderir ou cooperar com ataques de negação de serviços internos ou externos;
- Alterar registro de evento dos sistemas de TI;
- Modificar cabeçalho de qualquer protocolo de comunicação de dados;
- Obter acesso não autorizado, ou acessar indevidamente dados, sistemas ou redes, incluindo qualquer tentativa de investigar, examinar ou testar vulnerabilidades nos sistemas de TI;
- Monitorar ou interceptar o tráfego de dados nos sistemas de TI, sem a autorização de autoridade competente;
- Violar medida de segurança ou de autenticação, sem autorização de autoridade competente;
- Compartilhar conta de correio eletrônico corporativo;
- Acessar e divulgar informações que contenham material obsceno, apologia ao fanatismo, práticas religiosas, político partidário, qualquer forma de discriminação, bem como de material que, explícita ou implicitamente, se refira à conduta imoral;
- Fazer cópias de materiais da internet, inclusive desenhos, artigos, gráficos e fotografias, sem autorização do proprietário ou citação da fonte;
- Alimentar-se próximo aos servidores de rede e estações de trabalho;
- Fazer cópia não autorizada de softwares adquiridos ou desenvolvidos pela Trust Image.

5. Diretrizes Específicas

5.1 Controle de Acesso Lógico

Para cada colaborador é fornecida uma conta de usuário (login e senha), de uso individual e intransferível, para acesso aos sistemas e recursos de TIC da Trust Image.

O colaborador é responsável pelo uso e o sigilo de sua conta de usuário (login e senha), não sendo permitido compartilhá-la, divulgá-la ou transferi-la a terceiros.

Os usuários dos recursos de TI devem utilizar sempre senhas fortes, difíceis de serem deduzidas e descobertas.

Os usuários dos recursos de TI devem utilizar sempre novas senhas, realizando a troca periódica.

Em caso suspeita de exposição indevida do ambiente de TI, todas as senhas de acesso devem ser imediatamente alteradas.

Caso um colaborador suspeite do comprometimento da sua senha, então o colaborador tem a responsabilidade de alterá-la imediatamente.

O acesso às informações confidenciais ou restritas serão permitidas apenas quando uma necessidade de trabalho tiver sido identificada e tal acesso aprovado pelo responsável.

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser providos com base nos perfis de trabalho, de acordo com a necessidade para o cumprimento das funções, ou mediante solicitação feita pelo proprietário ou responsável da informação envolvida.

Acessos desnecessários ou com poder excessivo devem ser imediatamente retirados.

A concessão de acesso às informações e sistemas deve ser sempre autorizada com base na regra de mínimo acesso necessário para o desempenho da função.

Os privilégios e acessos concedidos para todos os usuários dos serviços da rede deverão ser revistos periodicamente.

Compete à Gerência da área de TIS (Tecnologia de Infraestrutura e Segurança) a elaboração de procedimento específico tratando da criação, proteção e uso de senhas.

Compete à Gerência da área de TIS (Tecnologia de Infraestrutura e Segurança) a elaboração de procedimento específico tratando da solicitação, aprovação, inclusão, alteração e exclusão de acessos.

5.2 Mesa Limpa e Tela Limpa

Nenhuma informação confidencial ou restrita da Trust Image deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não, usando-se, para tanto, a aplicação da prática de mesa limpa e tela protegida.

Os papéis contendo informações confidenciais ou restritas não devem ficar expostos em impressoras, fax, *scanner*, pátios, telas de computadores, áreas comuns, locais de trânsito de pessoas, elevador, refeitório e nas salas de reunião.

Ao usar uma impressora coletiva, quando manuseando informações confidenciais ou restritas, deve-se recolher o documento impresso imediatamente.

Aos colaboradores compete garantir que todas as informações confidenciais ou restritas, seja em papel ou em forma eletrônica, estarão seguras no espaço de trabalho ao final do expediente diário ou quando se ausentarem.

Todos os colaboradores são responsáveis por realizar o bloqueio com senha ao se distanciarem das estações de trabalho que estiverem usando. Dessa forma, quando os equipamentos de usuário não estiverem em uso deverão ser imediatamente bloqueados ou desligados.

As estações de trabalho devem ser completamente desligadas no final do expediente de trabalho.

Deve ser adotada a prática de exclusão de informações críticas e sensíveis das lixeiras das estações de trabalho.

Deve ser adotado o descarte apropriado de documentos contendo informações confidenciais ou restritas mediante uso de fragmentadoras.

5.3 Controle de Acesso Físico

Aplicação obrigatória de controles, equipamentos e procedimentos apropriados com o objetivo de administrar o acesso físico ao perímetro de segurança da empresa, disciplinando a circulação de pessoas, materiais e equipamentos, de modo a prevenir o acesso não autorizado, danos e interferências nas informações.

Para efeitos desta PSI define-se perímetro crítico o ambiente destinado a armazenar ativos de TIC (Tecnologia da Informação e Comunicação), cuja interrupção não programada do funcionamento ou a indisponibilidade comprometem significativamente as atividades da empresa.

O acesso aos perímetros críticos é restrito aos colaboradores da área de Tecnologia da Informação e Comunicação autorizados pela Gerência da área de TIS (Tecnologia de Infraestrutura e Segurança).

A responsabilidade pelo controle de acesso aos perímetros críticos é da Gerência da área de TIS (Tecnologia de Infraestrutura e Segurança).

No tocante ao controle de acesso aos perímetros críticos:

- O acesso será realizado por meio de senha, controle biométrico ou cartão eletrônico.
- A guarda dos cartões de acesso e/ou é de responsabilidade dos servidores designados, sendo expressamente proibido o empréstimo para qualquer outra pessoa.
- Serviços de terceiros deverão ser agendados previamente, com identificação da pessoa que executará o serviço e o detalhamento da atividade a ser realizada no local.
- Todo acesso realizado por terceiros será acompanhado por colaborador designado pela Gerência da área de TIS (Tecnologia de Infraestrutura e Segurança).

Todas as portas de acesso aos perímetros críticos deverão permanecer trancadas, mesmo durante o horário de expediente

É vedado o uso do espaço interno dos perímetros críticos para o armazenamento de quaisquer tipos de equipamentos ou itens de consumo que não estejam em utilização.

Os perímetros críticos devem estar protegidos contra a falta de energia elétrica e outras interrupções causadas por falhas, além de ter uma correta manutenção para assegurar a sua contínua integridade e disponibilidade.

Qualquer evento de quebra de segurança associado ao acesso ou a tentativa de acesso não autorizado aos perímetros críticos deve ser imediatamente reportado à área de TIS (Tecnologia de Infraestrutura e Segurança).

5.4 Backup

Compete à Gerência da área de TIS (Tecnologia de Infraestrutura e Segurança) a adoção e elaboração de procedimentos formais de backup (cópia de segurança) e restore (recuperação) para todo o acervo de software e dados sob a responsabilidade da Trust Image, de acordo com o perfil e as especificidades de utilização, devendo ser adotado, inclusive, o monitoramento e inspeção sistemática dos registros de ocorrências das rotinas de backup.

A frequência, o tipo e o tempo de retenção dos backups gerados deverão estar definidos no procedimento de backup e restore, observando as necessidades de negócio da Trust Image.

Adoção de procedimentos para efetuar testes de recuperação, de acordo com o perfil e a especificidade da cópia de segurança.

Disponibilização de local adequado e seguro para o armazenamento de mídias originais de softwares e aplicativos adquiridos, juntamente com as versões definitivas e aprovadas dos sistemas de informação desenvolvidos e em produção.

Guarda dos backups em local e ambiente adequado, seguro e distinto em relação ao local dos dados originais ou em produção.

5.5 Criptografia

Compete à Gerência da área de TIS (Tecnologia de Infraestrutura e Segurança) a criação de procedimentos e controles criptográficos, visando a proteção das informações sob a responsabilidade da Trust Image, bem como a adoção de soluções de criptografia que contemplem o seguinte escopo:

- Criptografia de dado armazenado (*data at rest*), no mínimo AES 256, para informações confidenciais
- Criptografia no tráfego de dados (*data in transit*), no mínimo TLS 1.2 ou SSL, para informações confidenciais

A criptografia de dado armazenado, mencionado anteriormente, refere-se à aplicação de criptografia em discos, storages, bancos de dados, arquivos, mídias removíveis,

etc. Tal contexto de aplicação de criptografia deve também ser estendida aos dados em backup.

Os procedimentos e controles criptográficos tem por escopo estabelecer o fluxo para a criação/geração de chaves de criptografia a serem utilizadas na Trust Image, bem como estabelecer o registro e a guarda das mesmas. Todas as chaves criptográficas deverão ser armazenadas em sistema especializado de gestão de chaves ou impressas e fisicamente armazenadas em cofre. Além disso, os procedimentos também devem definir os critérios para escolhas dos algoritmos, que nunca poderão ter criptografia inferior aos valores definidos na presente PSI.

5.5.1 Gerenciamento das Chaves

Todas as chaves a serem utilizadas, visando atender necessidades de negócio sob a perspectiva de proteção de informações confidenciais, deverão ser geradas consoante a prática de separação de responsabilidades, envolvendo a criação e o controle por duas pessoas da empresa. Neste caso, um diretor da Trust Image e o Gerente da área de TIS (Tecnologia de Infraestrutura e Segurança) serão os responsáveis pelas funções de criação e gerenciamento das chaves. Nesse contexto, nenhuma única pessoa está autorizada a gerar qualquer chave de criptografia.

5.5.2 Criptografia no Envio / Recebimento de Mensagens

Utilização de sistema ou soluções de criptografia para envio e recebimento de mensagens contendo informações confidenciais ou sensíveis, por meio do correio eletrônico corporativo.

5.5.3 Dispositivos Portáteis

Dispositivos portáteis, como notebooks, são uma categoria que contém *data at rest*. Quando hospedando dados confidenciais ou sensíveis, tais equipamentos deverão ter o disco rígido completamente criptografado a fim de evitar a exposição não autorizada.

5.6 Correio Eletrônico

O serviço de correio tem como finalidade o envio e o recebimento eletrônico de mensagens e documentos relacionados exclusivamente com as finalidades profissionais da Trust Image. Dessa forma, é vedado ao usuário o uso do serviço de correio eletrônico corporativo com objetivos que não sejam compatíveis com as atividades e finalidades da Trust Image.

Os endereços de correio eletrônico corporativos e o conteúdo das caixas postais disponibilizadas aos usuários são de propriedade da Trust Image.

A concessão da caixa de e-mail corporativa ao usuário é efetuada pela área de TIS (Tecnologia de Infraestrutura e Segurança), mediante solicitação encaminhada

através de formulário eletrônico específico. Da mesma maneira a desativação da caixa postal do usuário deve ser realizada quando da ocorrência do seu desligamento ou do encerramento de seu contrato junto à Trust Image.

O acesso à caixa postal corporativa é realizado através de senha de caráter pessoal e intransferível, sendo vedado ao usuário fornecê-la para terceiros ou anotá-la em suportes físicos.

Compete à área de TIS (Tecnologia de Infraestrutura e Segurança) prover meios para:

- Manter, em local seguro e restrito, dados de auditoria acerca da utilização do serviço, tanto no sentido de garantir a recuperação de mensagens em caso de incidentes com o ambiente de rede, bem como visando a identificação de uso indevido
- Suspender motivadamente o acesso à conta de correio quando constatado o uso indevido dos recursos, dando imediata ciência ao respectivo titular e ao responsável pela apuração formal
- Monitorar o uso do ambiente, por meio de ferramentas sistêmicas, a fim de preservar a integridade das informações e identificar possíveis violações ao disposto nesta PSI

5.7 Internet

O acesso à Internet deve restringir-se à esfera profissional com conteúdo relacionado às atividades desempenhadas pela Trust Image, observando-se sempre a conduta compatível com a moralidade administrativa. Os usuários devem fazer uso da internet em estrita observância das leis em vigor, respondendo pelo seu descumprimento.

O acesso à internet é concedido aos colaboradores e terceirizados por meio de login e senha, que é pessoal e intransferível, sendo o titular o único responsável pelas ações
e/ou danos, se houver.

As contas de usuários deverão ter níveis de acesso distintos à internet, conforme a necessidade dos serviços, de acordo com os perfis definidos pela diretoria da Trust Image em conjunto com Gerência área de TIS (Tecnologia de Infraestrutura e Segurança).

Comprovada a utilização irregular do serviço de Internet, o usuário envolvido terá o seu acesso à Internet bloqueado pela área de TIS (Tecnologia de Infraestrutura e Segurança), sendo comunicado o fato à chefia imediata e ao responsável pela apuração formal.

É vedado o uso de provedores de acesso externos ou de qualquer outra forma de conexão não autorizada no ambiente da Trust Image.

Compete à área de TIS (Tecnologia de Infraestrutura e Segurança) prover o serviço de conexão à Internet implementando mecanismos de segurança adequados, bem como de trilhas de auditoria visando o cumprimento das leis em vigor.

5.8 Aplicativo de Comunicação

O uso de aplicativo de comunicação pelos colabores para compartilhar informações de negócio, deve ser feito exclusivamente por meio do aplicativo devidamente selecionado e homologado pela equipe de TIS – Tecnologia de Infraestrutura como ferramenta corporativa oficial para comunicação na Trust Image.

O uso deve ser feito de forma responsável para evitar riscos desnecessários que comprometam atividades, projetos ou a própria Trust Image, respeitando sempre o sigilo da informação, atendendo aos requisitos de segurança previstos nesta Política e respeitando as leis nacionais em vigor para evitar riscos desnecessários relacionados ao vazamento da informação ou que comprometam a Trust Image.

Compete, portanto, à equipe de TI – Tecnologia de Infraestrutura a seleção, adoção e o gerenciamento de uma ferramenta de comunicação corporativa oficial.

6. Gestão da Segurança da Informação

A responsabilidade pela gestão da Segurança da Informação compete ao **gerente da área de TIS (Tecnologia de Infraestrutura e Segurança),** qual tem as seguintes atribuições no âmbito da segurança da informação:

- Revisar e propor anualmente melhorias desta PSI
- Definir e garantir a aderência da empresa às diretrizes de Segurança da Informação estabelecidas na presente política
- Adotar todos os meios necessários para identificar as ameaças significativas e a exposição da informação
- Desenvolver campanhas visando garantir a conscientização de todos os colaboradores da Trust Image

7.Sanções

De forma geral, cabe a todos os colabores e prestadores de servicos da Trust Image cumprir fielmente a presente Política de Segurança da Informação, bem como as Normas e Procedimentos relacionados.

Na ocorrência de violação desta Política de Segurança da Informação, o Conselho Diretivo poderá adotar sanções administrativas e/ou legais, que poderão culminar com o desligamento e eventuais processos criminais, se aplicáveis.

8. Disposições Finais

O presente documento deve ser lido e considerado em conjunto com outros padrões e procedimentos aplicáveis e relevantes adotados pela Trust Image. Além disso, esta política deve ser desdobrada em outros documentos contendo procedimentos específicos, sempre alinhados às diretrizes e princípios aqui estabelecidos.

As diretrizes aqui estabelecidas devem nortear a atuação das áreas da empresa Trust Image, destacadamente, as áreas relacionadas à tecnologia da informação, contribuindo para uma visão única e integrada.

Deve ser assegurado que esta política e os documentos com os procedimentos complementares sejam amplamente divulgados a todos os colaboradores, visando a sua disponibilidade para todos que se relacionam com a Trust Image.

9. Documentos de Referência

O presente documento será complementado por Procedimentos de Segurança da Informação específicos e está em consonância com os seguintes documentos:

- ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos;
- ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- ABNT NBR ISO/IEC 27014:2013 – Tecnologia da informação — Técnicas de segurança — Governança de segurança da informação;
- Norma ISO/IEC 27005:2011 – Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação;
- COBIT 5.