1 - OBJETIVO

Prover orientação e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes para a melhor utilização dos recursos disponíveis e entrega de valor para o cliente, contribuindo assim para a sustentabilidade financeira da organização.

2 - ESCOPO

Esta "Política de Segurança" mantém a integridade na prestação do serviço em todas as unidades da Algar Tech de acordo com as estratégias da empresa, legislação vigente e requisitos contratuais.

As diretrizes aqui estabelecidas devem ser seguidas por todos os associados, prestadores de serviços, fornecedores, estagiários, contratados, parceiros, e clientes que utilizam informações da Algar Tech. Exceções somente quando aprovado pelo corpo diretivo.

3 - DEFINIÇÃO

3.1 - Segurança da Informação

São esforços contínuos para a proteção dos ativos de informação contra vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco à organização, auxiliando a Algar Tech a cumprir sua missão;

É obtida a partir da implementação de objetivos de controle e controles adequados para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

3.2 – SGSI

Sistema de Gestão de Segurança da Informação.

4 - RESPONSABILIDADES

A Algar Tech, por intermédio da sua presidência e diretoria afirma seu compromisso para com à segurança da informação, leis e regulamentações aplicáveis ao negócio, a partir desta "Política de Segurança" e estabelece no documento "Funções e Responsabilidades pela Segurança da Informação" disponível para consulta na intranet Algar Tech>Políticas e Diretrizes, as responsabilidades relativas à segurança da informação para as principais funções envolvidas com o sistema de gestão de segurança da informação.

5 - PRINCIPAIS ÁREAS DO SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

- Presidência;
- Tecnologia da Informação;
- Gestão por Processos;
- Talentos Humanos;
- Operações.

6 - OBJETIVO DA SEGURANÇA

Garantir o índice de confiabilidade da segurança da informação, refletida nos negócios da organização.

7 - DESCRIÇÃO

7.1 - Pessoas

7.1.1 - Associados Algar Tech

a) Todo associado deve ter conhecimento do Código de Conduta do Grupo Algar e do Treinamento de Conscientização em Segurança da Informação, e ser coerente com os mesmos;
b) Todo associado deve assinar o "Termo de Confidencialidade" no ato de sua admissão ou sempre que for solicitado pela empresa;
c) É vedado a qualquer associado à utilização indevida de informações da empresa e/ou de seus clientes, transmitirem-nas para a concorrência, utilizá-las para benefício próprio e/ou armazenar arquivos e e-mails de forma imprópria;
d) A Algar Tech pode receber e armazenar automaticamente informações sobre as atividades de qualquer pessoa que utilize seus recursos, incluindo endereço IP, usuário, aplicativos, tela/página e conversação efetuada dentro ou por meio da empresa;
e) Qualquer ID de autenticação (usuário e senha) na rede corporativa ou em aplicativos fornecidos pela Algar Tech é pessoal e intransferível e cada usuário será responsável pelo armazenamento e uso do mesmo;
f) Ao final do vínculo empregatício e/ou contratual, dos associados e/ou prestadores de serviço, a Algar Tech desabilitará todos os ID's de autenticação utilizados durante a prestação de serviço.

7.1.2 - Fornecedor e Terceiros

a) Toda criação, invenção e desenvolvimento de ideias, processos, sistemas, produtos e serviços realizados durante a prestação de serviço na Algar Tech devem ser transferidos à mesma. As exceções devem ser definidas em acordos especiais conforme previsto no Código de Conduta Algar;

b) É vedado a qualquer pessoa prestadora de serviço utilizar indevidamente informações da empresa e de seus clientes, transmiti-las para concorrência, utilizá-las para benefício próprio e/ou armazenar arquivos e e-mails de forma imprópria;
c) Recebendo acesso a qualquer recurso da Algar Tech, o prestador de serviço estará sujeito às políticas e diretrizes internas da organização e a todos os critérios estabelecidos nas cláusulas de confidencialidade disponíveis no contrato de prestação de serviço assinado no ato da contratação;
d) Ao final do vínculo contratual, o responsável pelo contrato dos prestadores de serviço da Algar Tech deve garantir que os ID's de autenticação utilizados durante os trabalhos sejam devidamente desabilitados.

7.2 - Ativos

a) Todo associado é responsável por zelar pelo bom funcionamento e pela integridade de qualquer recurso provido pela empresa para realização de suas atividades e, quando aplicável, deve assinar um termo de compromisso de uso de recurso;
b) Todo produto ou equipamento da Algar Tech que se faça necessário transportar, deve ser acomodado de forma segura, garantindo assim sua integridade física e lógica quando aplicável;
c) Na rede corporativa, não é permitida a utilização de computadores pessoais. Salvo exceções previamente autorizadas pela área de segurança da informação;
d) O acesso por meio de dispositivos móveis (smartphones, celulares, tablets, ipad's e etc.) será permitido através do SSID AlgarTec - Mobile, na qual permite somente o uso de aplicações necessárias para este tipo de dispositivo. Para estes casos o único responsável por zelar pelo funcionamento destes ativos é o associado proprietário do equipamento;
e) Toda entrada, movimentação e saída de ativos das unidades da Algar Tech devem obedecer aos procedimentos internos da empresa.

7.3 - Processos

a) A empresa deve mapear todos os processos críticos ao negócio e realizar uma análise e avaliação de riscos com controles e tratativas. Os mesmos devem ser conhecidos, aprovados e aceitos pelo corpo diretivo;
b) O mapeamento dos processos críticos deve ser revisado sempre que mudanças de impacto ocorram no ambiente.

7.4 - Risco

a) A empresa deve definir e seguir uma única metodologia de análise e avaliação de riscos para os processos e tecnologias existentes e seus resultados devem ser comparáveis e reproduzíveis;

b) A análise e avaliação de risco deve ser capaz de identificar as vulnerabilidades, ameaças, impactos e níveis de risco aceitáveis para os ativos, pessoas, informação, sistemas, aplicação e mapeamento dos principais processos do negócio de acordo com as estratégias da empresa, legislação vigente e requisitos contratuais;

c) A análise e avaliação de risco deve ser revisada pelo menos uma vez a cada ano, ou sempre que mudanças de impacto ocorram no ambiente.

7.5 - Informação

a) O acesso a informações da Algar Tech ou de seus clientes em seu ambiente empresarial e computacional é restrito e será disponibilizado somente ao perfil de pessoas formalmente autorizadas;

b) Todas as cláusulas de confidencialidade acordadas com os clientes em relação às suas informações devem ser respeitadas pelos associados Algar Tech ou terceiros a serviços que porventura venham a ter acesso a estas informações;

c) É expressamente proibido para todo usuário que não possua autorização formal de uso, o acesso a quaisquer sistemas e aplicativos ou mesmo a simples tentativa;

d) Toda e qualquer informação gerada dentro da Algar Tech ou em seu nome, que seja fruto de trabalho dos associados, fornecedores ou prestadores de serviço são de direito da Algar Tech e somente ela pode determinar seu destino e finalidade;

e) Toda criação, invenção e desenvolvimento de ideias, processos, sistemas, produtos e serviços, criados no âmbito do trabalho ou das responsabilidades e missão da função ou cargo do associado na empresa, devem ser transferidos à Algar Tech, com as exceções definidas em acordos especiais conforme previsto no Código de Conduta Algar;

f) É proibida a divulgação* de qualquer informação da empresa ou de seus clientes para outrem que não pertença ao mesmo grupo de trabalho, em meios de comunicação públicos (incluindo fotos/filmagens em redes sociais) ou internos, sem autorização prévia ou que esteja vinculado ao termo de responsabilidade e confidencialidade, salvo exceções quando previstas em contrato;

g) *A divulgação em canais públicos inclui comentários em redes sociais de uso particular do associado. Qualquer divulgação deve ser aprovada previamente pela área de marketing ou endomarketing;

h) A informação gerada no âmbito da organização deve ser armazenada em um processo de backup com garantia de restore em local seguro validados pela equipe competente;

i) Não é permitido o uso de pendrives, HD externo ou qualquer outro tipo de dispositivo removível para o transporte ou armazenamento de dados. Exceções devem ser formalmente autorizadas pela área de segurança da informação;

j) Ao final do vínculo contratual com o cliente ou prestador de serviços, toda informação armazenada nos equipamentos da Algar Tech deve ser apagada ou repassada para o mesmo quando previsto em contrato;

k) Ao final do vínculo empregatício e/ou contratual, os associados e/ou prestadores de serviço que porventura tenham permissão de acesso a equipamentos ou mídias de armazenamento devem eliminar quaisquer vestígios físicos e/ou lógicos de informações geradas ou adquiridas dentro da Algar Tech.

7.6 - Sistemas e Aplicativos

a) Todos os softwares instalados em máquinas de propriedade ou a serviço da Algar Tech devem possuir licença de uso previamente adquiridas, devendo a área usuária registrar solicitação ao Service Desk para instalação, autorização e uso;
b) Não será permitida a instalação de software shareware, freeware ou equivalentes que não esteja previsto na lista de soluções homologadas disponível na intranet Algar Tech>Utilidades;
c) Todas as atualizações e correções de segurança devem ser implantadas conforme regra de cada aplicação e homologada pela equipe de segurança e tecnologia da informação;
d) Todos os equipamentos (servidores, desktops, notebooks dentre outros) que permitam a instalação de antivírus, devem tê-los instalados e atualizados de forma online, não podendo o usuário desabilitar ou desinstalar;
e) Todo software de antivírus deve garantir o bloqueio de vírus, worms, spyware ou outra nova tecnologia de ataque existente;
f) Todo e-mail e acesso à internet deve ser monitorado e protegido com antivírus e regras de firewall;
g) O e-mail corporativo da Algar Tech deve ser utilizado apenas para tratar assuntos relacionados à empresa, sendo as informações armazenadas ou transmitidas de propriedade da organização, cabendo ao usuário garantir sua correta classificação e tratamento conforme Procedimento - Classificação e Rótulo da Informação disponível para consulta na intranet Algar Tech>Políticas e Diretrizes;
h) A utilização do e-mail corporativo para fins pessoais, cadastro em sites de compras e outros formulários não é permitida;
i) Nenhum acesso aos sistemas e aplicativos da Algar Tech ou de seus clientes pode ser compartilhado, sendo o associado dono do usuário, o único responsável por manter a confidencialidade de suas senhas de logon, usuário de rede, internet, arquivos de trabalho e demais aplicativos da Algar Tech;
j) É vedado o uso de ferramentas de Instant Messaging não homologadas pela equipe de segurança e tecnologia, salvo exceções, quando comprovado o seu uso efetivo nas atividades desempenhadas pelo associado ou cliente;
k) É vedada a transferência de arquivos por qualquer ferramenta de Instant Messaging e compartilhamento de arquivos, salvo exceções autorizadas e/ou ferramentas homologadas e autorizadas.

8 – Violação das Políticas e Diretrizes do SGSI

8.1 - As violações de segurança devem ser informadas à área de Segurança da Informação, por meio do Service Desk. Toda violação ou desvio deve ser investigado para a determinação das medidas necessárias, visando à correção da falha ou reestruturação de processos;

8.2 – São consideradas violações de segurança:

- Uso ilegal de software;
- Introdução (intencional ou não) de vírus de informática;
- Compartilhamento de informações sensíveis do negócio;
- Divulgação de informações de clientes e das operações contratadas.

8.3 - Os princípios de segurança estabelecidos na presente política possuem total aderência da presidência e diretoria da Algar Tech e devem ser observados por todos na execução de suas funções;

8.4 – O não atendimento as diretrizes desta política ou das demais políticas e diretrizes da organização estão sujeitas à aplicação da gestão disciplinar conforme previsto no Procedimento – Registros de Não Conformidades, Planos de Ações e Aplicação da Gestão Disciplinar, disponível para consulta na intranet Algar Tech>Políticas e Diretrizes, e Política – Gestão de Consequências do grupo Algar.

9 - Auditoria

9.1 - Todos os associados, bem como os terceiros que utilizam o ambiente tecnológico da Algar Tech, estão sujeitos a auditoria de rede, telefonia e utilização das aplicações;

9.2 - Os procedimentos de auditoria e monitoramento devem ser realizados periodicamente pela área de segurança da informação ou empresa contratada, com o objetivo de observar o cumprimento das diretrizes estabelecidas nesta política pelos usuários e com vistas a gestão de performance da rede;

9.3 - Havendo evidência de atividades que possam comprometer a segurança da rede, será permitido a área de segurança da informação auditar e monitorar as atividades de um usuário, além de inspecionar seus arquivos e registros de acesso, a bem do interesse da Algar Tech, sendo o fato imediatamente comunicado à Alta Direção.