PSI – POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PROCEDIMENTO DO SISTEMA (NTQA)

NTQA	1180	-	08
SIGLA	NÚMERO/PARTE		REVISÃO

Data da Homologação:	26/07/2023

1 OBJETIVO

A Política de Segurança da Informação da TIGRE é uma declaração formal da empresa acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores, prestadores de serviços e terceiros. Seu propósito é estabelecer as diretrizes a serem seguidas através de normas internas no que diz respeito à adoção de procedimentos e mecanismos relacionados à Segurança da Informação.

2 INTRODUÇÃO

A informação é um ativo que possui grande valor para a TIGRE, devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação e proteção de dados deve ser prioridade constante da empresa, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição.
A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger três aspectos básicos, destacados a seguir:

- **Confidencialidade**: somente pessoas devidamente autorizadas pela empresa devem ter acesso à informação;
- **Integridade**: somente alterações, supressões e adições autorizadas pela empresa devem ser realizadas nas informações;
- **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado.

Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças.
Em empresas grandes e complexas, a proteção da informação não é uma tarefa trivial. Em geral, o sucesso da Política de Segurança da Informação e Proteção de Dados adotada por uma instituição depende da combinação de diversos elementos, dentre eles, a estrutura organizacional da empresa, as normas e os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, as campanhas de conscientização das pessoas assim como o comportamento de diretores, funcionários e colaboradores.

3 DOCUMENTOS COMPLEMENTARES

Não aplicável.

4 DEFINIÇÕES

- **CGSI e DP:** Comitê Gestor de Segurança da Informação e Dados Pessoais
- **PSI:** Política de Segurança da Informação e Proteção de Dados
- **Comitê:** Reuniões de alinhamento estratégico entre as áreas envolvidas

5 ESTRUTURA NORMATIVA DA SEGURANÇA DA INFORMAÇÃO

5.1 DEFINIÇÕES

A estrutura normativa da Segurança da Informação da TIGRE é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- **Política de Segurança da Informação (Política):** constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação;

- **Normas de Segurança da Informação (Normas):** estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada;

- **Procedimentos de Segurança da Informação (Procedimentos):** instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades da TIGRE.

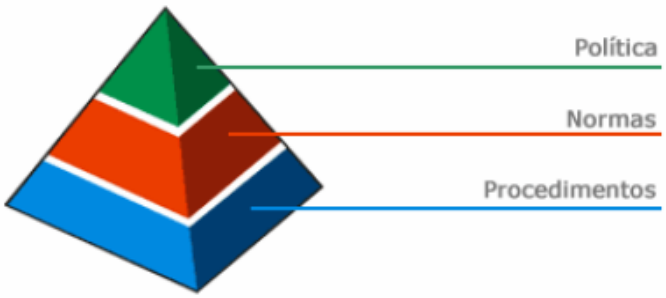

Figura 1 – Estrutura normativa de Segurança da Informação da Tigre

5.2 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os colaboradores da TIGRE através de treinamentos, integrações e outras ações de conscientização e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento.
Os Procedimentos de Segurança da Informação devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

5.3 GOVERNANÇA DE TI

A Governança fornece uma base para tomadas de decisões da TI com o negócio utilizando componentes como comitês, políticas e métricas que permitem alinhamento, eficiência e accountability da TI.

- **Alinhamento:** Garante investimentos alinhados com o negócio. Garante que as iniciativas de TI estejam alinhadas com os padrões de arquitetura, controle e segurança. Garante alinhamento da TI com o ecossistema de fornecedores da TI
- **Eficiência:** Otimiza a alocação do orçamento de TI de acordo com as prioridades do Negócio. Racionaliza e otimiza o desenvolvimento e manutenção de soluções

- **Accountability:** Melhora o desempenho do serviço e os retornos nos investimentos de TI, à medida em que as pessoas trabalham para alcançar os resultados pelos quais eles são responsáveis

Figura 2 – Estrutura de Governança de TI da Tigre

5.4 APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura Normativa da Segurança da Informação da TIGRE deverão ser aprovados e revisados conforme os seguintes critérios:

- **Política**
  - **Nível de Aprovação**: Diretoria Executiva
  - **Periodicidade de Revisão:** Anual
- **Normas**
  - **Nível de Aprovação:** Comitê Gestor de Segurança da Informação e Dados Pessoais
  - **Periodicidade de Revisão:** Anual
- **Procedimentos**
  - **Nível de Aprovação:** Diretoria responsável pela área envolvida
  - **Periodicidade de Revisão:** Anual

6 ATIVIDADES, RESPONSABILIDADES E AUTORIDADES

Atividades	Responsabilidades	Autoridades
Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da TIGRE.	Todos os Funcionários e Terceiros	Todos os gestores
Buscar orientação do superior hierárquico imediato ou do especialista em Segurança da Informação Corporativo em caso de dúvidas relacionadas ao tema.	Todos os Funcionários e Terceiros	Todos os gestores
Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento.	Todos os Funcionários e Terceiros	Todos os gestores

Ciência a Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento de acordo com o contrato celebrado.	Todos os terceiros que possuem acesso à tecnologia da informação	Todos os gestores
Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela TIGRE.	Todos os Funcionários e Terceiros	Todos os gestores
Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela TIGRE.	Todos os Funcionários e Terceiros	Todos os gestores
Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual.	Todos os Funcionários e Terceiros	Todos os gestores
Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.	Todos os Funcionários e Terceiros	Todos os gestores
Atualizar a Política de Segurança da Informação.	Segurança da Informação com aporte do CGSI e PD	Diretoria de Finanças e TI
Identificar e atribuir responsabilidades com relação à Segurança da Informação.	Segurança da Informação	Gestor de Operações de TI
Avaliar e monitorar o nível de Segurança da Informação.	Segurança da Informação	Gestor de Operações de TI
Monitorar alterações que possam afetar a segurança da informação e, caso necessário, levar ao CGSI as iniciativas de melhoria do nível de segurança.	Segurança da Informação	Gestor de Operações de TI
Identificar e documentar as violações e suas consequentes ações disciplinares, juntamente com os gerentes locais e o Departamento de Recursos Humanos.	Segurança da Informação com apoio do CGSI e PD	Diretoria de Finanças e TI
Propor soluções e alternativas para elevar o nível de segurança da informação da Tigre.	Segurança da Informação	Gestor de Operações de TI
Auditar o cumprimento das regras definidas nas políticas de segurança da informação.	Segurança da Informação	Gestor de Operações de TI
Restringir o acesso e assegurar a proteção de todos os ativos físicos que contenham informações confidenciais.	Segurança da Informação	Gestor de Operações de TI
Restringir o acesso e assegurar a proteção dos ativos constantes nos servidores da Tigre.	Segurança da Informação	Gestor de Operações de TI
Aprovar a Política de Segurança da Informação e suas revisões.	Diretoria de Finanças, Jurídica e TI	Presidência
Aprovar a nomeação dos “proprietários” da informação.	Diretoria de Finanças, Jurídica e TI	Presidência
Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação e Proteção de Dados.	Diretoria de Finanças, Jurídica e TI	Presidência

7 REGIMENTO INTERNO DO COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO E DADOS PESSOAIS

7.1 REGIMENTO

As responsabilidades, competências e atribuições do Comitê Gestor de Segurança da informação e dados pessoais do Grupo Tigre estão definidas e estabelecidas neste Regimento.

7.2 MISSÃO

O Comitê Gestor de Segurança da Informação e dados pessoais é um órgão consultivo e propositivo, vinculado à Gestão, que tem por objetivo formular, aprovar e monitorar políticas e diretrizes relacionadas à segurança das informações corporativas, bem como à proteção de dados pessoais para integral cumprimento da Lei nº 13.709, Lei Geral de Proteção de Dados – LGPD, sendo responsável por:

- Acompanhar a implementação do Programa de Proteção de Dados, constituindo grupos de trabalho, quando necessário, atuando através de treinamentos e comunicações para estabelecimento de uma cultura de Proteção de Dados e Segurança da Informação;
- Analisar os casos de violação da Política de Segurança da Informação NTQA 1180 e das demais Normas de Segurança da Informação e recomendar as providências necessárias;
- Analisar, averiguar, tratar e responder dentro do prazo legal todas as solicitações referentes à LGPD recebidas pelo Grupo Tigre, acompanhando até a sua conclusão;
- Revisar e manter atualizada as normas, políticas e procedimentos do Grupo Tigre, relacionadas à Proteção de Dados e Segurança da Informação, promovendo sempre a melhoria contínua através da identificação de oportunidades de aprimoramento nos processos internos;

7.3 COMPOSIÇÃO

O Comitê será composto por representantes das áreas de Tecnologia da Informação, Jurídico, Compliance, Controles internos e Gestão de Riscos e Recursos Humanos do Grupo Tigre. De acordo com a necessidade, convidados de outras áreas ou convidados externos poderão participar das reuniões Comitê.

7.4 FUNCIONAMENTO

- O Comitê reunir-se-á ordinariamente, no mínimo, 06 (seis) vezes por ano, bimestralmente, por convocação do seu Coordenador e, extraordinariamente, sempre que um de seus membros solicitar ao Coordenador;
- As deliberações recomendativas e propositivas do Comitê serão tomadas preferencialmente por consenso;
- A pauta e os materiais constitutivos das reuniões serão encaminhados por meio do Coordenador, aos membros, com até 03 (três) dias de antecedência;
- Com vistas ao melhor desempenho de suas atribuições, o Comitê poderá agendar reuniões com membros da Diretoria Executiva ou quaisquer outros funcionários da Companhia, bem como, com empresas que prestam serviços de assessoria/consultoria em Privacidade e Proteção de Dados / Segurança da Informação;
- O Comitê, no âmbito de suas atribuições, poderá contratar os serviços de especialistas desde que haja aprovação orçamentária;
- As reuniões do Comitê serão registradas em ata elaborada e enviada aos membros.

7.5 ATRIBUIÇÕES

7.5.1 CABE AO COMITÊ:

- Direcionar as análises, coleta de dados e informações e tomar providências e medidas que entenderem mais adequadas para resolver as questões, assim como dar encaminhamentos às sugestões apresentadas para as respectivas áreas de interesse;
- Avaliar e formular recomendações com respeito à estratégia de Proteção de Dados com seu público interno e externo, a fim de elevar o nível de confiança e preservar a imagem e a reputação do Grupo Tigre.
- Avaliar e acompanhar o desempenho dos indicadores, iniciativas e práticas de Privacidade de Proteção de Dados e Segurança da Informação, apresentando, estatísticas, status, dados, soluções encontradas e informações, quando solicitado.
- Avaliar os riscos de Privacidade de Proteção de Dados e Segurança da Informação decorrentes de questões legais, bem como, propor em conjunto com as áreas, planos de ações de mitigação;
- Zelar para que as políticas relacionadas a Privacidade de Proteção de Dados e Segurança da Informação estejam permanentemente compatíveis com a necessidade da Companhia;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à Proteção de Dados e Segurança da Informação;
- Promover e preservar a Cultura de Privacidade de Proteção de Dados e Segurança da Informação;
- Definir a classificação das informações pertencentes ou sob a guarda da TIGRE, com base no inventário de informações apresentado pela Área de Gestão de Segurança da Informação e nos critérios de classificação constantes de Norma específica;
- Analisar os casos de violação das Políticas e das Normas de Segurança da Informação, encaminhando-os à Diretoria Executiva, quando for o caso;
- Propor projetos e iniciativas relacionados à melhoria da segurança da informação da TIGRE e acompanhar o andamento dos projetos em curso;
- Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;
- Definir os critérios que garantem que a TI esteja alinhada com as obrigações de Negócio;
- Gerir e monitorar os pontos de auditoria relacionados à Segurança da Informação;

7.5.2 CABE AO ENCARREGADO DE DADOS (DPO): (PESSOA INDICADA PELA TIGRE PARA ATUAR COMO CANAL DE COMUNICAÇÃO ENTRE A TIGRE E OS TITULARES DOS DADOS E A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD);

- Atuar com o suporte técnico da área de TI e demais áreas quando necessário, aceitando reclamações e comunicações dos titulares, prestando esclarecimentos e adotando as providências, necessárias;
- Receber comunicações da ANPD e adotar providências;
- Orientar, diretamente ou através do Comitê, os funcionários e os contratados da Tigre a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;
- Atuar ativamente para o estabelecimento de uma cultura de proteção de dados no Grupo Tigre;

7.5.3 CABE À TI - SEGURANÇA DA INFORMAÇÃO:

- Suportar tecnicamente o encarregado de dados em todo e qualquer incidente de segurança envolvendo dados pessoais;
- Garantir que as responsabilidades de Infraestrutura e desenvolvimento estão sendo seguidas;
- Identificar, apresentar e tratar riscos, vulnerabilidades e falhas de segurança;
- Definir controles compensatórios para proteção de sistemas e dados em caso de não correção de vulnerabilidades;

- Implantar e Administrar soluções de segurança tais como Antimalware, Firewalls, Antispam, SIEM etc;
- Criar e manter controles técnicos relacionados a acessos;
- Garantir o armazenamento de logs de segurança e eventos de segurança, assim como sua integridade.

7.5.4 CABE À TI – INFRAESTRUTURA:

- Armazenar e prover logs de acesso e auditoria;
- Remover ou prover dados pessoais armazenados em bancos de dados locais;
- Gerenciar e monitorar backups das aplicações e sistemas e garantir sua integridade;
- Manter sistemas operacionais atualizados;
- Analisar termos contratuais com fornecedores e parceiros de infraestrutura ou cloud.

7.5.5 CABE À TI – DESENVOLVIMENTO DE SOFTWARE:

- Coletar somente os dados necessários para o sistema;
- Disponibilizar temos de privacidade de dados e cookies;
- Disponibilizar termo de “Aceite” ou “Não aceite” de cookies;
- Realizar o armazenamento dos cookies de forma centralizada e integra;
- Realizar desenvolvimentos seguindo boas práticas de segurança.

7.5.6 CABE AO COMPLIANCE:

- Atuar como PMO durante a implementação do Programa de Proteção de Dados para atendimento da Lei nº 13.709, Lei Geral de Proteção de Dados;
- Auxiliar nos treinamentos e comunicação sobre o tema aos funcionários;
- Apoiar no recebimento e tratamento das reclamações relacionadas à Proteção de Dados e Segurança da Informação;

7.5.7 CABE AO JURÍDICO:

- Revisar e aprovar a política da governança de privacidade e proteção de dados pessoais;
- Apoiar no tratamento das reclamações relacionadas à Proteção de Dados e Segurança da Informação;
- Suportar o encarregado de dados com a base legal e recomendações técnicas jurídicas para atendimento da Lei nº 13.709, Lei Geral de Proteção de Dados;
- Manter as áreas da TIGRE informadas sobre eventuais alterações legais e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;
- Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses da TIGRE;

7.5.8 CABE A RISCOS:

- Auxiliar na identificação de riscos relacionados a privacidade e proteção de dados, por meio de metodologia para mapeamento, validação e acompanhamento de riscos;
- Auxiliar os responsáveis pelos riscos no tratamento por meio do monitoramento e acompanhamento dos planos de ação.

7.5.9 CABE A CONTROLES INTERNOS:

- Apoiar na construção e revisão de controles relacionados as atividades que visam a privacidade e proteção de dados;

- Revisão e Homologação das políticas relacionadas à segurança da informação e proteção de dados.

7.5.10 CABE AO RH:

- Auxiliar nos treinamentos e comunicação sobre o tema aos funcionários
- Colher a assinatura do Termo de Responsabilidade dos funcionários e estagiários, arquivando-o nos respectivos prontuários;

8 DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação da TIGRE. Tais diretrizes constituem os principais pilares da Segurança da Informação, norteando a elaboração das Normas e dos Procedimentos.

8.1 ADOÇÃO DE COMPORTAMENTO SEGURO

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações, com destaque para os seguintes itens:

- Diretores, gerentes, coordenadores, funcionários e prestadores de serviços devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da TIGRE.
- Os colaboradores da TIGRE devem compreender as ameaças externas que podem afetar a segurança das informações da empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.
- Todo tipo de acesso à informação da TIGRE que não for explicitamente autorizado é proibido.
- Informações confidenciais da TIGRE não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel etc.) sem as devidas autorizações e proteções.
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.).
- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores da própria empresa), anotadas em papel ou em sistema visível ou de acesso não-protegido.
- Somente softwares homologados pela TIGRE podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe do Global Services TI, especialista Windows Tigre ou fornecedores de suporte Windows.
- A política para uso de internet e correio eletrônico deve ser rigorosamente seguida. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados.
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a área de Segurança da Informação.

8.2 INVENTÁRIO DE INFORMAÇÕES

As informações inventariadas devem ser associadas a um “proprietário”, o qual é um Gestor Tigre formalmente designado pela Diretoria Executiva como responsável pela autorização de acesso às informações sob a sua responsabilidade.

8.3 AVALIAÇÃO CONTÍNUA DOS RISCOS DE SEGURANÇA DA INFORMAÇÃO

A área de Segurança da Informação deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação da TIGRE.
A análise dos riscos deve atuar como ferramenta de orientação ao Comitê Gestor da Segurança da Informação, principalmente, no que diz respeito à:

- Identificação dos principais riscos aos quais a informação de nível estratégico pode sofrer;
- Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas etc.

O escopo da análise/avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.

8.4 GESTÃO DE ACESSO A SISTEMAS DE INFORMAÇÃO E A OUTROS AMBIENTES LÓGICOS

Todo acesso às informações e aos ambientes lógicos da TIGRE deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação.
A política de controle de acesso deve ser documentada e formalizada por meio de Normas e Procedimentos que contemplem, pelo menos, os seguintes itens:

- Procedimento formal de concessão e cancelamento de autorização de acesso à usuário aos sistemas de informação;
- Comprovação da autorização do proprietário da informação;
- Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;
- Verificação se o nível de acesso concedido é apropriado ao propósito do negócio e se é consistente com a Política de Segurança da Informação e suas Normas;
- Remoção imediata de autorizações dadas a usuários afastados ou desligados da empresa, ou que tenham mudado de função;
- Processo de revisão periódica das autorizações concedidas;
- Política de atribuição, manutenção e uso de senhas.

8.5 MONITORAÇÃO E CONTROLE

Os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade da TIGRE, não podendo ser interpretados como de uso pessoal.
Todos os profissionais e colaboradores da TIGRE devem ter ciência de que o uso das informações e dos sistemas de informação pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

8.6 SEGURANÇA FÍSICA

O acesso ao escritório, sala de servidores ou outro local da Tigre que contenha informação sensível deve ser restrito fisicamente. Isso vale para ambientes on premisses (Matriz e filais) e para ambiente em Cloud.

8.7 ATIVIDADES SUSPEITAS

Devem ser imediatamente informados à área de Tecnologia da Informação, através do Help Desk, incidentes de segurança para todas as constatações ou suspeitas de:

- Violação da política de segurança da informação;
- Intrusões no sistema;
- Infecção por vírus ou outros programas maliciosos;
- Acesso físico não autorizado;
- Eventos que de alguma forma possam comprometer a segurança das informações.

A omissão ou negligência por parte do usuário será considerada conivência com a atividade não.

8.8 LEGISLAÇÃO

A Tigre tem como princípio cumprir as leis e normas aplicáveis aos locais onde está estabelecida. Para tanto, periodicamente deve ser verificada a publicação ou alteração da legislação. Cabe a área de Tecnologia da Informação, com o apoio do Departamento Jurídico, identificar a legislação cabível e propor a adequação da Tigre.

8.9 CASOS OMISSOS

Antes de efetuar um acesso, armazenamento, transmissão, destruição ou qualquer outro ato envolvendo os sistemas ou as informações da Tigre, o usuário deve consultar a política de segurança da informação para certificar-se de que o ato seja permitido. Toda e qualquer atividade que não seja expressamente permitida é proibida.

8.10 DESCARTE DE INFORMAÇÕES

Informações sensíveis não devem ser descartadas utilizando-se o lixo comum. Documentos impressos que contenham informações sensíveis devem ser fragmentados de forma que se torne impossível a leitura. Discos ou outras formas de armazenamento eletrônico de dados devem ser entregues à área de Tecnologia da Informação, através do Help Desk para que sejam destruídos.

8.11 NORMAS DE SEGURANÇA DA INFORMAÇÃO

Conforme explicado anteriormente, os aspectos de segurança física, lógica e de pessoal, serão tratados em documentos independentes, tendo em vista suas peculiaridades e deverão compor este documento principal da Política de Segurança da Informação em forma de anexos, a fim de complementar com maior especificidade e detalhamento, as normas e recomendações de segurança no trato das informações.

A. NTQA-1181 - Política de Segurança da Informação - Gestão de Incidentes de Segurança da Informação
B. NTQA-1182 - Política de Segurança da Informação - Controle de Acesso Lógico
C. NTQA-1183 - Política de Segurança da Informação - Estações de Trabalho, Equipamentos Portáteis e Telefonia
D. NTQA-1184 - Política de Segurança da Informação - Segurança para Uso de Internet
E. NTQA-1185 - Política de Segurança da Informação - Uso de Correio Eletrônico
F. NTQA-0204 - Política de Segurança da Informação – Backup
G. NTQA-40001 - Política de Segurança da Informação – Cloud
H. NTQA-1428 - Política de Segurança da Informação - Tecnologias, Configurações e Processos
I. NTQA-1411 - Política de Segurança da Informação - Concessão de acesso lógico ao sistema SAP ECC
J. NTQA-1413 – Política de Segurança da Informação - Controle de abertura de mandante SAP ECC

8.12 VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Em nenhum momento será admitido, a qualquer funcionário ou terceiros, invocar o desconhecimento desta norma para justificar violações ou falta de cumprimento da mesma.
Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com o desligamento e eventuais processos criminais, se aplicáveis.

9 BIBLIOGRAFIA

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR: ISO/IEC Código de Prática de Segurança da Informação, 27002. Rio de Janeiro, 2005. 1. ed.

10 ANEXOS

Não aplicável.