POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E DADOS PESSOAIS PARA FORNECEDORES

NTQA	1186	-	00
SIGLA	NÚMERO/PARTE		REVISÃO

Data da Homologação:	18/03/2024

1 OBJETIVO

As diretrizes de Segurança da Informação da Tigre acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus fornecedores. 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 DEFINIÇÕES

- **Segurança da Informação**: Está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização.
- **Fornecedores**: Toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira que prestam serviços e celebram um contrato de fornecimento, parceria ou prestação de serviços com a Tigre.
- **Propriedade Intelectual**: – Área do Direito que, por meio de leis, garante a inventores ou responsáveis por qualquer produção do intelecto industrial, o direito de obter, por um determinado período de tempo, recompensa pela própria criação.
- **Incidente de Segurança da Informação**: Evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade de um ativo de informação, assim como qualquer violação da Política de Segurança da Informação.
- **Dispositivos Móveis:** Computador de dimensões reduzidas que, muitas vezes, pode executar serviços semelhantes aos computadores comuns. Ex. Notebooks, celulares e todos equipamentos que se encaixam no conceito de IOT (dispositivos capazes de conectar com internet).
- **Estação de Trabalho**: É o local onde você trabalha, no caso, sua mesa e tudo quanto é tipo de material fisico que não seja transportável, como o computador de mesa (*desktop*), por exemplo.
- **Equipamento:** Quando nos referimos a equipamento, estamos abrangendo dispositivos móveis, BYOD e os equipamentos pertencentes a estação de trabalho.
- **Software:** São quaisquer sistemas, programas e/ou jogos utilizados no meio computacional;
- **Pirataria:** distribuição ou uso de programas de computador sem a permissão do detentor dos direitos autorais. Isso pode incluir o uso de chaves de licença ilegais, a distribuição de cópias não autorizadas ou a instalação em múltiplos dispositivos além do permitido pela licença.
- **Hardware:** É a parte física de qualquer equipamento de informática.
- **Códigos Maliciosos:** É um software destinado a se infiltrar em um sistema de computador com o intuito de causar algum dano ou roubo de informações. Vírus de computador, *worms*, ransonware, cavalos de tróia e *spywares* são considerados códigos maliciosos.
- **Vírus:** São programas criados para danificar o sistema operacional que faz cópias de si mesmo e se espalham por outros computadores.
- **Ransomware:** Virus que sequestra os arquivos de rede e do computador e solicita um valor e moeda digital para que o usuário tenha novamente acesso ao conteúdo.
- **Firewall:** Dispositivo de uma rede de computadores que tem por objetivo bloquear acessos indevidos e interligar lógicamente as filiais Tigre.
- **Segurança:** Neste documento, sempre que citado isoladamente o termo Segurança, este é entendido como Segurança da Informação.
- **Homologado:** Algum serviço ou produto que já foi testado e teve seu uso aprovado pela Tigre.
- **BYOD:** Sigla em inglês (Bring your own device), ou seja, utilização de equipamento próprio dentro do ambiente de trabalho.
- **USB:** Do termo em inglês “Universal Serial Bus”, ou seja, tecnologia que permite a conexão de periféricos e armazenamento de dados.
- **Software homologado:** É o sistema/aplicação que passou pela analise de requisitos da área de segurança da informação e pode ser utilizado nos equipamentos corporativos.
- **Hardware homologado:** É o equipamento físico que passou pela analise de requisitos da área de segurança da informação e pode ser utilizado nos equipamentos corporativos.
- **Log:** Registro de acessos, alterações e exclusões de um sistema.
- **O365:** Software como serviço (SaaS) da empresa Microsoft que possui diversas facilidades como: office (excel, word, access e power point), power BI (Big Data), exchange (e-mail) e outros.
- **Hacker:** Pessoa com grandes conhecimentos computacionais usados para o crime digital, buscam invadir empresas através da exploração de falhas em seus sistemas com objetivos de roubo/sequestro de dados ou alterações que afetem diretamente o negócio da empresa
- **Cofre de Senhas:** Local/sistema de armazenamento de senhas de usuários privilegiados, sistemas, genéricos e outros que podem impactar diretamente no core business da empresa.

- **Privilégio mínimo:** Nível de permissionamento que libera somente o que for necessário para as atividades do usuário.
- **Dupla autenticação:** É uma dupla validação no login onde é solicitado um código que é gerado a partir de um aplicativo de autenticação homologado pela área de Segurança da Informação.

3 ATIVIDADES, RESPONSABILIDADES E AUTORIDADES

Atividades	Responsabilidades	Autoridades
Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da TIGRE.	Todos os Fornecedores que possuem acesso à tecnologia da informação	Todos os gestores responsáveis pelo contrato de prestação de serviço
Buscar orientação do superior hierárquico imediato ou do especialista em Segurança da Informação Corporativo em caso de dúvidas relacionadas ao tema.	Todos os Fornecedores que possuem acesso à tecnologia da informação	Todos os gestores responsáveis pelo contrato de prestação de serviço
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 Fornecedores que possuem acesso à tecnologia da informação	Todos os gestores responsáveis pelo contrato de prestação de serviço
Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela TIGRE.	Todos os Fornecedores que possuem acesso à tecnologia da informação	Todos os gestores responsáveis pelo contrato de prestação de serviço
Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela TIGRE.	Todos os Fornecedores que possuem acesso à tecnologia da informação	Todos os gestores responsáveis pelo contrato de prestação de serviço
Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual.	Todos os Fornecedores que possuem acesso à tecnologia da informação	Todos os gestores responsáveis pelo contrato de prestação de serviço
Comunicar imediatamente à área de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.	Todos os Fornecedores que possuem acesso à tecnologia da informação	Todos os gestores responsáveis pelo contrato de prestação de serviço

4 DESCRIÇÃO DAS ATIVIDADES

4.1 RESPONSABILIDADES SOBRE SEGURANÇA DA INFORMAÇÃO

A Tigre define a área de Tecnologia da Informação como autoridade maior para avaliação de políticas, padrões e procedimentos com referência a Segurança da Informação.

4.2 ESFORÇO CONJUNTO

Independente de qual área possui a responsabilidade sobre o tema Segurança da Informação, para ser efetivo, o sistema de segurança da informação deve contar com a participação e apoio de todos os Fornecedores que prestam serviço para a Tigre, especialmente das pessoas que lidam com os sistemas de informação.

5 ORIENTAÇÕES

5.1 SOBRE A POLÍTICA

Esta política estabelece diretrizes e princípios gerais de segurança da informação e dados pessoais para os fornecedores, e deve ser parte integrante do contrato do fornecedor com a Tigre.

No ato da assinatura dos contratos, o fornecedor deve assumir total conhecimento e concordância com as diretrizes expostas nesta Política de Segurança da Informação e Dados Pessoais.

Os fornecedores que acessarem ou processarem dados pessoais, dado pessoais sensíveis e/ou informações sensíveis, devem ter ciência desta política.

Dúvidas sobre a aplicação desta política ou sugestões de alteração e melhoria podem ser encaminhadas para a equipe de Segurança da Informação através do email seguranca.informacao@tigre.com.

6 VIGÊNCIA

Esta Diretriz deve ser revisada anualmente ou, quando necessário, caso haja alguma mudança nas normas, diretrizes da empresa ou órgão regulamentador.

7 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1 Definição de incidente

Situação não planejada envolvendo sistemas da informação, que cause impacto na disponibilidade de serviços, ativos e dados da empresa, bem como sua violação ou acesso indevido.

São exemplos de incidente ataques por vírus, sequestro de dados, ataques de falha de disponibilidade, etc.

7.2 Informando os Incidentes

Quaisquer incidentes que possam ser considerados falha de segurança ou violação da Política de Segurança e que geram indisponibilidade do ambiente, falta de integridade e confidencialidade das informações corporativas e danos a marca Tigre devem ser imediatamente e formalmente relatadas a área de Segurança da Informação, através do Global Services TI ou para o e-mail seguranca.informacao@tigre.com.
.

8 ESTAÇÕES DE TRABALHO, DISPOSITIVOS MÓVEIS E TELEFONIA

As estações de trabalho e os dispositivos móveis caso fornecidos pela Tigre devem ter seu uso dedicado para o meio corporativo, devendo sempre possuir um responsável.

A função de responsável é delegada automaticamente para o usuário que utiliza continuamente ou na maior parte do tempo o equipamento. Todo equipamento Tigre que estiver ultrapassado e desatualizado, deve ser descartado de forma segura e sustentável.

A Tigre apoia fortemente as normas de direitos autorais e não aceita nenhum tipo de pirataria de qualquer natureza, inclusive de softwares. Por este motivo, as configurações dos equipamentos devem permanecer originais, conforme entregue pelo setor de Tecnologia da Informação, não devendo, o usuário alterar quaisquer itens de software, mesmo que licenciados, gratuitos ou homologados pela Tigre. Todas as alterações deste tipo, assim como alterações de hardware deverão ser efetuadas pela área de Tecnologia da Informação, através do Global Services TI.

A Tigre não se responsabiliza por softwares piratas instalados em equipamentos pessoais. Recomendamos a boa prática de utilização de softwares licenciados para todos os tipos de equipamentos, desde os equipamentos corporativos, até os equipamentos pessoais. A Tigre tem como pré-requisito para todo o equipamento pessoal a utilização de um antivírus ou sistema de segurança, equipamentos que não possuem esta possibilidade de configuração/instalação, não serão permitidos na rede corporativa. Deste modo o único acesso será via rede Wireless para visitantes fornecida pela Tigre aprovada pelo time de Segurança da Informação.

8.1.1 Atividades Proibidas em caso de utilização de computadores fornecidos pela Tigre

Criar ou armazenar qualquer material com as características abaixo relacionadas:

a. De cunho extremo como: político, racial e religioso;

b. Modificar ou decompor qualquer software, arquivo ou banco de dados instalado nos computadores;

c. Quaisquer conteúdos que mencionem alguma atividade ilegal;

d. Instalar códigos maliciosos como: vírus, cavalos de tróia ou programas de controle de computadores;

e. Instalar ou de qualquer forma inserir qualquer tipo de programa, software ou arquivo no equipamento sem a prévia autorização da área de Tecnologia da Informação da Tigre;

f. Remover, desabilitar ou alterar softwares de segurança, como antivírus, firewall, etc.;

g. Realizar qualquer reparo ou substituição de peças sem a prévia e expressa autorização da área de Tecnologia da Informação da Tigre;

h. Instalar modems ou quaisquer outros hardwares nas estações de trabalho sem prévia análise da Tecnologia da Informação via chamado no Global Services TI.

8.1.2 Recomendações de uso

- Use apenas aplicações de fontes confiáveis e que sejam bem avaliadas pelos usuários. Verifique comentários de outros usuários e se as permissões necessárias para a execução são coerentes com a destinação da aplicação;
- Não deixar os equipamentos portáteis desprotegidos em locais de alto risco de furto e roubo, tais como: locais públicos, eventos, hotéis, carros, entre outros;
- Se os usuários, para executarem uma tarefa precisam compartilhar dados entre si, devem usar obrigatoriamente diretórios compartilhados no O365 da Tigre.
- Não siga links recebidos por meio de mensagens eletrônicas;
- Caso os dispositivos móveis não estejam de acordo com as regras mencionadas, eles serão bloqueados, ficando inutilizáveis e seus relatórios analisados;

A instalação de ferramentas de proteção para estações de trabalho e dispositivos móveis é obrigatória para todos os equipamentos corporativos e a Tigre pode exigir a utilização de ferramentas de proteção em equipamentos BYOD para proteção dos seus dados.

A área de Segurança da Informação poderá efetuar bloqueios, solicitar a desinstalação ou a não utilização de aplicativos que por ventura seja identificado que não é um software que justifica o uso pela empresa para fins de trabalho, que seja considerado malicioso ou que possa trazer prejuízos para empresa.

9 USO DO CORREIO ELETRÔNICO

Fornecedores somente podem ter e-mail da Tigre se alocados de forma permanente na empresa e trabalhando exclusivamente com informações da companhia, sendo que o mesmo já deve ter um contrato vigente com a Tigre.

A criação do e-mail será realizada após aprovação do Gerente da área responsável pelo Terceiro e da área de Segurança da Informação.

À Tigre se reserva o direito de, sem consentimentos prévios, registrar e analisar as mensagens eletrônicas enviadas e recebidas, em todo seu conteúdo e disponibilizar estas informações para seus respectivos responsáveis, área de Tecnologia da Informação, Compliance e Recursos Humanos para gerir, monitorar, auditar e tomar as devidas providências quando necessário.

Toda a informação vinda de mensagens eletrônicas deve ser considerada suspeita até que se confirme o contrário. Antes de utilizar uma informação recebida via correio eletrônico, os usuários devem conferir a confiabilidade desta informação, sempre valide os e-mails, verifique o domínio do e-mail recebido, acesse o site da empresa que enviou o e-mail com promoções, mova o mouse em cima das imagens e links e verifique se os mesmos direcionam para o site da empresa em questão.

Evite abrir, clicar e passar qualquer informação relacionada a credenciais, senhas, dados ou informações confidenciais relacionada ao ambiente da Tigre.

Caso não seja possível validar a informação junto ao emissor, a área de Segurança da Informação, através do Global Services TI, deve ser acionada.

10 SEGURANÇA PARA USO DE INTERNET

O serviço de Internet disponibilizado pela Tigre é dedicado para uso em atividades profissionais e atividades de estudos e pesquisas, não devendo comprometer a produtividade dos seus usuários. Este serviço é de extrema importância para a empresa e o seu mau uso pode gerar diversos problemas, tais como: infecção por vírus, invasão de hackers e vazamento de informações.

Entende-se como utilização adequada, toda a navegação que é realizada respeitando direitos autorais, regras de licenciamento de *softwares*, direitos de propriedade, privacidade e proteção de propriedade intelectual.

O acesso à internet somente será liberado para os fornecedores que têm necessidade legítima para tal.

11 CONTROLE DE ACESSO LÓGICO

O Acesso à informação de propriedade da Tigre ou sob sua guarda baseia-se no conceito de que o usuário deve ter apenas o nível de acesso suficiente para executar suas tarefas (privilégio mínimo).

Portanto, toda informação, sistema, software e dados da Tigre devem ser protegidos contra o acesso não autorizado, garantindo sua confidencialidade, integridade e disponibilidade.

Para que o usuário possua acesso à rede, obrigatoriamente deve ter uma conta e senha cadastrada em seu nome dentro da Tigre. Logo, não é permitido acessar qualquer sistema da empresa por meio de contas de outros usuários, ou seja, é proibido o compartilhamento de usuários.

O uso da Dupla Autenticação é obrigatório em todos os sistemas que suportarem esse recurso, abaixo os principais sistemas que possuem dupla autenticação para os usuários:

- Acesso VPN
- Office 365 e sistemas integrados
- Portais para gerenciamento de domínios
- Cofre de Senhas

Todos os acessos VPN devem possuir a dupla autenticação ativa usando o método Push com o Microsoft Authenticator, exceções devem ser tratadas e aprovadas por Segurança da Informação.

Os acessos são monitorados e auditados, se identificado uso incomum ou malicioso, o departamento de Segurança da informação pode bloquear o acesso com a aprovação do Gerente de Segurança da informação.

É obrigatório escolher senhas com complexidade elevada, buscando proteger sua conta na rede da Tigre e assim evitando acessos não autorizados. Não é recomendado o uso de senhas que possam ser relacionadas ao trabalho ou vida pessoal, senhas de banco ou que são usadas de forma pessoal em outros locais (como e-mail, redes sociais, etc). As senhas devem ser únicas para a Tigre e diferente de senhas pessoais.

O compartilhamento de senhas é proibido, sendo que ela deve ser única e é dever do usuário mantê-la segurança.

Qualquer tipo de acesso inadequado nos sistemas ou rede Tigre, detectados pela área de Segurança da Informação e que possa estar colocando em risco a segurança da informação, poderão ser bloqueados imediatamente sem a necessidade de aprovação previa do gestor do funcionário, gestor de tecnologia da informação ou afins. A área de Segurança da Informação tem total autonomia para bloquear acessos que de alguma forma burlem as políticas e boas práticas de gestão de acessos da companhia ou que trazem riscos ao negócio.

12 TREINAMENTO E CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

É de responsabilidade da empresa fornecedora de serviços, treinar seus funcionários com compromisso de promover a capacitação e conscientização sobre segurança da informação e privacidade de dados. A Tigre pode adotar ações e iniciativas para promover o aculturamento sobre o tema segurança da informação e privacidade de dados com fornecedores e parceiros comerciais.

13 AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO NA CONTRATAÇÃO DE SERVIÇOS

Os processos e os controles necessários para reduzir os riscos associados às iniciativas de terceirização, incluindo acordos de computação em nuvem, devem fazer parte dos acordos comerciais entre os Fornecedores e a Tigre.

A Tigre se reserva ao direito de avaliar se o Fornecedor atende aos requisitos de segurança da informação, baseados em normas e boas práticas de mercado.

Os contratos com Terceiros devem garantir que a equipe ou subcontratados da organização externa cumpram os documentos normativos de segurança da informação da Tigre.

14 PRIVACIDADE DE DADOS PESSOAIS

A Tigre se preocupa com a privacidade de seus clientes e fornecedores, e está comprometida com a proteção de seus dados pessoais e as demais informações compartilhadas conosco.

A Tigre possuí política disponível em local público, por meio do link: https://tigresite.s3.amazonaws.com/2024/02/privacidade-de-dados.pdf, devendo ser cumprida integralmente por todos os fornecedores e parceiros comerciais.

Em caso de necessidade de atendimento, o Grupo Tigre conta com canal para atender as demandas dos titulares de dados, parceiros comerciais e fornecedores, por meio do link: https://contatoseguro.com.br/tigre.

15 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:

Todos os fornecedores devem assumir atitude proativa e engajada no que diz respeito à proteção das informações da Tigre.

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.

Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.

16 DESENVOLVIMENTO SEGURO

A Tigre se preocupa com o desenvolvimento seguro dos sistemas desenvolvidos internamente, estabelecendo as melhores práticas de segurança com o conceito de security by design e privacy by design.

O fornecedor que desenvolver softwares para a Tigre precisa manter os conjuntos de boas práticas de DevSecOps no ciclo de desenvolvimento dos sitemas.

17 MONITORAMENTO E CONTROLE

Os acessos são monitorados e auditados, se identificado uso incomum ou malicioso, o departamento de Segurança da informação pode bloquear o acesso com a aprovação do Gerente de Segurança da informação.

Qualquer tipo de acesso inadequado nos sistemas ou rede Tigre, detectados pela área de Segurança da Informação e que possa estar colocando em risco a segurança da informação, poderão ser bloqueados imediatamente sem a necessidade de aprovação previa do gestor do funcionário, gestor de tecnologia da informação ou afins. A área de Segurança da Informação tem total autonomia para bloquear acessos que de alguma forma burlem as políticas e boas práticas de gestão de acessos da companhia ou que trazem riscos ao negócio.

18 SANÇÕES

Em nenhum momento será admitido, a qualquer funcionário ou terceiro, invocar o desconhecimento desta norma para justificar violações ou falta de cumprimento dela. A inobservância às normas estabelecidas sujeita o infrator e aqueles que colaborarem com ele, às sanções previstas nas regulamentações de Recursos Humanos das empresas a qual estão vinculados, além das penalidades previstas em lei, nos âmbitos cível, criminal e administrativo

19 ANEXOS

Não aplicável.