NORMA DE SEGURANÇA DA INFORMAÇÃO

Instituto Algar

CAPÍTULO I - OBJETIVO

1.1. Apresentar as principais regras que conduzem os procedimentos de segurança da informação no Instituto Algar, bem como respectivos registros eletrônicos (“dados”) dentro do ambiente do Instituto, uma vez que na execução de suas operações, são coletadas, manuseadas e armazenadas informações de relevância, além de assegurar atuação em conformidade com leis e regulamentos aplicáveis, visando disseminar a prática por todos os níveis do Instituto Algar.

CAPÍTULO II - DEFINIÇÕES

2.1. Os seguintes termos, quando iniciados por letra maiúscula, no singular ou no plural, masculino ou feminino, são usados nesta Norma com os significados abaixo especificados:

“Instituto”: Instituto Algar

“Voluntário”: É quem doa tempo, trabalho e/ou talento. Aquele que exerce trabalho sem retorno financeiro, isto é, sem remuneração nem vínculo empregatício, nas ações focadas em interesses sociais e comunitários para a população atendida pelo Instituto Algar ou terceiros.

“Alta Direção”: Todos que compõe a Diretoria Estatutária e a Gerência.

“Confidencial”: Que se diz ou se faz em confidência; secreto: aviso confidencial. Que não se pode divulgar tornar público; sigiloso: documento confidencial de campanha.

“Associados”: Membro do Instituto Algar.

“Colaboradores”: Pessoa contratada para exercer função específica pelo Instituto Algar em regime CLT.

CAPÍTULO III - PRINCÍPIOS GERAIS

3.1. Difundir elevados padrões de integridade e valores éticos, através da disseminação de cultura que aborda a importância da conformidade no Instituto Algar.

3.2. Estar em conformidade com as leis e regulamentações aplicáveis de proteção de dados.

3.3. Promover a conscientização da companhia em relação à segurança da informação, garantindo confidencialidade, integridade, disponibilidade, autenticidade e legalidade do Instituto e terceiros.

CAPÍTULO IV – DIRETRIZES GERAIS

4.1. Dados pessoais de colaboradores, voluntários e/ou beneficiários: O Instituto se compromete em não acumular ou manter intencionalmente dados pessoais de colaboradores, voluntários e/ou beneficiários, além daqueles relevantes na condução do trabalho do Instituto. Todos esses dados pessoais são considerados confidenciais. Os mesmos não serão usados para fins diferentes daqueles para os quais foram coletados.

4.1.1. Os dados pessoais não serão transferidos para terceiros, exceto quando exigido pela regularidade do Instituto e desde que eles mantenham a confidencialidade das informações.

4.2. Admissão e demissão de colaboradores: A gerência do Instituto deverá informar ao setor responsável toda e qualquer movimentação de temporários, aprendizes, estagiários e/ou admissão/demissão de colaboradores, para que os mesmos possam ser cadastrados ou descadastrados nos sistemas do Instituto.

4.2.2. A gerência ou recursos humanos fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, que deverá ser trocada pelo usuário no seu primeiro acesso.

4.2.3. No caso de desligamento, a gerência deverá comunicar o fato na mesma data ao setor responsável, para que todos os acessos concedidos sejam revogados.

4.2.4. Cabe ao setor responsável dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Norma de Segurança da Informação do Instituto.

4.3. Concessão e revogação de acessos: Quando houver necessidade de concessão ou revogação de acesso aos sistemas, repositórios de arquivos de trabalho e/ou equipamentos de informática do Instituto, o setor solicitante comunicará esta necessidade à gerência, copiando a área técnica de informática da Algar.

4.4. Norma de senhas: Recomendamos que as senhas tenham no mínimo 8 (oito) caracteres alfanuméricos, contendo pelo menos uma letra maiúscula e um caractere especial.

4.4.1. Recomendamos que as senhas sejam trocadas pelos usuários a cada 3 meses, não devendo se repetir nos últimos 12 meses.

4.4.2. Sempre que um usuário é desligado da organização, todas as suas senhas e acessos devem ser revogados no mesmo dia.

4.5. Compartilhamento de pastas e dados: O compartilhamento de pastas e arquivos de trabalho, cujo conteúdo seja classificado como sendo de informação confidencial ou restrita, é proibido.

4.5.1. Havendo necessidade de se realizar o compartilhamento de dados entre usuários (internos e/ou externos) não confidencial deve-se utilizar os canais oficiais, como o *Teams*, e-mail ou drive do Instituto.

4.6. Cópias de segurança, recuperação e integridade dos sistemas e de seus bancos de dados: Cópias de segurança dos sistemas, repositórios de arquivos de trabalho, bancos de dados e configurações dos equipamentos e servidores de rede são de responsabilidade exclusiva do Instituto.

4.7. Uso da internet: O uso da internet poderá ser monitorado pela alta direção, através do uso de sistema de registro de navegação que informa qual usuário está conectado, o tempo que usou a internet e qual página acessou.

4.7.1. Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros.

4.7.2. Quando navegando na internet, é proibido a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

I. De estações de rádio;
II. De jogos on-line;
III. De conteúdo pornográfico ou relacionados a sexo;
IV. Que defendam atividades ilegais;
V. Que menosprezem, depreciem ou incitem o preconceito a determinadas classes.

4.8. Uso do correio eletrônico (“e-mail”): O correio eletrônico fornecido pelo Instituto é um instrumento de comunicação interna e externa para a atuação do Instituto.

4.8.1. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem do Instituto, não podem ser contrárias à legislação vigente e nem aos princípios éticos estabelecidos no código de conduta.

4.8.2. O uso do e-mail é de responsabilidade do usuário e ele é responsável por toda mensagem enviada pelo seu endereço.

4.8.3. É terminantemente proibido o envio de mensagens que:

I. Contenham declarações difamatórias e linguagem ofensiva;
II. Possam trazer prejuízos a outras pessoas;
III. Sejam hostis;

IV. Sejam relativas a “correntes”, de conteúdos pornográficos ou equivalentes;
V. Possam prejudicar a imagem do Instituto e/ou de outras empresas;
VI. Sejam incoerentes com as políticas estabelecidas no Código de Conduta do Instituto.

4.9. Programas ilegais: É terminantemente proibido o uso de programas ilegais (software pirata) no Instituto. Os usuários não podem, em hipótese alguma, instalar este tipo de programa nos equipamentos do Instituto.

4.9.1. Todos os computadores estão sujeitos a verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz, pela gerência ou técnico indicado por ela.

4.10. Necessidades de novos sistemas, aplicativos e/ou equipamentos: A gerência é responsável pela definição de compra, substituição e instalação de todo e qualquer “software” e “hardware”.

4.10.1. Não é permitida a compra ou o desenvolvimento de “softwares” diretamente pelos usuários.

4.11. Uso de equipamentos de propriedade do Instituto: Os usuários que estiverem de posse de qualquer equipamento (desktop, notebook, celular ou tablet) de propriedade do Instituto devem estar cientes de que:

I. Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais.
II. A proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário.
III. É de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo.
IV. O usuário não deve alterar a configuração do equipamento recebido.
V. O usuário não deve instalar ou remover nenhum programa do equipamento recebido, sem autorização prévia. Também não

deve alterar a configuração de nenhum programa previamente instalado.

4.11.1. Fora do trabalho:

I. Mantenha o equipamento sempre com você.
II. Atenção em hall de hotéis, aeroportos, aviões, táxi e etc.
III. Quando transportar o equipamento em automóvel utilize sempre o porta-malas ou lugar não visível.
IV. Atenção ao transportar o equipamento na rua.

4.11.2. Em caso de furto:

I. Registre a ocorrência em uma delegacia de polícia.
II. Comunique o fato o mais rápido possível à gerência.
III. Envie uma cópia do boletim de ocorrência para o administrativo.

4.11.3. Em caso de dano:

I. Reparo de qualquer gênero deve ser realizado por prestador de serviço técnico de informática indicado pelo Instituto.
II. Comunique o fato o mais rápido possível à gerência.

4.12. Sistema de telecomunicações: O controle de uso, a concessão de permissões e a aplicação de restrições em relação aos ramais telefônicos do Instituto, assim como, o uso de eventuais ramais virtuais instalados nos computadores, é responsabilidade da gerência.

4.13. Uso de antivírus: Todo arquivo obtido através da internet ou recebido de entidade externa ao Instituto deve ser verificado por programa antivírus.

4.13.1. Todas as máquinas devem possuir software antivírus instalado.

4.13.2. O usuário não pode desabilitar o programa antivírus instalado nas estações de trabalho.

4.14. Violação da segurança da informação: Será considerado violação qualquer ato que:

I. Exponha o Instituto a uma perda efetiva ou potencial por meio do comprometimento da segurança dos dados ou de informações ou ainda da perda de equipamento.
II. Envolva a revelação de dados confidenciais, direitos autorais, negociações, marcas ou uso não autorizado de dados corporativos.
III. Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.

CAPÍTULO V - RESPONSABILIDADES

5.1. De forma geral, cabe a todos os associados, diretores, membros, colaboradores, prestadores de serviço e demais stakeholders:

I. Cumprir as medidas de segurança da informação do Instituto.
II. Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pelo Instituto.
III. Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo Instituto.
IV. Cumprir as leis e as normas que regulamentam a propriedade intelectual.
V. Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais.
VI. Não compartilhar informações confidenciais de qualquer tipo.

5.2. É dever de todos os colaboradores, diretores e conselheiros do Instituto:

I. Considerar a informação como sendo um ativo da organização, um dos recursos críticos para a realização da gestão, que possui

grande valor para o Instituto e deve sempre ser tratada profissionalmente.

5.3. São boas práticas:

I. Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos.
II. Manter mesas organizadas e documentos com informações confidenciais trancados, quando não os estiver utilizando.

CAPÍTULO VI – ARQUIVO

6.1. Arquivos de trabalho: Os arquivos de trabalho, considerados dados essenciais ao desenvolvimento do Instituto, são mantidos nos servidores de arquivos em rede que permite o controle, comparação e gestão de diferentes versões.

6.1.1. São exemplos de arquivos de trabalho:

I. Planilha de faturamento.
II. Notas fiscais.
III. Propostas comerciais.
IV. Relatórios de análise técnica.
V. Relatório de orçamento.
VI. Relatório de doações.
VII. Relatório dos programas sociais.

6.2. Arquivos individuais: São considerados arquivos individuais aqueles criados, copiados ou desenvolvidos pelos usuários, que não sejam parte integrante do produto entregável pelo seu trabalho, seja ele interno ou para parceiros. Alguns exemplos são: rascunhos ou lembretes, memórias de cálculo, mensagens, diagramas ou instruções técnicas.

6.2.1. A cópia de segurança destes arquivos é de responsabilidade dos próprios usuários.

6.2.2. Não é permitido aos usuários o uso ou armazenamento dos tipos de arquivos abaixo relacionados em suas estações de trabalho:

I. Programas não licenciados ou não homologados para uso no Instituto.
II. Músicas, filmes, séries, programas de TV.
III. Vídeos não relacionados à atividade profissional.
IV. Conteúdo pornográfico ou relacionado a sexo.

CAPÍTULO VII - PENALIDADES

7.1. O não cumprimento desta norma implica em falta grave e poderá resultar em advertência formal, suspensão, rescisão do contrato de trabalho, outra ação disciplinar e/ou processo civil ou criminal.

CAPÍTULO VIII - DEFINIÇÕES FINAIS

8.1. Uma Norma de Segurança da Informação não garante que leis, normas e procedimentos sejam cumpridos. Isso só pode ser obtido quando cada envolvido ao Instituto Algar cumpre as leis, normas e procedimentos ao executar as suas tarefas, a cada dia. Por esse motivo, é de fundamental importância que todos entendam a relevância dessa norma e se dediquem ao seu trabalho, realizando-o com uma conduta de ética e integridade.

8.2. O presente documento e suas atualizações entram em vigor na data da sua aprovação pela diretoria estatutária.

Uberlândia-MG, 11 de novembro de 2023