POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

ANYMALHAS

1. INTRODUÇÃO

Esta Política de Segurança da Informação tem como objetivo estabelecer normas, princípios, diretrizes, responsabilidades e procedimentos que assegurem a proteção das informações da Any Malhas.

A política visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

2. ESCOPO

Esta Política se aplica a todos os ativos de informação da Any Malhas, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações da empresa. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela empresa.

A PSI abrange áreas como administração, produção, logística, marketing, vendas, recursos humanos e tecnologia da informação, cobrindo os sistemas de gestão corporativa (ERP, CRM e sistemas de controle de produção), redes locais e virtuais (LAN, VPN), redes sem fio (Wi-Fi) e serviços hospedados em nuvem. Além disso, estende-se às informações sensíveis e estratégicas da empresa, incluindo dados operacionais, financeiros, de clientes e fornecedores, bem como documentos armazenados em repositórios digitais ou físicos. Também engloba todos os dispositivos utilizados na operação, como computadores, notebooks, equipamentos de rede, assegurando que sejam protegidos conforme os padrões estabelecidos.

3. TERMOS E DEFINIÇÕES

Abaixo seguem, em ordem alfabética, os principais conceitos referidos neste documento, de forma a evitar dificuldades de interpretação ou ambiguidades:

- Algoritmo: conjunto das regras e procedimentos lógicos perfeitamente definidos que levam à solução de um problema em um número finito de etapas;
- Ameaça: causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização (ABNT, 2005);
- Antispyware: software de segurança que tem o objetivo de detectar e remover softwares maliciosos;
- Assinatura Digital: mecanismo criptográfico que tem por objetivo assinar documentos digitalmente;
- Ativo de Informação: os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que têm acesso a eles;
- Autenticidade: propriedade que determina que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- Backup: é o processo de cópia de dados de um dispositivo de armazenamento para outro com o objetivo de proporcionar a proteção contra a perda dos originais;
- Certificação Digital: é um arquivo eletrônico que serve como identidade virtual para uma pessoa física ou jurídica, e por ele podem ser feitas transações online com garantia de autenticidade e proteção das informações trocadas;
- Classificação da informação: processo que tem como objetivo identificar e definir níveis e critérios adequados para a proteção das informações, de acordo sua importância para as organizações;
- Código Malicioso: tipo de código de computador ou script da Web nocivo que tem como objetivo criar vulnerabilidades no sistema, violações de segurança, roubo de dados e informações, além de outros danos possíveis;

- Confidencialidade: somente pessoas devidamente autorizadas pelo órgão devem ter acesso à informação;
- Continuidade de Negócios: Capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação de atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definida);
- Controle de Acesso: processo por meio do qual os acessos aos sistemas e a seus respectivos dados são autorizados ou negados; os acessos autorizados e, em alguns casos, também os negados ficam registrados para posterior auditoria;
- Criptografia: mecanismo de segurança e privacidade que torna determinada comunicação (textos, imagens, vídeos, entre outros) ininteligível para quem não tem acesso aos códigos de "tradução" da mensagem;
- Disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- Dispositivos Móveis: equipamentos portáteis dotados de capacidade computacional ou dispositivos removíveis de memória para armazenamento;
- Engenharia Social: habilidade de conseguir acesso a informações confidenciais ou a áreas importantes de uma instituição por meio de habilidades de persuasão;
- FTP (File Transfer Protocol): protocolo que permite a transferência de arquivos entre computadores conectados à Internet;
- Gestão de Risco: avalia os riscos relativos à segurança, disponibilidade de dados e desempenho dos ativos de informação e a conformidade com exigências regulatórias e legais;
- Gestão de Segurança de Informação e Comunicação: processo que visa a proteção dos ativos de informação contra a negação de serviço a usuários autorizados, assim como contra a intrusão e a modificação desautorizada de dados armazenados ou em trânsito, inclusive a segurança dos recursos humanos, da documentação, das áreas e das instalações computacionais e de comunicações;
- Informação: dados estruturados, organizados e processados, apresentados dentro do contexto, o que o torna relevante e útil para a pessoa que o deseja.

- Integridade: alterações, supressões e adições nas informações devem ser realizadas apenas sob processos legalmente válidos, por pessoas devidamente autorizadas para tal (autênticas). Garante que as ações que modifiquem as informações não ocorram de forma acidental ou não autorizada;
- Incidente: qualquer evento adverso, confirmado ou sob suspeita, relacionado a segurança dos sistemas, das informações ou das redes de computadores; x) Impacto: mudança adversa no nível obtido dos objetivos do negócio (ABNT, 2008); y)
- Login: processo para acessar um sistema informático restrito feita por meio de autenticação ou identificação do utilizador;
- Mídia Removível: tipo de memória que pode ser removida do seu aparelho de leitura, conferindo portabilidade para os dados que carrega;
- Plano de Continuidade de Negócio (PCN): documento que estabelece mecanismos para restabelecer a atividade de uma organização, em caso de interrupção;
- Programas Antivírus: programas usados para proteger e prevenir computadores e outros aparelhos de códigos ou vírus, a fim de dar mais segurança ao usuário;
- Risco: efeito da incerteza nos objetivos (ABNT ISO GUIA 73,2009);
- Segurança da Informação e das Comunicações: ações que visam viabilizar e assegurar disponibilidade, integridade e confidencialidade das informações;
- Servidor: software ou hardware que fornece um ou mais serviços a uma rede de computadores;
- Software: programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador;
- Termo de Responsabilidade e Sigilo: documento pelo qual o empregado ou colaborador se compromete a não revelar as informações de caráter secreto, sigiloso e confidencial da Companhia;
- Vírus de Computador: software malicioso capaz de infectar um sistema, fazer cópias de si e se espalhar para outros computadores e dispositivos;

- Wireless: tecnologia que significa “sem fio” (em livre tradução), e possibilita a transmissão da conexão entre pontos distantes sem precisar usar fios (como ocorrem em telefones sem fio, rádios ou celular).

4. PRINCÍPIOS

O conjunto de documentos que compõe esta PSI deverá se guiar pelos seguintes princípios:

1. Simplicidade: a complexidade aumenta a chance de erros, portanto, todos os controles de segurança deverão ser simples e objetivos;
2. Privilégio Mínimo: usuários devem ter acesso apenas aos recursos de tecnologia da informação necessários para realizar as tarefas que lhe foram designadas;
3. Segregação de função: funções de planejamento, execução e controle devem ser segregadas, de forma a reduzir oportunidades de modificação, uso indevido, não autorizado ou não intencional dos ativos, bem como para permitir maior eficácia dos controles de segurança;
4. Auditabilidade: todos os eventos significantes de usuários e os processos devem ser rastreáveis até o evento inicial por meio de registro consistente e detalhado;
5. Resiliência: os controles de segurança devem ser projetados para que possam resistir ou se recuperar dos efeitos de um desastre;
6. Defesa em profundidade: os controles de segurança devem ser concebidos em múltiplas camadas, de modo a prover redundância para que, no caso de falha, outro controle possa ser aplicado.

5. OBJETIVOS

São objetivos desta Política:

1. Proteger a informação da Any Malhas de forma a garantir sua confiabilidade, autenticidade e integridade;
2. Estabelecer diretrizes para a utilização dos recursos de informação, serviços de redes de dados, estações de trabalho, Internet, telecomunicações, correio eletrônico e outros;
3. Designar papéis e responsabilidades relativas à segurança da informação na empresa;
4. Ser transparente e inclusiva, de forma a conscientizar todos os funcionários da Any Malhas sobre a importância das informações e de suas vulnerabilidades;
5. Promover e desenvolver a cultura de segurança da informação em todos os níveis da empresa;
6. Ser parte integrante dos processos organizacionais;
7. Possibilitar a criação de controles e promover a otimização dos recursos de tecnologia da informação.
8. Assegurar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes

6. DIVULGAÇÃO E ACESSO À POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação deve ser divulgada a todos os funcionários da Any Malhas e disposta de maneira que seu conteúdo possa ser consultado a qualquer momento.

Os Procedimentos de Segurança da Informação ficarão disponíveis na rede interna da empresa, e devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

7. ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

7.1 GERAIS

Cabe a todos os funcionários, diretores/presidente, estagiários, prestadores de serviço e terceirizados da Any Malhas:

a. Cumprir fielmente a Política e os Procedimentos de Segurança da Informação da Any Malhas;

b. Manter-se atualizado em relação a esta Política, demais normas e procedimentos relacionados, buscando informação junto a seu superior ou junto à autoridade competente sempre que não estiver absolutamente seguro quanto a obtenção, uso e/ou descarte de informações;

c. Promover a segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados, credenciais de acesso e quaisquer informações a que tenha acesso em virtude do cargo que ocupa;

d. Utilizar de forma ética, legal e consciente os recursos computacionais e informacionais da Any Malhas, estando ciente de que sua estrutura não poderá ser utilizada para fins particulares e que quaisquer ações que tramitem em sua rede poderão ser auditadas;

e. Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pela Any Malhas;

f. Cumprir as leis e as normas que regulamentam os aspectos da propriedade intelectual;

g. Comunicar imediatamente à Assessoria de Informática (ASINF) qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos;

h. Ser responsável por qualquer prejuízo ou dano que vier a sofrer ou causar à Any Malhas, em decorrência da não obediência às diretrizes e às normas referidas na Política de Segurança da Informação e das Comunicações e às normas e aos procedimentos específicos dela decorrentes.

Adicionalmente, são definidas as seguintes responsabilidades e atribuições específicas relacionadas à segurança da informação:

7.2 ALTA GESTÃO

Em relação à segurança da informação, cabe à alta gestão:

a. Aprovar a Política de Segurança da Informação e suas revisões.

7.3 COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)

A gestão da segurança da informação na Any Malhas será realizada por comitê multidisciplinar, chamado COMITÊ de SEGURANÇA DA INFORMAÇÃO - CSI.

Cabe ao CSI:

a. Propor normas relativas à segurança da informação e de comunicações;

b. Assessorar a implementação das ações de segurança da informação e comunicações da empresa;

c. Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e de comunicações;

d. Analisar os casos de violação da Política de Segurança da Informação, encaminhando-os à autoridade competente, quando for o caso;

e. Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;

f. Determinar a elaboração de relatórios, levantamentos e análises que deem suporte à gestão de segurança da informação e à tomada de decisão;

g. Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;

h. Propor a relação de “responsáveis” pelas informações da Any Malhas.

7.4. ÁREA DE TECNOLOGIA DA INFORMAÇÃO (AT)

Cabe à Assessoria de Informática (ATI):

a. Propor ajustes, aprimoramentos e modificações de regras, em relação à Segurança da Informação;

b. Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação da Any Malhas, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;

c. Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso lógico da Any Malhas, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;

d. Prover todas as informações de gestão de segurança da informação solicitadas pelo CSI, podendo solicitar informações às demais áreas da Any Malhas (diretorias, coordenações, entre outras), caso necessário;

e. Prover ampla divulgação da Política de Segurança da Informação para todos os funcionários da Any Malhas;

f. Oferecer orientação e treinamento sobre a Política de Segurança da Informação a todos os funcionários da Any Malhas;

g. Realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política de Segurança da Informação;

h. Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações da Any Malhas;

i. Estabelecer mecanismo de registro e controle de não-conformidades com a Política de Segurança da Informação, solicitando que o CSI tome as providências.

7.5 RESPONSÁVEL PELA INFORMAÇÃO

O responsável pela informação é um diretor ou um coordenador da Any Malhas, formalmente indicado pela Presidência, responsável por concessão, manutenção, revisão e cancelamento de autorizações de acesso ao conjunto de informações pertencentes à sua área de atuação.

Cabe ao responsável pela informação:

a. Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções da Any Malhas às autorizações de acesso concedidas;

b. Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política e os Procedimentos de Segurança da Informação da Any Malhas;

c. Manter registro e controle atualizados, em relação a todas as liberações de acesso concedidas. Deve ser determinada, sempre que necessário, a pronta suspensão ou a alteração de tais liberações;

d. Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;

e. Solicitar relatórios de controle de acesso com o objetivo de identificar desvios em relação à Política de Segurança da Informação, tomando as ações corretivas necessárias;

f. Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;

g. Participar, sempre que convocado, das reuniões do COMITÊ DE SEGURANÇA DA INFORMAÇÃO, prestando os esclarecimentos solicitados.

8. DIRETRIZES GERAIS DE SEGURANÇA DA INFORMAÇÃO

Neste capítulo, são apresentadas as diretrizes gerais da Política de Segurança da Informação da Any Malhas.

8.1. ADOÇÃO DE COMPORTAMENTO SEGURO

Independentemente do meio ou da forma em que se encontre, a informação está presente no dia a dia de todos os empregados da Any Malhas Têxtil. A proteção das informações depende de práticas seguras adotadas por todos os colaboradores. Destaques:

a. Todos os funcionários e prestadores de serviços devem manter uma atitude proativa e engajada na proteção das informações;
b. Todos os funcionários da Any Malhas devem compreender as ameaças externas e internas que podem afetar a segurança da informação na empresa, tais como vírus de computador, interceptação de mensagens eletrônicas, bem como engenharia social e outras artimanhas frequentemente utilizadas para a roubar senhas e obter acesso a sistemas de informação;
c. Todos os recursos de informação da Any Malhas devem ser projetados e utilizados para a consecução dos objetivos finalísticos da empresa. É vedada a utilização desses recursos para fins particulares;
d. Toda informação produzida ou recebida pelos funcionários, terceirizados, fornecedores e prestadores de serviço, em resultado da função exercida e/ou atividade profissional contratada, no âmbito dela, é de propriedade da empresa. Quaisquer exceções devem ser devidamente formalizadas;
e. Cada usuário é responsável pela segurança das informações dentro da Any Malhas;
f. Todo tipo de acesso à informação da Any Malhas que não for explicitamente autorizado é proibido;
g. As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive funcionários da própria empresa), anotadas em papel ou em sistema visível ou de acesso não protegido;
h. Qualquer tipo de dúvida sobre a Política de Segurança da Informação deve ser imediatamente esclarecida com o COMITÊ DE SEGURANÇA DA INFORMAÇÃO ou com a Área de Tecnologia Da Informação (ATI).

8.2 ADOÇÃO DE SISTEMA DE CLASSIFICAÇÃO DA INFORMAÇÃO

Todas as suas informações sejam categorizadas e disponibilizadas apenas às pessoas que tenham acesso.

As informações serão classificadas em três categorias:

1. Confidencial: Divulgar pode causar danos a empresa.
2. Restrita: Internas, acessíveis apenas por equipes específicas.
3. Pública: Podem ser compartilhadas externamente sem prejuízo.

8.3 ADOÇÃO DE INVENTÁRIO DA INFORMAÇÃO

a. As áreas de negócio devem manter um inventário atualizado que identifique e documente a existência e as principais características de todos os seus ativos de informação (base de dados, arquivos, diretórios de rede, trilhas de auditoria, códigos fonte de sistemas, documentação de sistemas, manuais, planos de continuidade, entre outros);
b. As informações inventariadas devem ser associadas a um "responsável", que deverá ser diretor ou coordenador da Any Malhas, formalmente designado pela Presidência como responsável pela autorização de acesso às informações sob a sua responsabilidade;
c. O COMITÊ DE SEGURANÇA DA INFORMAÇÃO será responsável por verificar a conformidade do inventário elaborado pelas coordenações, de modo a orientá-las sobre a correção de eventuais falhas.

8.4 ACESSO À INFORMAÇÃO

A informação é o ativo mais valioso de qualquer instituição e, como tal, deve ser protegida.

a. A Any Malhas deve fornecer informações aos cidadãos, desde que não exista impedimento legal relativo à confidencialidade da informação;
b. É vedado às pessoas físicas ou jurídicas que de alguma forma estão relacionadas com a Any Malhas divulgar quaisquer informações a que tenham acesso em virtude do cargo sem autorização por escrito de autoridade competente da Any Malhas sob pena de aplicação das sanções cabíveis;
c. É vedada a alteração ou a deturpação do teor de quaisquer documentos, bem como a retirada das instalações da Any Malhas sem estar devidamente autorizado, de qualquer documento ou bem pertencente ao patrimônio da empresa;
d. A liberação de Acesso Físico ou Lógico a qualquer sistema de informação, documento ou recurso de processamento e ou armazenamento de dados da Any Malhas somente será efetuado após a concordância do usuário com o Termo de Responsabilidade e Sigilo da empresa, sendo completamente vedada a liberação de acesso a qualquer recurso informacional sem a assinatura do documento.

8.5 SEGURANÇA FÍSICA

A proteção do ambiente da Any Malhas deve prevenir a perda, dano ou comprometimento dos ativos e a interrupção das atividades do negócio. Devem ser adotadas medidas contra riscos como roubo, fogo, explosões, falhas no abastecimento de água, danos elétricos (curtos-circuitos ou interferências), intempéries (raios, ventos fortes, granizo), impactos de veículos ou aeronaves, vandalismo, sabotagem, e infestações por fungos, roedores ou insetos.

a. Áreas cuja natureza ou o manuseio de documentos e a utilização dos recursos de processamento da informação não exijam proteção são consideradas áreas de acesso livre;
b. Áreas que abriguem em seu interior documentos, processos, recursos de processamento da informação ou reuniões e eventos de caráter reservado devem ser consideradas áreas de acesso restrito;
c. A localização das áreas de acesso restrito, bem como a sua capacidade de resistência a acessos não autorizados devem ser adequados ao grau de confidencialidade de documentos e informações existentes em seu interior;

8.6 MEIOS DE INFORMAÇÃO

Faz-se necessário proteger e controlar os meios de armazenagem de informações contra danos que possam prejudicar as atividades do negócio:

a. Todos os meios de informação devem ser armazenados de forma segura, seguindo as recomendações dos fabricantes;
b. Informações confidenciais da Any Malhas não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel, entre outros) sem as devidas autorizações e proteções especificadas por Diretrizes ou Normas;
c. Os meios que possuírem informações sensíveis devem ser descartados de forma segura, como, por exemplo: fragmentação de listagens, eliminação de

informações magnéticas (de forma a não ter como se recuperar), desmagnetização de meios defeituosos, entre outros.

8.7 CRIPTOGRAFIA

A criptografia é uma grande aliada da segurança da informação, e poderá ser utilizada para manter a confidencialidade, a autenticidade e a integridade das informações pertencentes à Any Malhas.

a. O uso de criptografia poderá ser utilizado somente quando aprovado pela ATI, ou seja, em casos específicos, devidamente formalizados, e seguindo normas ou procedimentos relativos ao manuseio de informações classificadas;
b. Certificação digital e assinatura digital poderão ser utilizados como forma de garantir a segurança nas comunicações institucionais.

8.8 CONTROLE DE ACESSO

Todo acesso às informações e aos ambientes lógicos da Any Malhas deve ser controlado, de forma a garantir permissão apenas às pessoas autorizadas pelo respectivo proprietário da informação, observando as seguintes diretrizes:

a. Procedimento formal de concessão e cancelamento de autorização de acesso aos sistemas de informação;
b. Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;

c. Verificação se o nível de acesso concedido é apropriado ao propósito da atividade exercida e se é consistente com a Política de Segurança da Informação e com suas Normas;
d. Remoção imediata de autorizações dadas a usuários afastados ou desligados da empresa, ou que tenham mudado de função;
e. Processo de revisão periódica das autorizações concedidas;
f. Política de atribuição, manutenção e uso de senhas.

O controle de acesso deverá considerar e respeitar o princípio do menor privilégio, em que cada usuário deverá possuir o mínimo de privilégios necessários para desempenhar suas atividades.

8.9 USO E ACESSO À INTERNET E À INTRANET

A utilização dos recursos informacionais da empresa deve ser pautada de forma ética e profissional, sempre priorizando a proteção dos ativos de informação da Any Malhas.

a. O uso de recursos e serviços de TI da empresa é restrito a funcionários e usuários autorizados. A Any Malhas pode monitorar, restringir, capturar e auditar o uso desses recursos a qualquer momento para garantir conformidade com sua Política de Segurança da Informação;
b. É proibido utilizar a Internet e recursos computacionais para acessar ou compartilhar conteúdos não relacionados ao trabalho ou ilegais, como arquivos protegidos por direitos autorais ou via *Torrent*. Exceções para sites bloqueados devem ser aprovadas pela ATI;
c. Privilégios administrativos locais só podem ser concedidos com aprovação formal da ATI. Justificativas para exceções devem ser solicitadas pela chefia imediata e avaliadas pela ATI;
d. É proibido utilizar qualquer meio para burlar ou fraudar os sistemas de segurança da informação implementados na Any Malhas;
e. Usuários devem reportar imediatamente falhas ou incidentes de segurança à ATI;

8.10 CORREIO ELETRÔNICO

O correio eletrônico é uma ferramenta de trabalho disponibilizada para todos os usuários da Any Malhas, independentemente de seu vínculo funcional. Dessa forma, ela deverá ser

utilizada somente para fins corporativos e relacionados às atividades do funcionário, sendo vedada a sua utilização para tratar de assuntos de cunho pessoal. É proibido abrir anexos de fontes desconhecidas para evitar ataques de *phishing*.

8.11 PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

Devem ser implementadas medidas de prevenção e detecção automática de softwares maliciosos, assim como programas de conscientização dos usuários. Os usuários devem ser orientados de que a prevenção é sempre a melhor solução.

a. Os recursos de TI da Any Malhas devem utilizar soluções de detecção e bloqueio de programas maliciosos, como antivírus, *antispyware* e ferramentas de análise de e-mails e navegação;
b. A instalação, configuração e atualização desses softwares são responsabilidade exclusiva da ATI, que deve garantir sua execução periódica e abrangente;
c. Mídias removíveis ou arquivos de origem desconhecida devem ser inspecionados antes de serem utilizados;
d. A instalação de softwares nos dispositivos da empresa é permitida apenas com autorização prévia da ATI, devendo ser utilizados apenas softwares licenciados e homologados;

8.12 DATACENTER (CENTRO DE PROCESSAMENTO DE DADOS)

Regras para a administração do centro de processamento de dados da empresa poderão ser fixadas em Enunciado Normativo próprio, considerando as seguintes diretrizes gerais:

a. O datacenter deve possuir sistema de tranca e monitoramento 24 horas por dia, permitindo acesso apenas a pessoas autorizadas e credenciadas;
b. A entrada de terceiros só será permitida com acompanhamento de um funcionário da ATI;
c. O acesso de usuários desligados ou não autorizados deve ser imediatamente revogado;

8.13 BACKUP (CÓPIA DE SEGURANÇA)

Os procedimentos próprios ao serviço de backup (cópia de segurança) organizacional deverão ser fixados em Enunciado Normativo complementar, considerando as seguintes diretrizes gerais:

a. O backup institucional será realizado nos servidores da Any Malhas. Dados armazenados localmente em estações de trabalho são de responsabilidade do usuário, e a empresa não se responsabiliza por sua perda;
b. Documentos relacionados às atividades institucionais devem ser armazenados exclusivamente nos servidores da empresa. Arquivos armazenados localmente não serão incluídos na rotina de *backup*, e sua perda será de responsabilidade do usuário;
c. Arquivos pessoais ou não relacionados às atividades institucionais não devem ser copiados para os drives de rede. Caso identificados, poderão ser removidos sem aviso prévio;
d. O armazenamento de informações corporativas em locais não autorizados, como nuvens públicas, computadores pessoais ou servidores de terceiros, é proibido, salvo autorização expressa da ASINF.

8.14 MONITORAMENTO, CONTROLE E AUDITORIA

Todos os funcionários da Any Malhas devem ter ciência de que o uso da rede, das informações e dos sistemas de informação da empresa pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais. Visando efetivar esse controle, a Any Malhas poderá:

a. Monitorar dispositivos, e-mails, conexões de internet e outros componentes da rede, rastreando informações geradas ou trafegadas para identificar acessos;

b. Divulgar informações de auditorias quando exigido judicialmente ou autorizado por autoridade competente;
c. Realizar inspeções físicas nos equipamentos da empresa;
d. Remover softwares ou sistemas que representem riscos ou estejam em desacordo com as políticas da empresa;

8.15 TRATAMENTO DE INCIDENTES EM REDES COMPUTACIONAIS

No Tratamento de Incidentes em redes computacionais, a equipe técnica da ASINF deverá considerar as seguintes diretrizes:

a. Investigar, registrar e solucionar incidentes, preservando a disponibilidade, integridade, confidencialidade e autenticidade das informações;
b. Registrar todos os incidentes notificados ou detectados para manter um histórico das atividades realizadas;
c. Garantir que os usuários comuniquem falhas ou incidentes imediatamente à ATI;
d. Acionar as autoridades competentes em casos de indícios de ilícitos criminais, em conjunto com o CSI, conforme necessário.

8.16 GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O CSI deverá realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação da Any Malhas, que servirá como base, entre outros, para o Plano de Continuidade de Negócios institucional (PCN).

8.17 GESTÃO DE CONTINUIDADE DE NEGÓCIOS

A Any Malhas deverá criar, manter e testar periodicamente uma estratégia de continuidade dos processos críticos institucionais, pronta para operar em caso de interrupção total ou parcial de suas atividades.

9. VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

O descumprimento ou a inobservância de quaisquer regras ou diretrizes definidas nesse instrumento e em suas normas complementares constituem falta grave, sobre as quais a Any Malhas aplicará todas as medidas cabíveis nos âmbitos administrativo, civil e judicial.

São considerados comportamentos contrários à Política de Segurança da Informação:

a. Praticar atos irregulares que causem prejuízo à Any Malhas, como abuso de confiança, uso indevido de senhas ou meios fraudulentos para obter vantagens;
b. Manipular informações, sistemas ou redes de forma indevida, causando danos à empresa, funcionários ou terceiros;
c. Utilizar recursos da empresa para fins particulares sem autorização;

d. Apagar, destruir, modificar ou inutilizar dados, programas ou documentos sem permissão;
e. Obter, fornecer ou manter acessos não autorizados a sistemas, dados ou informações sigilosas;
f. Inserir programas ou dados maliciosos em sistemas para comprometer sua funcionalidade;
g. Realizar download ou upload de conteúdos não autorizados, como jogos, filmes ou material impróprio;
h. Distribuir cópias não autorizadas de arquivos, softwares ou ativos da empresa;
i. Utilizar correio eletrônico para fins alheios às atividades da empresa, incluindo mensagens de teor político, racista, preconceituoso ou pornográfico;
j. Burlar ou fraudar os sistemas de segurança implementados na empresa;
k. Descumprir padrões e procedimentos específicos para uso de recursos e serviços de rede corporativa.

10. DISPOSIÇÕES FINAIS

Para a uniformização da informação organizacional, esta Política de Segurança da Informação deverá ser distribuída a todos os gestores, funcionários, terceirizados e prestadores de serviço da Any Malhas, a fim de que seja conhecida e cumprida.

Esta PSI entra em vigor na data de sua publicação e será revisada periodicamente para garantir sua adequação às necessidades da Any Malhas.

11. REFERENCIAIS

BASTA, Alfred; BASTA, Nadine; BROWN, Mary. Segurança de computadores e teste de invasão. São Paulo (SP): Cengage Learning, c2015. E-book (355 p.) ISBN 9788522121366.

BIRKNER, Matthew H. Projeto de Interconexão de Redes: Cisco Internetwork Design.

CID. Editora Pearson, 636 p. ISBN 9788534614993.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Regula o tratamento de dados pessoais e estabelece diretrizes de proteção e privacidade no Brasil.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Marco Civil da Internet. Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

CASSIANA FAGUNDES DA SILVA. Projeto estruturado e gerência de redes. Contentus, 91 p. ISBN 9786557454633.

DASWANI, Neil; KERN, Christoph; KESAVAN, Anita. Foundations of security: what every programmer needs to know. Berkeley, CA: Apress; New York: Distributed to the book trade worldwide by Springer-Verlag, c2007. xxvii, 290 p. ISBN 1590597842.

GOODRICH, Michael T. Introdução à segurança de computadores. Porto Alegre: Bookman, 2012. ISBN 9788540701939.

ISO/IEC 27001:2013. Padrão internacional para sistemas de gestão de segurança da informação.

LYRA, Maurício Rocha. Segurança e auditoria em sistemas de informação. 2. ed. Rio de Janeiro (RJ): Ciência Moderna, 2017. xii, 316 p. ISBN 9788539907731., Nº de Exemplares: 2., Nº de Exemplares: 2.

PAQUET, Catherine; Teare, Diane. Construindo Redes Cisco Escaláveis. Editora Pearson, 786 p. ISBN 9788534614924.