TroianoBranding
www.troianobranding.com
+55 11 4688 1555

# PSI TB

## Política de Segurança da Informação & Privacidade da TroianoBranding

### Documento de Diretrizes e Normas Administrativas

**Primeira Edição_Ano 2012_ Versão 1.0**
**Revisão Ano 2020_Junho_Versão: 2.0**
**Revisão Ano 2021_Junho_Versão: 3.0**
**Revisão Ano 2022_Junho_Versão: 4.0**
**Revisão Ano 2023_Junho_Versão: 5.0**
**Revisão Ano 2024_Junho_Versão: 6.0**

## Sumário

A Política de Segurança da Informação é o documento que orienta e estabelece as diretrizes corporativas da TroianoBranding 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.

## 1. OBJETIVOS

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

Nortear a definição de normas e procedimentos específicos de segurança da informação, bem como a implementação de controles e processos para seu atendimento.

Portanto, este documento visa preservar as informações do TroianoBranding de 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 aos ativos correspondentes sempre que necessário.

## 2. APLICAÇÕES DA PSI

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada sócio, colaborador ou prestador de serviços, doravante denominados de "colaboradores", de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

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

## 3. PRINCÍPIOS DA PSI

Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pelo TroianoBranding pertence à referida organização. As exceções devem ser explícitas e formalizadas em contrato entre as partes.

Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços.

O TroianoBranding, por meio da Gerência de Segurança da Informação, poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

## 4. REQUISITOS DA PSI

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

Tanto a PSI quanto as normas deverão ser revistas e atualizadas periodicamente, sempre que algum fato relevante ou evento motive sua revisão antecipada.

Deverá constar em todos os contratos do TroianoBranding o anexo de Acordo de Confidencialidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição.

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.

Todo incidente que afete a segurança da informação deverá ser comunicado à Gerência de Sistemas e aos sócios majoritários. Um plano de contingência e a continuidade dos principais sistemas e serviços deverão ser implantados e testados no mínimo anualmente, visando reduzir riscos de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Deverão ser criados e instituídos controles apropriados em todos os pontos e sistemas em que a instituição julgar necessário para reduzir os riscos dos seus ativos de informação como, por exemplo, nas estações de trabalho, notebooks, nos acessos à internet, no correio eletrônico pelo TroianoBranding ou por terceiros.

A TroianoBranding exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

Esta PSI será implementada no TroianoBranding por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis.

## 5. AS RESPONSABILIDADES ESPECÍFICAS

### 5.1 RESPONSABILIDADE

Cecília Machado Russo Troiano, é sócia proprietária e gestora responsável por Privacidade e Proteção de Dados Pessoais da TroianoBranding.

### 5.2 DOS COLABORADORES EM GERAL

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.
Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar ao TroianoBranding e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

### 5.2. DOS COLABORADORES EM REGIME DE EXCEÇÃO (Temporários)

Devem entender os riscos associados à sua condição especial e cumprir rigorosamente o que está previsto no termo de aceite concedido pelo TroianoBranding.
A concessão poderá ser revogada a qualquer tempo se for verificado que a justificativa de motivo de negócio não mais compensa o risco relacionado ao regime de exceção ou se o colaborador que o recebeu não estiver cumprindo as condições definidas no aceite.

### 5.3. DOS GESTORES DE PESSOAS OU PROCESSOS

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI do TroianoBranding .

Exigir dos colaboradores a assinatura do Termo de Compromisso, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações do TroianoBranding.

Antes de conceder acesso às informações da organização, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

## 5.4. DOS CUSTODIANTES DA INFORMAÇÃO

### 5.4.1. ÁREA DE SEGURANÇA DA INFORMAÇÃO

As atribuições do gerente de segurança da informação são as aqui expressas. Desenhar topologia de rede e realizar devidos controles de roteamento. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais. Acordar com os gestores o nível de serviço que será prestado e os procedimentos de resposta aos incidentes. Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI, e em sua versão educacional, pelas Normas de Segurança da Informação complementares.

Os administradores e operadores dos sistemas computacionais podem, pela característica de seus privilégios como usuários, acessar os arquivos e dados de outros usuários. No entanto, isso só será permitido quando for necessário para a execução de atividades operacionais sob sua responsabilidade como, por exemplo, a manutenção de computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o TroianoBranding .

Quando ocorrer movimentação interna dos ativos de TI, garantir que as informações de um usuário não serão removidas de forma irrecuperável antes de disponibilizar o ativo para outro usuário.

Planejar, implantar, fornecer e monitorar a capacidade de armazenagem, processamento e transmissão necessários para garantir a segurança requerida pelas áreas de negócio.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de funcionários serão de responsabilidade do próprio funcionário.

- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante. Proteger continuamente todos os ativos de informação da empresa contra código malicioso, e garantir que todos os novos ativos só entrem para o ambiente de produção após estarem livres de código malicioso e/ou indesejado.

Garantir que não sejam introduzidas vulnerabilidades ou fragilidades no ambiente de produção da empresa em processos de mudança, sendo ideal a auditoria de código e a proteção contratual para controle e responsabilização no caso de uso de terceiros.
Definir as regras formais para instalação de software e hardware em ambiente de produção corporativo, bem como em ambiente exclusivamente educacional, exigindo o seu cumprimento dentro da empresa.
Realizar auditorias periódicas de configurações técnicas e análise de riscos. Realizar inventários anuais dos programas instalados nas máquinas de cada um dos funcionários.
Responsabilizar-se pelo uso, manuseio, guarda de assinatura e certificados digitais.
Garantir, da forma mais rápida possível, com solicitação formal, o bloqueio de acesso de usuários por motivo de desligamento da empresa, incidente, investigação ou outra situação que exija medida restritiva para fins de salvaguardar os ativos da empresa.
Garantir que todos os servidores, estações e demais dispositivos com acesso à rede da empresa operem com o relógio sincronizado com os servidores de tempo oficiais do governo brasileiro.
Monitorar o ambiente de TI, gerando indicadores e históricos de:

- uso da capacidade instalada da rede e dos equipamentos;
- tempo de resposta no acesso à internet e aos sistemas críticos do TroianoBranding;

- períodos de indisponibilidade no acesso à internet e aos sistemas críticos do TroianoBranding;
- incidentes de segurança (vírus, trojans, furtos, acessos indevidos, e assim por diante);
- atividade de todos os colaboradores durante os acessos às redes externas, inclusive internet (por exemplo: sites visitados, e-mails recebidos/enviados, upload/download de arquivos, entre outros);

#### 5.4.2. ÁREA DE SEGURANÇA DA INFORMAÇÃO

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação.
Propor e apoiar iniciativas que visem à segurança dos ativos de informação do TroianoBranding .
Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.
Buscar alinhamento com as diretrizes corporativas da instituição.

### 5.5. DO MONITORAMENTO E DA AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta PSI, bem como de sua versão educacional, o TroianoBranding poderá:

- implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a internet, dispositivos móveis ou wireless e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
- tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação do gerente (ou superior).

- realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
- instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

## 6. CORREIO ELETRÔNICO

O objetivo desta norma é informar aos colaboradores do TroianoBranding quais são as atividades permitidas e proibidas quanto ao uso do correio eletrônico corporativo.

O uso do correio eletrônico do TroianoBranding é para fins corporativos e relacionados às atividades do colaborador usuário dentro da instituição. A utilização desse serviço para fins pessoais é permitida desde que feita com bom senso, não prejudique o TroianoBranding e também não cause impacto no tráfego da rede.

Acrescentamos que é proibido aos colaboradores o uso do correio eletrônico do TroianoBranding :

- enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da organização;
- enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar;

- enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou o TroianoBranding ou suas unidades vulneráveis a ações civis ou criminais;
- divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
- falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas;

- apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades do TroianoBranding estiver sujeita a algum tipo de investigação.
- produzir, transmitir ou divulgar mensagem que:
    - contenha qualquer ato ou forneça orientação que conflite ou contrarie os interesses do TroianoBranding, que contenha ameaças eletrônicas, como: spam, mail bombing, vírus de computador; contenha arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    - vise obter acesso não autorizado a outro computador, servidor ou rede;
    - vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    - vise burlar qualquer sistema de segurança;
    - vise vigiar secretamente ou assediar outro usuário;

- vise acessar informações confidenciais sem explícita autorização do proprietário;
- vise acessar indevidamente informações que possam causar prejuízos a qualquer pessoa;
- inclua imagens criptografadas ou de qualquer forma mascaradas;
- tenha conteúdo considerado impróprio, obsceno ou ilegal;
- seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
- contenha perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas;
- tenha fins políticos locais ou do país (propaganda política);

- inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:

- Nome do colaborador, Gerência ou departamento, Nome da empresa, Telefone(s), Correio eletrônico

## 7. ACESSO À INTERNET

Todas as regras atuais do TroianoBranding visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da internet. Embora a conexão direta e permanente da rede corporativa da instituição com a internet

ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na internet está sujeita a divulgação e auditoria. Portanto, o TroianoBranding , em total conformidade legal, reserva-se o direito de monitorar e registrar todos os acessos a ela.

Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

O TroianoBranding, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e ao respectivo gestor. O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades.

No entanto, o acesso a e-mails pessoais desde máquinas com acesso ao servidor em rede não poderá ocorrer. O colaborador poderá checar contas de email pessoais desde dispositivos pessoais ou computadores sem acesso ao servidor do TroianoBranding .

Ainda sim, como é do interesse do TroianoBranding que seus colaboradores estejam bem informados, o uso de sites de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos nem implique conflitos de interesse com os seus objetivos de negócio.

Somente os colaboradores que estão devidamente autorizados a falar em nome do TroianoBranding para os meios de comunicação poderão manifestar-se, seja por e-mail, entrevista on-line, podcast, seja por documento físico, entre outros.

Apenas os colaboradores autorizados pelos sócios majoritários poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, sites ou comunidades de relacionamento, salas de bate-papo ou chat, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na internet.

Os colaboradores com acesso à internet poderão fazer o download (baixa) somente de programas ligados diretamente às suas atividades no TroianoBranding e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela gestão.

Programas que necessitem de investimento por parte do TroianoBranding necessitam de aprovação via Diretor Sócio, ou Sócios Majoritários, caso o valor supere os R$500,00 (quinhentos reais).

O uso, a instalação, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente na internet, são expressamente proibidos. Qualquer

software não autorizado baixado será excluído pela Gerência de Informação. Os colaboradores não poderão em hipótese alguma utilizar os recursos do TroianoBranding para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O download e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias. Para tal, grupos de segurança, cujos integrantes deverão ser definidos pelos respectivos gestores, precisam ser criados a fim de viabilizar esse acesso especial.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. Caso seja necessário, grupos de segurança deverão ser criados para viabilizar esse perfil de usuário especial e seus integrantes definidos pelos respectivos gestores.

Colaboradores com acesso à internet não poderão efetuar upload (subida) de qualquer software licenciado ao TroianoBranding ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo software ou pelos dados.

Os colaboradores não poderão utilizar os recursos do TroianoBranding para deliberadamente propagar qualquer tipo de vírus, worm, cavalo de troia, spam, assédio, perturbação ou programas de controle de outros computadores.

O acesso a softwares peer-to-peer não serão permitidos. Já os serviços de streaming (rádios on-line, canais de broadcast) serão permitidos a grupos específicos. O mesmo funcionará com os serviços de comunicação instantânea (MSN, etc.) serão inicialmente disponibilizados aos usuários e poderão ser bloqueados caso o gestor requisite formalmente à Gerencia de Sistemas. Não é permitido acesso a sites de proxy.

## 8. IDENTIFICAÇÃO

Os dispositivos de identificação e senhas protegem a identidade do colaborador usuário, evitando e prevenindo que uma pessoa se faça passar por outra perante o TroianoBranding e/ou terceiros.

O uso dos dispositivos e/ou senhas de identificação de outra pessoa constitui crime tipificado no Código Penal Brasileiro (art. 307 – falsa identidade). Tal norma visa estabelecer critérios de responsabilidade sobre o uso dos dispositivos de identificação e deverá ser aplicada a todos os colaboradores.

Todos os dispositivos de identificação utilizados no TroianoBranding , como o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal).

Todo e qualquer dispositivo de identificação pessoal, portanto, não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante o TroianoBranding e a legislação (cível e criminal) será dos usuários que dele se utilizarem. Somente se for identificado conhecimento ou solicitação do gestor de uso compartilhado ele deverá ser responsabilizado.

É proibido o compartilhamento de login para funções de administração de sistemas.

O Departamento de Recursos Humanos do TroianoBranding é o responsável pela emissão e pelo controle dos documentos físicos de identidade dos colaboradores.

A Gerência de Informação responde pela criação da identidade lógica dos colaboradores a organização, nos termos do Procedimento para Gerenciamento de Contas de Grupos e Usuários. Devem ser distintamente identificados os visitantes, estagiários, empregados temporários, empregados regulares e prestadores de serviços, sejam eles pessoas físicas e/ou jurídicas. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.

Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 10 (dez) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente. Os logins de administrador devem estar sob dupla custódia, impreterivelmente destinada a um dos dois sócios majoritários: Jaime Troiano ou Cecília Russo.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais (como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento); e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 5 (cinco) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com a Gerência de Informação do TroianoBranding .

Deverá ser estabelecido um processo para a renovação de senha (confirmar a identidade). Os usuários podem alterar a própria senha, e devem ser orientados a fazê-lo, periodicamente ou caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

A periodicidade máxima para troca das senhas é 120 (cento e vinte) dias, não podendo ser repetidas as 3 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, assim que algum usuário for demitido ou solicitar demissão, o Departamento de Recursos Humanos deverá imediatamente comunicar tal fato ao Departamento de Informação, a fim de que essa providência seja tomada.

De forma prática, o ex colaborador terá sua conta de email eliminada em até 2 horas após a comunicação da sua rescisão de trabalho. Antes de ausentar-se, no entanto, deve entregar itens de posse que sejam relacionados aos projetos, assim como entregar seu crachá de entrada e identificação, e suas chaves, caso as possua.

A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares. Caso o colaborador esqueça sua senha, ele deverá requisitar formalmente a troca ou comparecer pessoalmente à área técnica responsável para cadastrar uma nova.

## 9. COMPUTADORES E RECURSOS TECNOLÓGICOS

Os equipamentos disponíveis aos colaboradores são de propriedade do TroianoBranding , cabendo a cada um utilizá-los e manuseá-los corretamente para as atividades de interesse da instituição, bem como cumprir as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico da Gerência de Informação do TroianoBranding, ou de quem este determinar. As gerências que necessitarem fazer testes deverão solicitá-los previamente à Gerência de Sistemas e/ou diretamente aos sócios majoritários, ficando responsáveis jurídica e tecnicamente pelas ações realizadas.

Todas as atualizações e correções de segurança do sistema operacional ou aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instalados, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico responsável mediante registro de chamado no service desk.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio do TroianoBranding (fotos, músicas, vídeos, etc.) não deverão ser copiados/movidos para os drives de rede, pois podem sobrecarregar o armazenamento no servidor. Caso identificada a existência desses

arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da organização deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

Os colaboradores do TroianoBranding e/ou detentores de contas privilegiadas não devem executar nenhum tipo de comando ou programa que venha sobrecarregar os serviços existentes na rede corporativa sem a prévia solicitação e a autorização da Gerência de Informação.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

- Todos os computadores de uso individual deverão ter senha de acesso para restringir o acesso de colaboradores não autorizados. Tais senhas serão definidas pela Gerência de Informação do TroianoBranding , que terá acesso a elas para manutenção dos equipamentos.
- Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
- É vedada a abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da Gerência de Informação do TroianoBranding ou por terceiros devidamente contratados para o serviço.
- Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para

planos de contingência mediante a autorização dos gestores das áreas e dos sócios majoritários.

- É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
- O colaborador deverá manter a configuração do equipamento disponibilizado pelo TroianoBranding, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da organização, assumindo a responsabilidade como custodiante de informações.
- Deverão ser protegidos por senha (bloqueados) todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
- Todos os recursos tecnológicos adquiridos pelo TroianoBranding devem ter imediatamente suas senhas padrões (default) alteradas.
- Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Acrescentamos ainda algumas situações em que é proibido o uso de computadores e recursos tecnológicos do TroianoBranding :

- Tentar ou obter acesso não autorizado a outro computador, servidor ou rede.
- Burlar quaisquer sistemas de segurança.
- Acessar informações confidenciais sem explícita autorização do proprietário.
- Vigiar secretamente outrem por dispositivos eletrônicos ou softwares, como, por exemplo, analisadores de pacotes (sniffers).
- Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado.

- Usar qualquer tipo de recurso tecnológico para cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
- Hospedar pornografia, material racista ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

## 10. DISPOSITIVOS MÓVEIS

O TroianoBranding deseja facilitar a mobilidade e o fluxo de informação entre seus colaboradores. Por isso, permite que eles usem equipamentos portáteis.

Quando se descreve "dispositivo móvel" entende-se qualquer equipamento eletrônico com atribuições de mobilidade de propriedade da instituição, ou aprovado e permitido por sua Gerência de Sistemas, como: notebooks, smartphones e pendrives.

No entanto, o uso de dispositivos como pendrives para troca de localização de arquivos é proibido desde máquinas com acesso ao servidor local do TroianoBranding . O uso em máquinas pessoais portáteis ou equipamentos sem acesso a rede está permitido. Casos emergenciais para uso destes dispositivos, a autorização de uso deverá ocorrer via sócios majoritários. (Anexo 2.4)

Essa norma visa estabelecer critérios de manuseio, prevenção e responsabilidade sobre o uso de dispositivos móveis e deverá ser aplicada a todos os colaboradores que utilizem tais equipamentos.

O TroianoBranding , na qualidade de proprietário dos equipamentos fornecidos, reserva-se o direito de inspecioná-los a qualquer tempo, caso seja necessário realizar uma manutenção de segurança.

Os colaboradores que receberem dispositivos móveis de propriedade do TroianoBranding devem assinar um Termo de Responsabilidade do aparelho.

O colaborador, também assume o compromisso de não utilizar, revelar ou divulgar a terceiros, de modo algum, direta ou indiretamente, em proveito próprio ou de terceiros, qualquer informação, confidencial ou não, que tenha ou venha a ter conhecimento em razão de suas funções no TroianoBranding , mesmo depois de terminado o vínculo contratual mantido com a organização.

O suporte técnico aos dispositivos móveis de propriedade do TroianoBranding e aos seus usuários deverá seguir o mesmo fluxo de suporte contratado pela organização.

Todo colaborador deverá utilizar senhas de bloqueio automático para seu dispositivo móvel. Não será permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um técnico da Gerência de Sistemas.

O colaborador deverá responsabilizar-se em não manter ou utilizar quaisquer programas e/ou aplicativos que não tenham sido instalados ou autorizados por um técnico da Gerência do TroianoBranding .

A reprodução não autorizada dos softwares instalados nos dispositivos móveis fornecidos pela instituição constituirá uso indevido do equipamento e infração legal aos direitos autorais do fabricante.

É permitido o uso de rede banda larga de locais conhecidos pelo colaborador como: sua casa, hotéis, fornecedores e clientes.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pelo TroianoBranding, notificar imediatamente seu gestor direto e a Gerência de Informação.

Também deverá procurar a ajuda das autoridades policiais registrando, assim que possível, um boletim de ocorrência (BO).

O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracterizará a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar ao TroianoBranding e/ou a terceiros.

O colaborador que deseje utilizar equipamentos portáteis particulares ou adquirir acessórios e posteriormente conectá-los à rede do TroianoBranding deverá submeter previamente tais equipamentos ao processo de autorização da Gerência de Informação.

Equipamentos portáteis, como smartphones, palmtops, pendrives e players de qualquer espécie, quando não fornecidos ao colaborador pela instituição, não serão validados para uso e conexão em sua rede corporativa.

## 11. DATACENTER

O acesso ao Datacenter somente deverá ser feito por sistema de autenticação. Deverá ser executada mensalmente uma auditoria nos acessos ao Datacenter por meio do relatório do sistema de registro.

Além disso, a área destinada ao Datacenter deve possuir acesso restrito, destinado somente ao Gerente de Informação e sócios majoritários.

O usuário "administrador" do sistema de autenticação ficará de posse e administração do coordenador de infraestrutura, de acordo com o controle de contas administrativas.

A lista de funções com direito de acesso ao Datacenter deverá ser constantemente atualizada, de acordo com os termos do Procedimento de Controle de Acesso ao Datacenter, e salva no diretório de rede.

Na eventualidade em que não existam colaboradores da área de tecnologia da informação em dias úteis, pessoas de outros departamentos deverão ser cadastradas no sistema de acesso para que possam exercer as atividades operacionais dentro do Datacenter, como: troca de fitas de backup, suporte em eventuais problemas, e assim por diante.

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

O Datacenter deverá ser mantido limpo e organizado. Qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração do Departamento de Apoio Administrativo.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável. A entrada ou retirada de quaisquer equipamentos do Datacenter somente se dará apenas diante de autorização formal dos sócios maioritários.

No caso de desligamento de empregados ou colaboradores que possuam acesso ao Datacenter, imediatamente deverá ser providenciada a troca do sistema de acesso.

## 12. BACKUP

Todos os backups devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de backup" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

As mídias de backup (como DAT, DLT, LTO, e outros) devem ser acondicionadas em local seco, climatizado, seguro (de preferência em cofres corta-fogo segundo as normas da ABNT) e distantes o máximo possível do Datacenter.

As fitas de backup devem ser devidamente identificadas, inclusive quando for necessário efetuar alterações de nome, e de preferência com etiquetas não manuscritas, dando uma conotação mais organizada e profissional.

O tempo de vida e uso das mídias de backup deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

É necessária a previsão, em orçamento anual, da renovação das mídias em razão de seu desgaste natural, bem como deverá ser mantido um estoque constante das mídias para qualquer uso emergencial.

Mídias que apresentam erros devem primeiramente ser formatadas e testadas. Caso o erro persista, deverão ser inutilizadas.

É necessário que seja inserido, periodicamente, o dispositivo de limpeza nas unidades de backup nos termos do Procedimento de Controle de Mídias de Backup.

Os backups imprescindíveis, críticos, para o bom funcionamento dos negócios do TroianoBranding, exigem uma regra de retenção especial, conforme previsto nos procedimentos específicos e de acordo com a Norma de Classificação da Informação, seguindo assim as determinações fiscais e legais existentes no país.

Na situação de erro de backup e/ou restore é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Caso seja extremamente negativo o impacto da lentidão dos sistemas derivados desse backup, eles deverão ser autorizados apenas

mediante justificativa de necessidade nos termos do Procedimento de Controle de Backup e Restore.

Testes de restauração (restore) de backup devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do backup.

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

Para formalizar o controle de execução de backups e restores, deverá haver um formulário de controle rígido de execução dessas rotinas, o qual deverá ser preenchido pelos responsáveis e auditado pela gerência de informação, nos termos do Procedimento de Controle de Backup e Restore.

Os colaboradores responsáveis descritos nos devidos procedimentos e na planilha de responsabilidade poderão delegar a um custodiante a tarefa operacional quando, por motivos de força maior, não puderem operacionalizar. Contudo, o custodiante não poderá se eximir da responsabilidade do processo.

## 13. INFORMAÇÕES CONFIDENCIAIS DE CLIENTES

Caso contratantes dos serviços do TroianoBranding exijam maior controle e confidencialidade de dados utilizados em projetos, a TroianoBranding segregará o acesso a determinados locais no servidor aos sócios majoritários e ao diretor direto responsável pelo projeto (Jacqueline de Bessa Santos ou Eduardo Martins de Araujo), permitindo que o acesso a tais informações seja apenas realizado mediante senha. Outros colaboradores não poderão ter acesso a tais informações.

Esta política será aplicada a cada cliente, caso seja solicitado, através de criação de diferentes senhas e determinação de

autorização de acesso aos documentos confidenciais. Em caso exemplo é o do Banco Itaú, cliente do TroianoBranding . Para acessar as pastas nos servidores que contém informações confidenciais providas pelo cliente, apenas os sócios majoritários e o diretor responsável pelos projetos vigentes terão acesso ao conteúdo no servidor. O controle de acesso será realizado através de senhas.

Os dados poderão ser enviados por email, que após salvamento, deverão ser excluídos imediatamente.

Após 15 dias da conclusão de um projeto, o TroianoBranding se responsabiliza pelo descarte de materiais confidenciais utilizados durante seu trabalho, através de equipamentos especializados para destruição digital e física. Tal prática será aplicada a todos os clientes que assim solicitarem. O descarte de conteúdos digitais ocorrerá através da exclusão permanente de documentos diretamente nos servidores onde os arquivos estavam previamente alocados. Dispositivos de armazenamento de dados serão eliminados através de um aparelho específico para destruição de papeis e tais dispositivos, como CD's e DVD's.

Além disso, para arquivamento e envios de documentos elaborados de/a clientes e institucionais, o TroianoBranding criou Recomendações de Classificação de seus documentos. Esta classificação se baseará por cor:

- **ROXO:** Documentos institucionais internos, confidenciais e direcionados para sócios e sócios majoritários.
- **VERMELHO:** Documentos de clientes com informações confidenciais sobre a empresa ou dados que devem permanecer protegidos durante o projeto em questão. Acesso apenas por parte de sócios majoritários e sócios diretamente responsáveis pelo projeto.

- **AMARELO:** Documentos de clientes ou institucionais confidenciais, mas de livre uso dentre os membros da equipe responsável pelo projeto.
- **VERDE:** Documentos públicos sem qualquer restrição.

**Volume e a variedade dos dados pessoais.**

O volume de dados e o conteúdo dependerá da natureza do projeto e portanto do perfil do público entrevistado no projeto. Para pesquisas qualitativas pedimos 15 contatos para cada entrevista realizada. Para pesquisas quantitativas com disparo a partir de base externa, pedimos 100 contatos potenciais para cada formulário a ser completado, sem garantia de respostas.

**Consentimento:**

A cada remessa de dados enviado à TroianoBranding é necessário o envio de uma manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para finalidade determinada no projeto em questão;

**Necessidade de envio de dados:**

A depender do perfil entrevistado em uma pesquisa, poderá ser feito o uso de paineis de consumidores, evitando a necessidade de envio de dados. Caso o perfil seja passível de ser identificado apenas através de dados provenientes do cliente, será necessário o envio de dados para a TroianoBranding.

## 14. PROCESSOS DE CONTRATAÇÃO

O TroianoBranding desenvolveu seu próprio processo de contratação de colaboradores e terceiros e se responsabiliza em divulgar seu processo a todos os colaboradores.No momento da contratação de um novo funcionário este deve receber itens de identificação, como crachá, login de acesso, informações quanto aos horários de entrada e saída, além de informações necessárias. Além disso, deve assinar o Contrato de Confidencialidade antes de receber autorização de acesso ao servidor.

## 15. SOBRE TREINAMENTOS E CAPACITAÇÕES

Um importante objetivo do TroianoBranding é promover a conscientização e capacitação dos colaboradores em relação à relevância da segurança da informação para o negócio do TroianoBranding , mediante campanhas, palestras, treinamentos e outros meios de endomarketing. Tais treinamentos e capacitações são feitos pela Diretora, que também exerce a função de responsável pela segurança da informação.

Organiza semanalmente reuniões com toda a equipe nas quais temas relacionados à Segurança da Informação são ministrados. Um item da pauta da reunião semanal é destinado a essa reciclagem e conscientização. Tais treinamentos e reuniões são conduzidas pelo gerente de segurança da informação e/ou pela diretora da empresa, responsável pela operação.
Além disso, o processo admissional inclui a entrega deste documento, assim como um breve Manual de Boas Vindas, que contém informações relevantes no que se refere a segurança de informações, como necessidade de travamento de telas, organização de pertences sobre a mesa de trabalho, entre outros. O Manual também contém informações relevantes sobre o TroianoBranding, amenidades sobre sua equipe e localização geográfica.

15.1. – SOBRE A POLÍTICA DE MESA LIMPA

O colaborador poderá manter sobre a mesa materiais relacionados à sua prática laboral, desde que não contenham informações confidenciais de clientes. Objetos de cunho afetivo ou apego emocional serão permitidos, desde que não apresentem risco aos equipamentos eletrônicos utilizados. Não será permitida a presença de documentos com dados pessoais, tais como exames médicos, dados bancários, entre outros. Para tais documentos disponibilizamos gavetas com chave. Também não será permitida também qualquer alimentação na mesa de trabalho ou qualquer prática cosmética que possa danificar a superfície (exemplo: uso de removedor de esmalte, entre outros).

15.2. – SOBRE A POLÍTICA DE TELA LIMPA

Solicitamos aos colaboradores que não guardem documentos pessoais nos seus respectivos computadores. Ainda sim, caso sejam necessários, todos os arquivos deverão ser armazenados fora da rede, após

Além disso, cada colaborador deverá realizar bloqueio de tela ao ausentar-se de seu local de trabalho. Tal medida de segurança evita que terceiros utilizem a máquina do colaborador ausente.

15.3. – SOBRE O GERENCIAMENTO DE CHAVES

Todos os colaboradores com cargos acima de analistas poderão deter controle de chaves de entrada do TroianoBranding . Disponibilizaremos 3 (três) chaves que corresponderão aos mecanismos da porta principal, que é segurada em duas etapas (porta 1 e porta 2).

A Porta 1 possui dois mecanismos de fechadura. A Porta 2 possui um mecanismo de fechadura, adicionando-se a restrição eletrônica que permite a entrada apenas com o crachá. A perda do crachá ou de alguma das chaves deverá ser reportada imediatamente aos sócios

majoritários para que todas as chaves ou código eletrônico do crachá sejam alterados.

15.4. – SOBRE A CHECAGEM DE EMAILS EXTERNA

A conta de email do TroianoBranding é provida pelo Google. Desta forma, o acesso ao email é possibilitado desde qualquer máquina conectada a internet. Basta que o colaborador acesse a página escrevendo no navegador o endereço: **mail.troianobranding.com.br.**
O colaborador deverá utilizar o mesmo login e senha que lhe foi indicado no momento de sua contratação. O Google solicita alteração de senha sazonalmente, para segurança da conta. Os acessos realizados fora do ambiente Troiano não possuem acesso aos servidores.

15.5. – SOBRE TREINAMENTOS E CONSCIENTIZAÇÃO

Semanalmente ocorrerão reuniões de acompanhamentos gerais dos projetos vigentes. Posteriormente, serão apresentados temas relacionados à segurança e capacitações durante 15 minutos.
Uma vez ao ano, durante a reunião oficial de resultados anual, este documento sobre a política de segurança será apresentada de forma completa a todos os funcionários.

15.6. – SOBRE A SEGURANÇA INTERNA

Afim de proteger os colaboradores de qualquer dano ou perda material, afim de proteger colaboradores de qualquer intervenção de intrusos não identificados, a TroianoBranding disporá de 2 câmeras de vigilância para tais fins. A primeira delas está instalada logo na entrada do estabelecimento (em conjunto com a segurança geral do edifício em que reside). A segunda câmera será instalada dentro do escritório, de forma que as mesas de trabalho, e salas de reunião estejam cobertas.

## 16. DISPOSIÇÕES FINAIS

Assim como a ética, a segurança deve ser entendida como parte fundamental da cultura interna do TroianoBranding . Ou seja, qualquer incidente de segurança subtende-se como alguém agindo contra a ética e os bons costumes regidos pela organização.

## 17. PENALIZAÇÕES

A violação à política, às normas ou aos procedimentos de segurança da informação ou a não aderência à política de segurança da informação da TroianoBranding são consideradas faltas graves, podendo ser aplicadas penalidades previstas em lei.