Repositório: [Repositório]\Manual e Política\Políticas	
Modelo: 012021	Aprovado por: Alta Direção
Emitido em: 06/04/2021	Editado por: Eduardo Ostos

1. Objetivo

1.1. Esta política tem o objetivo de estabelecer as diretrizes e normas de segurança da informação e proteção de dados pessoais da NETADMIN, suportada por uma decisão estratégica da diretoria da companhia e desenvolvida no âmbito de um Sistema de Gestão da Segurança da Informação (SGSI) normatizado. Busca-se, em especial:

a. garantir a adoção de normas e procedimentos que permitam aos colaboradores e demais partes interessadas da NETADMIN seguir padrões de comportamento seguros, protetivos às informações sensíveis da companhia e adequados à legislação aplicável, conforme definido no item 2.4 abaixo;

b. observar os 3 (três) pilares da segurança da informação (confidencialidade, integridade, disponibilidade) para melhor atendimento às necessidades dos clientes e colaboradores da NETADMIN e para assegurar que a imagem da companhia perante o mercado se mantenha e se consolide como a de uma fornecedora de produtos e serviços de alta qualidade;

c. prevenir incidentes de segurança, como, acessos indevidos, perda, destruição, divulgação e/ou modificação não autorizada de dados, bem como, proteger as informações contra uma ampla gama de ameaças.

1.2. Esta política se aplica a (i) todos os dados pessoais que a NETADMIN eventualmente trate em relação a pessoa física identificada ou identificável; bem como (ii) a todas as informações sensíveis da companhia e de seus clientes, conforme definido abaixo.

2. Termos e Definições

2.1. Dados Pessoais. Consideram-se dados pessoais toda informação relacionada a pessoa natural identificada ou identificável.

2.2. Informações Sensíveis. Consideram-se informações sensíveis todos os dados que possuam algum valor para a operação da NETADMIN, independentemente do formato e meio de armazenamento.

2.3. Informações. Consideram-se Informações as Informações Sensíveis e os Dados Pessoais, quando conjunta e genericamente considerados.

2.4. Legislação Aplicável. Considera-se Legislação Aplicável as leis que regulam aspectos de propriedade intelectual e tratam de Proteção de dados, incluindo LGPD (Lei Geral de Proteção de Dados), GDPR (*General Data Protection Regulation*) e CCPA (*California Consumer Privacy Act*).

2.5. Para efeitos desta Política, aplicam-se os demais termos e definições constantes do manual do Sistema de Gestão de Segurança da Informação.

3. Aplicabilidade

3.1. Esta Política é aplicável a todos os colaboradores da NETADMIN, empresas associadas e/ou afiliadas, *joint ventures* e/ou quaisquer terceiros que possuam ou venham a possuir vínculo com a companhia.

3.1.1. A diretoria da NETADMIN, juntamente com os gestores responsáveis pela segurança da informação, está comprometida com uma gestão efetiva e com a aplicação das políticas definidas no SGSI, de modo a primar pela segurança da organização e pelas diretrizes aqui estabelecidas.

3.1.2. É responsabilidade de todos os colaboradores conhecer e respeitar a política do SGSI, envolvendo-se nas questões relacionadas à segurança e atuando ativamente para que suas habilidades sejam usadas para a melhoria contínua do SGSI.

3.1.3. A melhoria contínua dos procedimentos e processos estabelecidos no SGSI é responsabilidade conjunta da direção da NETADMIN, dos representantes da direção e da equipe de segurança

da informação. Os procedimentos e processos devem ser regularmente revisitados e melhorados, garantindo a efetividade da política estabelecida no SGSI.

3.1.4. A NetAdmin observará esta política em quaisquer circunstâncias, inclusive em relacionamentos externos com clientes, fornecedores e/ou quaisquer outras partes interessadas.

3.1.5. Nos casos de relacionamentos externos em que a outra parte não possui uma política de segurança da informação, ou em que a respectiva política não garanta os mesmos níveis de segurança que a presente, um representante da direção, em conjunto com a equipe de segurança da informação, deverá avaliar se há algum risco para a segurança da NETADMIN.

4. Diretrizes

4.1. Ativos de informação. Os ativos associados às Informações e os recursos de processamento de informação estão devidamente identificados e inventariados.

4.1.1. Para cada ativo de Informação está definido um proprietário, responsável por assegurar que ele seja utilizado conforme esta Política.

4.1.2. Somente softwares aprovados e publicados pela área de TI poderão ser utilizados nos ativos controlados pelo SGSI.

4.1.3. As diretrizes para utilização adequada dos ativos são informadas durante o processo de contratação de pessoas. Ativos específicos possuem como responsável profissional capacitado para manipulação garantindo a devida utilização.

4.1.4. Não é permitido o compartilhamento de dados corporativos processados pelos ativos de Informação sem a autorização prévia e específica do gestor responsável.

4.2. Controle de Acesso. Controle de acesso é um dos mecanismos utilizados para proteger física e logicamente o ambiente com Informações da NETADMIN. O acesso aos ativos de informação deve ser permitido somente a pessoas autorizadas, nos termos desta Política.

4.2.1. O direito de uso dos ativos é controlado e cedido no momento da contratação, durante o vínculo profissional do colaborador na companhia, cessado ao término do vínculo com a NETADMIN quando os ativos físicos são recolhidos.

4.2.2. Caso o contratado tenha a necessidade de acesso a um sistema corporativo específico, este será provido via autorização do gestor da Informação envolvida.

4.3. Controle de Acesso Físico.

4.3.1. Entrada de Colaboradores. O acesso às Informações, equipamentos, documentos e áreas seguras são devidamente controlados para que somente pessoas autorizadas tenham acesso a estes recursos.

a. A identificação dos colaboradores para acesso às instalações da NETADMIN é controlada por dispositivo de segurança que garante acesso apenas ao pessoal autorizado. Os ambientes restritos são controlados por dispositivos de segurança e o acesso só é permitido via autorização do responsável.

b. Colaboradores demitidos somente poderão entrar em dependências da NetAdmin se devidamente acompanhados por um colaborador responsável.

4.3.2. Entrada de Visitantes. A entrada e atendimento de visitantes somente são permitidos em horário comercial, mediante o acompanhamento de um colaborador responsável. O visitante deverá passar pelos processos de segurança realizados pela portaria do condomínio e, ao término da visita, deverá ser acompanhado até que deixe as instalações da companhia. Durante todo o prazo em que o visitante estiver nas instalações da NETADMIN, deverá estar no

campo de visão de algum colaborador da companhia, exceto no caso de lugares privados, como sanitários.

4.3.3. Entrada de Fornecedores. O acesso de fornecedores à NETADMIN deverá acontecer mediante solicitação de serviço ao fornecedor e com a devida autorização de um responsável da companhia. O fornecedor deve portar identificação capaz de certificar que se trata da pessoa contratada para o serviço, bem como ser acompanhado por um colaborador NETADMIN.

4.3.4. Áreas de Entrega e de Carregamento. A NETADMIN possui pontos de acesso para entregas e carregamentos que estão localizados nas docas do edifício e a antessala de nossa instalação. As encomendas devem ser recebidas e entregues em um desses dois pontos, exceto quando o volume, o peso, ou outro fator inviabilizar a operação. Neste caso a pessoa responsável pela entrega/carregamento deve ser identificada e acompanhada por um colaborador da NETADMIN durante todo o tempo em que estiver em nossas instalações.

4.3.5. Mesa Limpa. Todos os colaboradores devem se comprometer a não deixar qualquer Informação confidencial à vista, seja em papel e/ou anotadas em lugar visível ou de possível acesso. Especial atenção também deve ser dada quando da utilização de impressoras coletivas, recolhendo o documento impresso imediatamente após a sua impressão.

4.4. Controle de Acesso Lógico.

4.4.1. Acessos no Processo de Contratação. Durante o processo de contratação, os colaboradores receberão a devida liberação de acesso lógico aos ativos das Informações necessários às suas atividades.

a. O colaborador receberá acesso aos ativos da Informação, como rede e sistemas, e deverá se responsabilizar pelo sigilo das Informações recebidas. Não é permitido a nenhum colaborador fornecer sua senha de acesso a outros colaboradores.

b. Acessos específicos não contemplados no processo de contratação deverão ser tratados diretamente com o responsável pelo ativo da Informação.

4.4.2. Cancelamento de Acessos. O processo de desligamento de colaboradores realiza a retirada dos direitos de acesso aos diversos ativos de Informação.

4.4.3. Acesso à Internet. A NETADMIN disponibiliza acesso à internet a colaboradores e visitantes, sendo que o acesso a visitantes é feito através de rede específica e apartada de nossa rede corporativa.

a. A internet disponibilizada pela NETADMIN aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que este uso não cause riscos a imagem, reputação e infraestrutura da companhia.

b. A NetAdmin se dá ao direito de restringir o acesso a sites que podem colocar em riscos a companhia.

c. É proibida a divulgação de informações confidenciais da NETADMIN em quaisquer grupos de discussão, listas ou bate-papos.

4.4.4. Acesso ao Correio Eletrônico. Todos os usuários de correio eletrônico estão habilitados a enviar e receber mensagens externas.

a. O padrão para criação de e-mail institucional é nome.sobrenome@netadmin.software. Em casos excepcionais, de duplicidade ou que causem constrangimento aos usuários, o padrão deverá ser revisto.

b. A conta de e-mail é disponibilizada exclusivamente para uso institucional, não sendo admitido para uso pessoal.

4.4.5. Acesso ao Código-fonte. O acesso ao código-fonte de programas e de itens associados (como desenhos, especificações, planos de verificação e de validação) é restrito para os profissionais envolvidos no processo de desenvolvimento e implantação de sistemas.

a. Todos os produtos gerados durante o ciclo de vida de desenvolvimento de sistemas devem estar armazenados em repositórios sujeitos a mecanismos de controle de acesso, garantindo que somente colaboradores autorizados tenham acesso.

b. Os códigos-fontes dos sistemas de Informação de propriedade da NETADMIN devem ser adequadamente mantidos, incluindo o controle de versionamento, e a proteção contra acessos ou alterações indevidas.

4.4.6. Retirada ou Ajuste de Acessos. A liberação de acessos a sistemas, diretórios, grupos de acessos ou perfis administrativos oferecidos aos usuários necessitam de revisão, para assegurar que os acessos estejam compatíveis com o cargo, a área de atuação e as funções exercidas.

a. Devem ser submetidos a processo de revisão periódica: (i) acessos concedidos a sistemas e aplicações; e (ii) acessos concedidos a infraestrutura de TI.

b. A revisão de acesso a sistemas deverá ser feita conforme a classificação da Informação contida em cada sistema, ou outro critério estabelecido pela diretoria.

c. O processo de revisão deverá ser executado a cada vez que o colaborador passar por uma mudança de cargo ou função ou em análise crítica a ser realizada anualmente pela equipe de segurança da informação.

4.4.7. Acesso Privilegiado. As credenciais de acesso privilegiado a sistemas ou ativos físicos, deverá ser concedida mediante aprovação do gestor com base na função e na necessidade para desenvolvimento das atividades do trabalho.

a. O compartilhamento do uso das credenciais de acesso privilegiado deve ser vedado. Contudo, caso haja necessidade de compartilhamento por questões técnicas, estas devem ser autorizadas pelo gestor com formalização do motivo pelo qual a senha está sendo solicitada e realizando a alteração da senha assim que a causa da solicitação seja tratada.

b. Todos os usuários detentores de ID de acesso privilegiado devem também possuir ID de acesso de atividades não privilegiadas, de forma que a utilização do acesso ocorra quando for estritamente necessário.

4.4.8. Uso de Programas Utilitários Privilegiados. O uso de programas utilitários que podem ser capazes de sobrepor os controles dos sistemas e aplicações são restritos à equipe da TI e devem ser utilizados apenas para ajudar na administração do ambiente de rede de dados da NetAdmin.

4.4.9. Acesso Seguro aos Sistemas e Gerenciamento de Senhas. O procedimento de *logon* deve divulgar apenas as Informações necessárias às atividades de determinado colaborador, evitando fornecer a um usuário não autorizado Informações indevidas.

a. As mensagens de ajuda do processo de *logon* não devem possuir dicas capazes de permitir a um usuário não autorizado o acesso ao sistema.

b. Todo usuário deverá ter uma identificação única, pessoal e intransferível.

c. O titular assume a responsabilidade quanto ao sigilo da sua senha pessoal, e é responsável por qualquer ação executada com o seu login/senha.

d. Não é permitido o compartilhamento, a divulgação a terceiros, anotações em papel da identificação pessoal, nem a anotação de senha em lugar visível e/ou que possa ser acessado por outra pessoa.

e. Incentivamos o uso de senhas fortes, sugerimos que a senha possua ao menos à seguinte formação: (i) 08 (oito) ou mais caracteres; e (ii) inclusão de letras maiúsculas, minúsculas, números e caracteres especiais.

f. Não é permitido utilizar senhas fracas, como baseada em nomes próprios, dados pessoais tais como nome, data de nascimento, número de documentos entre outros.

g. As senhas dos sistemas da companhia devem ser alteradas sempre que existir qualquer indicação de possível comprometimento do sistema ou da própria senha. Incentivamos a não reutilização de senhas.

h. O colaborador, quando receber uma senha criada por terceiro, deve alterá-la em seu primeiro acesso para uma senha segura, conforme sugerido acima.

4.4.10. Acesso Remoto**.** O acesso remoto à infraestrutura é disponibilizado apenas para casos específicos e realizado através de conexão segura e protegida por senha. As Informações acessadas remotamente devem ser protegidas por meio de software que contribua para a segurança dos dados armazenados e do tráfego das Informações.

4.4.11. Tela Limpa. Os colaboradores, quando aplicável, devem bloquear todos os equipamentos, estações de trabalho e servidores em qualquer ausência temporária, evitando o uso indevido do equipamento.

4.4.12. Uso de Dispositivos Móveis. Não permitimos acesso dos dispositivos móveis pessoais à rede corporativa, somente na rede para convidados, de forma que todos os dispositivos móveis de nossos colaboradores possuem permissão de acesso apenas a rede de convidados.

a. Os ativos móveis pessoais não são cadastrados como ativos da segurança da informação da NETADMIN.

b. Os dispositivos móveis pessoais utilizados pelos colaboradores da NETADMIN para atividades de trabalho devem ser protegidos por senha ou identificação visual.

c. Não é permitido que documento de trabalho seja armazenado em dispositivo móvel pessoal a não ser que dentro de repositório próprio de ferramenta licenciada pela NETADMIN.

d. Os usuários de Informações corporativas em dispositivos móveis pessoais se comprometem a excluir todas as Informações mediante requerimento. É vedado o compartilhamento das Informações sem a autorização do gestor responsável do nível de diretoria.

e. Ativos móveis da NETADMIN são cadastrados como ativos de informação e seguem todos os requisitos desta Política.

4.4.13. Segurança nas Comunicações. É proibida a utilização dos Sistemas de Informação com o fim de realizar ações que sejam contra a legislação e normas nacionais e internacionais que podem provocar danos na rede ou em outros sistemas, prejudicando o tráfego da rede ou o acesso a recursos.

4.5. Segurança com Fornecedores. Acordos com terceiros, parceiros e fornecedores são estabelecidos e documentados para que não existam desentendimentos entre as partes, com relação à obrigação de ambos com os requisitos de segurança aplicáveis.

4.6. Segurança com Clientes. No caso de visita a clientes em que normas de segurança são definidas para acesso a áreas seguras, é obrigatório que os colaboradores NETADMIN participem de todos os treinamentos de segurança disponibilizados e sigam todas as orientações garantindo sua integridade física.

4.7. Conformidade Jurídica. A NETADMIN se compromete a observar toda a Legislação Aplicável.

4.7.1. Adequação à Legislação Aplicável. A NETADMIN se compromete a observar a Legislação Aplicável, as diretrizes a serem emanadas pela Agência Nacional de Proteção de Dados (“ANPD”) e a adotar todas as medidas de segurança técnica e organizacionais possíveis e necessárias ao resguardo dos Dados Pessoais tratados, incluindo, sem se limitar a:

a. adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

b. adotar os padrões técnicos mínimos determinados pela autoridade nacional para tornar aplicável o disposto no item anterior, considerada a natureza das Informações tratadas, as características específicas do

tratamento e o estado atual da tecnologia, especialmente no caso de dados pessoais sensíveis;

c. controlar e restringir o tratamento dos dados aos profissionais necessários para as respectivas atividades, que deverão ser instruídos sobre a forma adequada de tratamento;

d. observar todos os princípios para o tratamento de dados previstos na Legislação aplicável, respeitando os direitos dos titulares de dados.

4.7.2. Propriedade Intelectual. É também assegurada a utilização lícita de softwares, sempre com suas licenças oficiais e autorizadas de modo a não infringir direitos de propriedade intelectual e autoral de fabricantes e seus representantes.

4.8. Gestão de Incidentes de Segurança da Informação. As diretrizes para a gestão de incidentes de Segurança da Informação são estabelecidas em um documento específico, garantindo um enfoque consistente e efetivo de gerenciamento de incidentes, assegurando que fragilidades e incidentes de segurança da informação sejam detectados, registrados, investigados e sempre que possível, prevenidos.

4.9. Gestão da Continuidade de Negócio. A NETADMIN possui procedimentos estabelecidos para a recuperação de serviços e processos críticos de forma a assegurar que suas atividades consideradas essenciais continuem a ser executadas e que os serviços críticos fiquem disponíveis para o usuário, em situação de crises ou indisponibilidades não programadas.

5. Responsabilidades

5.1. Colaboradores. São obrigações atribuíveis a todo colaborador da companhia:

a. Conhecer e cumprir integralmente os termos da Política Geral de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;

b. Relatar ocorrências, suspeitas de incidentes de segurança ou quaisquer dúvidas ou pedidos à Equipe do Sistema de Gestão da Segurança da Informação - SGSI;

c. Responder pela inobservância da Política de Segurança da Informação e demais normas e procedimentos de segurança, conforme definido nas sanções previstas por esta política;

d. Zelar pela segurança das Informações e para que toda atividade que envolva o tratamento de Dados Pessoais seja realizada de forma segura e adequada, em respeito às políticas da companhia e a Legislações Aplicável.

5.2. Para além das obrigações gerais, acima previstas, são previstas as seguintes responsabilidades:

5.2.1. Gestores:

a. Ser agente multiplicador, informando, incentivando e conscientizando os colaboradores a cumprir a Política de Segurança da Informação;

b. Identificar, classificar e rotular as Informações geradas sob a responsabilidade da sua área de negócio, realizando os ajustes conforme necessário;

c. Garantir que, no momento da contratação, os colaboradores ou prestadores de serviços conheceram e aceitaram a Política de Segurança da Informação.

5.2.2. Equipe do Sistema de Gestão da Segurança da Informação:

a. Manter e melhorar o sistema de Segurança da Informação;

b. Revisar e atualizar os documentos que compõem a Política de Segurança da Informação;

c. Promover a conscientização e orientar os colaboradores em relação à Política de Segurança da Informação;

d. Estimular que as atividades de Segurança da Informação sejam executadas em conformidade com esta política;

e. Avaliar os incidentes de Segurança da Informação e comunicar o resultado aos gestores, se necessário.

5.2.3. Área de Recursos Humanos: garantir, no momento da contratação, que o processo relacionado a Segurança da Informação seja executado.

6. Sanções.

6.1.1. As violações das normas que compõem esta Política, tanto por colaboradores quanto por terceiros, bem como as demais normas e procedimentos de segurança, devem ser comunicadas imediatamente ao gestor imediato, aos recursos humanos e ao SGSI.

6.1.2. Violações são passíveis de penalidades administrativas, inclusive no que tange a comunicação às autoridades públicas competentes, se for o caso.

7. Casos Omissos

7.1.1. Os casos omissos deverão ser analisados pela Equipe do SGSI, que deliberará sobre cada caso específico e tomará as providências cabíveis.

7.1.2. As diretrizes estabelecidas nesta Política e nas demais normas de segurança da NETADMIN, não limitados a este conteúdo, espera que todos as partes envolvidas, sempre que possível, associem medidas que garantam a Segurança da Informação em todas as atividades da companhia.

8. Referências

- Manual do SGSI;
- NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação
- NBR ISO/IEC 27002 - Código de prática para a gestão da segurança da informação