1. OBJETIVO

Esta política de segurança da informação tem o objetivo de especificar os controles internos aplicáveis à segurança e ao sigilo da informação das sociedades que fazem parte da Conasa Infraestrutura S.A. (Companhia), com o objetivo de prover a segurança necessária para realização de suas operações, ainda que em situações adversas.

1.1. Público-alvo

Estão sujeitos ao disposto no presente documento todos os sócios, administradores, funcionários, prestadores de serviços e demais colaboradores da Conasa (individualmente "Colaborador" ou em conjunto "Colaboradores"), no que a cada um for aplicável.

1.2. Revisão e Atualização

O presente documento foi elaborado e deve ser interpretado em consonância com os demais manuais e políticas da Conasa. Será revisado e atualizado pela área de Tecnologia da Informação ("Diretoria de TI"), anualmente, ou em prazo inferior, em função de mudanças legais/regulatórias ou se a Companhia entender necessário, a fim de incorporar medidas relacionadas às atividades e aos procedimentos novos ou anteriormente não abordados.

1.3. Responsabilidade

É de responsabilidade de todos os Colaboradores conhecer e cumprir todas as obrigações decorrentes desta Política e regulamentações vigentes, bem como observar os mais altos padrões de conduta profissional ao conduzirem suas atividades.

Também é dever de todos os Colaboradores informar e reportar inconsistências em procedimentos e práticas definidas no presente documento, seja para seu superior imediato e/ou para a Diretoria de Tecnologia da Informação.

2. OBJETIVOS E PRINCÍPIOS

2.1. Objetivos

Esta Política tem como objetivos:

Permitir que a Conasa atenda à regulamentação, à legislação e à autorregulação aplicáveis;

Manter o nível de segurança da organização em um patamar definido como adequado pela Companhia;

Garantir que as diretrizes explicitadas nesta Política sejam praticadas, por meio da implementação de controles que visam garantir a Confidencialidade, a integridade e a Disponibilidade das informações.

Esta Política se aplica aos seguintes Ativos:

Ativos de informação: base de dados e arquivos, documentação de sistemas, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade, procedimentos de recuperação, informações armazenadas etc.;

Ativos de software: aplicativos, sistemas, ferramentas de desenvolvimento e utilitários;

Ativos físicos: equipamentos computacionais (computadores, processadores, monitores, laptops, modems, etc.), equipamentos de comunicação (roteadores, PABX, telefones fixos, etc.), mídias (fitas e discos magnéticos, discos ópticos, etc.), equipamentos técnicos (Nobreaks, aparelhos de ar-condicionado, etc.), mobília, acomodações, etc.

Para atingir os objetivos acima listados, a Conasa estabelece a presente Política como um dos pilares de sua estratégia de segurança, a qual deve ser seguida e implementada para garantir que os Ativos sejam protegidos, de acordo com a sua importância estratégica para a organização.

A presente Política se define como um documento que expressa a posição da organização sobre a segurança, e esclarece seus valores e direcionamentos para minimizar os riscos sobre seus Ativos. Desta forma, ela estabelece a linha mestra de atuação da Conasa em relação a todos os aspectos da Segurança da Informação, incluindo equipamentos, bens, informações e pessoas.

2.2. Princípios

A Política tem como princípios assegurar a:

Identificação: garantir que qualquer indivíduo seja identificado unívoca e inequivocamente;

Autenticação: garantir que a identidade de cada pessoa ou recurso seja expressamente comprovada;

Autorização: garantir que somente as pessoas e recursos permitidos tenham acesso aos Ativos;

Confidencialidade: garantir que as informações sejam acessadas apenas por aqueles que possuam esse acesso como pré-requisito para o exercício de suas funções ou que sejam expressamente autorizados;

Integridade: preservar a integridade das informações, salvaguardando-as contra ações não autorizadas e garantindo que todas estejam exatas e completas durante a sua criação, uso, guarda e destruição;

Disponibilidade: garantir que os usuários, quando devidamente autorizados, tenham acesso às informações e instalações sempre que necessitarem.

Com a finalidade de assegurar que os princípios acima sejam observados, a Conasa desenvolve as seguintes atividades:

- *Classificação da informação:*
- *Controle de Acesso às informações;*
- *Rastreamento e monitoramento.*
- *Avaliação de risco:*
- *Controle de mudanças;*
- *Plano de contingência;*
- *Segurança física dos dispositivos onde é armazenada e por onde transita a informação;*
- *Testes de segurança e de continuidade dos negócios.*

Este documento serve como um guia de melhores práticas definido pela Conasa em relação à Segurança da Informação e tem o propósito de oferecer uma base comum de atuação para ser usado por aqueles que são responsáveis pela criação, implementação e manutenção de processos, procedimentos, sistemas, tecnologias, conhecimento, estratégias, serviços, campanhas e quaisquer outros Ativos que compõem o dia a dia da organização. A Companhia tem como compromisso assegurar que as orientações definidas nesta Política sejam seguidas por todos os Colaboradores.

Antes de efetuar ações que envolvam acesso, uso, alteração, armazenamento, transmissão, destruição ou qualquer outra atividade envolvendo Ativos da Conasa, o usuário deve consultar esta Política para certificar-se de que a atividade é permitida. Toda e qualquer atividade que não seja claramente permitida é proibida. Em caso de dúvida, o usuário deve consultar a Gerência de TI para assegurar-se que a atividade seja permitida. Cabe aos representantes pela Gerência de TI avaliarem os riscos das atividades não previstas nas diretrizes de segurança da Conasa, levando ao conhecimento do Subcomitê de Riscos Corporativos e Operacionais a prática de alguma dessas atividades.

3. DEVERES E RESPONSABILIDADES

As responsabilidades aqui citadas seguem o mapeamento de riscos, o plano de autoria e outros documentos correlatos da Conasa.

3.1. São deveres de todos os Colaboradores no âmbito desta Política:

- *Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;*
- *Cumprir a presente Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis;*
- *Utilizar os Sistemas de Informações e os recursos relacionados somente para os fins previstos pela Diretoria de TI;*
- *Cumprir as regras específicas de proteção estabelecidas aos Ativos de informação;*
- *Manter o caráter sigiloso da senha de acesso aos recursos e sistemas, sem compartilhar acessos e permitir usos por outras pessoas ("caronas");*
- *Manter em sigilo informações confidenciais de outros que não tenham a devida autorização de acesso;*
- *Responder por todo e qualquer acesso aos recursos da Conasa, bem como pelos efeitos decorrentes de acesso efetivado através de seu código de identificação ou outro atributo para esse fim utilizado;*
- *Solicitar acesso às informações restritas somente quando houver real necessidade de acesso ao recurso;*
- *Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, sob pena de violação da legislação de propriedade intelectual pertinente, e;*
- *Comunicar ao seu superior imediato e à Diretoria de Tecnologia da Informação o conhecimento de qualquer irregularidade ou desvio verificado no âmbito da presente Política, com a garantia que sua comunicação será tratada de modo sigiloso e sem identificação pública de que foi feita.*

3.2. Responsabilidades dos Gestores de Áreas

- *Gerenciar o cumprimento desta Política, por parte de seus funcionários e prestadores de serviço;*
- *Identificar os desvios praticados e adotar as medidas corretivas apropriadas, reportando a situação à Gerência de TI;*
- *Impedir o acesso de empregados demitidos ou, se for o caso, demissionários aos Ativos de informação;*
- *Fornecer à Gerência de TI informações sobre movimentação de funcionários em sua equipe (desligamento, contratação, transferência, etc.) com antecedência, para que os*

responsáveis promovam a criação, a modificação ou o cancelamento da respectiva permissão de acesso;

- *Proteger os Ativos de informação e de processamento da Conasa;*
- *Garantir que o pessoal sob sua supervisão compreenda e desempenhe a obrigação de proteger todos os Ativos de informação da Companhia;*
- *Comunicar formalmente à unidade que efetua a concessão de privilégios a usuários de tecnologia da informação quais são os colaboradores e prestadores de serviço, sob sua supervisão, que podem acessar às informações da Conasa e;*
- *Comunicar formalmente à unidade que efetua a concessão de privilégios aos usuários de tecnologia da informação quais são os Colaboradores demitidos ou transferidos, para que esta possa prosseguir com as respectivas exclusões no cadastro de usuários.*

3.3. Responsabilidades da Diretoria/Gerência de TI

- *Estabelecer as regras de Proteção dos Ativos da Conasa;*
- *Revisar frequentemente as regras de proteção estabelecidas;*
- *Restringir e controlar o acesso e privilégios de usuários remotos e externos;*
- *Auxiliar as demais Diretorias/Gerências da Conasa a elaborar e a manter atualizado o Plano de Contingência e Continuidade dos Negócios;*
- *Executar as regras de proteção estabelecidas por esta Política;*
- *Detectar, identificar, registrar e comunicar à chefia violações ou tentativas de acesso não autorizadas;*
- *Definir e aplicar, para cada usuário de tecnologia da informação, restrições de acesso à rede, como horário e dia autorizados, entre outras;*
- *Limitar ao período da contratação o prazo de validade das contas de prestadores de serviço;*
- *Solicitar e gerir, quando necessário, auditoria para verificação de acessos indevidos;*
- *Solicitar, quando julgar necessário, o bloqueio de chaves de acesso de usuários;*
- *Excluir ou desabilitar as contas inativas;*
- *Fornecer senhas de contas privilegiadas somente aos Colaboradores que necessitem efetivamente de tais privilégios, mantendo-se o devido registro e controle;*
- *Garantir o cumprimento do procedimento de Backup para os servidores e Ativos, e*
- *Organizar treinamentos relacionados à segurança dos Ativos de informação periodicamente, com a finalidade de capacitar e avaliar os Colaboradores.*

3.4. Responsabilidades da Área de Compliance

- *Assessorar a Conasa na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os Ativos de informação;*
- *Liderar o processo de apuração das responsabilidades e causas quando da ocorrência de incidentes ou violações de Segurança da Informação aos regulamentos internos e externos da Conasa, ainda que auxiliado pela TI;*

- *Assegurar que as atividades da Conasa sejam desenvolvidas com base nos princípios estabelecidos em suas políticas e ou manuais internos e em consonância com a regulamentação, legislação e autorregulação aplicáveis e vigentes;*
- *Dirimir ou mitigar ao máximo a existência de conflitos de interesse relacionados ao desenvolvimento das atividades da Conasa, especialmente, para fins do disposto nesta Política;*
- *Para permitir que cumpra suas obrigações conforme acima expostas, a Diretoria de Compliance possui acesso irrestrito a todas as dependências da Conasa, inclusive salas com Controle de Acesso, bem como a toda a rede interna.*

3.5. Responsabilidades da Gerência Jurídica

- *Assessorar a Diretoria de Compliance na elaboração e verificação da legalidade dos regulamentos, termos, políticas e controles utilizados para proteger os ativos de informação;*
- *Garantir que os contratos celebrados com terceiros, sempre que necessário, contenham cláusula de Confidencialidade e que preservem a segurança das informações da Conasa;*
- *Garantir que a existência das diretrizes estabelecidas com base nesta Política e a necessidade do cumprimento de suas premissas sejam referenciadas nos contratos e acordos com terceiros, bem como nos contratos firmados com os Colaboradores da Conasa, de forma que cada um saiba suas obrigações, direitos e deveres no âmbito desta Política.*

3.6. Responsabilidades Administrativas da Área de Compliance

- *Assessorar a Diretoria de TI na criação, alteração e manutenção de novas políticas, normas, códigos ou regulamentos de Segurança da Informação;*
- *Participar, quando cabível, na apuração das responsabilidades e causas relacionadas aos incidentes ou às violações da Segurança da Informação, e;*
- *Divulgar e providenciar adesão dos novos Colaboradores, caso cabível, às normas, às políticas, aos códigos e aos regulamentos internos da Conasa, no ato da admissão.*

3.7. Responsabilidades dos Prestadores de Serviço

- *Respeitar as obrigações previstas nos respectivos contratos de prestação de serviço, especialmente para fins dessa Política, no que concerne à Segurança da Informação.*

4. GESTÃO DA INFORMAÇÃO

4.1. Classificação da Informação

As informações, sejam itens, dados, conjuntos ou documentos que circulam ou são produzidas pela Conasa, são confidenciais por definição, salvo disposição interna ou regulação ou legislação que obrigue sua divulgação. Todo Colaborador deve zelar pela manutenção de níveis de Confidencialidade adequados, e sempre que possível tornar a classificação adotada de maneira explícita, seja no desenho dos processos ou nos fluxos de informação, seja no próprio documento ou documentação daquele conjunto de informações. Todas as informações obtidas ou geradas pela Conasa e terceiros são classificadas nos seguintes níveis:

Confidencial: É o nível mais alto de segurança dentro deste padrão. As informações confidenciais são aquelas que, se divulgadas interna ou externamente, têm potencial para trazer grandes prejuízos financeiros ou à imagem da Conasa. São protegidas por rigorosos Controles de Acesso e Criptografia.

Restrita: É o nível intermediário de Confidencialidade. São informações estratégicas que devem estar disponíveis apenas para grupos restritos de Colaboradores. São protegidas por Controle de Acesso aos módulos de sistemas e/ou diretórios em nuvem.

Uso interno: Representa baixo nível de Confidencialidade. Informações de uso interno são aquelas que não podem ser divulgadas para pessoas de fora da organização, mas que, caso isso aconteça, não causarão grandes prejuízos. A preocupação nesse nível está relacionada principalmente à integridade da informação.

Pública: São dados que não necessitam de proteção sofisticada contra vazamentos, pois podem ser de conhecimento público.

Abaixo, uma tabela que lista alguns itens de informação em cada categoria:

Categoria de Classificação	***Exemplos de itens, conjuntos ou elementos de informação***
Confidencial	*Planos de negócio, Documentos de apreciação para Diretoria Colegiada, memorandos ou atas de reuniões restritas à Diretoria Colegiada, dados de Remuneração e Pessoais dos Colaboradores e Diretores, Documentos resultantes de Auditorias internas e externas, Documentos restritos de reguladores. Resultados de Background Check feito sobre Colaboradores, cotistas e outros prestadores de serviço.*
Restrita	*Estratégias de negócio ou de marketing, Documentos de Fundos de Investimento sobre operações a serem realizadas ou em realização, documentos e dados pessoais de cotistas, documentos e dados pessoais de Colaboradores.*
Uso Interno	*Apresentações internas das mais diversas, trocas de informações entre áreas, materiais de divulgação interna, políticas e manuais não públicos, documentos e dados de processos internos.*
Pública	*Apresentações institucionais, materiais de divulgação, textos de blog, documentos relativos a fundos que devem estar disponibilizados em sites públicos ou de forma pública nos sites da*

	Conasa.

4.2. Manutenção do Sigilo da Informações

As seguintes regras devem ser observadas por todos os Colaboradores, quando da utilização de informações confidenciais e/ou restritas:

Os Colaboradores devem proteger a Confidencialidade de quaisquer informações obtidas durante o exercício de suas funções na Conasa, que não devem ser (1) divulgadas a terceiros, (2) divulgadas ou disponibilizadas em domínio público, (3) copiadas ou transferidas (mesmo que por foto) a celulares, tablets, computadores pessoais ou quaisquer outros dispositivos portáteis e/ou (4) enviadas para correio eletrônico (e-mails) externos, ainda que pertencentes ao próprio Colaborador;

A obrigação de sigilo prevista no item anterior se aplica mesmo após a rescisão do vínculo do Colaborador da Conasa, qualquer que seja a razão, permanecendo o Colaborador obrigado a manter sigilo e a proteger a Confidencialidade das informações obtidas durante o exercício de suas funções na Companhia;

Os Colaboradores respondem individual, civil e criminalmente, pela divulgação indevida de Informações Confidenciais ou pela divulgação de quaisquer informações que tenham por objetivo atingir a honra ou a imagem da Conasa ou dissuadir seu relacionamento com clientes.

Questões envolvendo informações confidenciais e restritas de titularidade da Conasa não devem ser discutidas pelos Colaboradores em locais públicos, como corredores, elevadores, meios de transporte coletivos, restaurantes etc.

Os programas de correio eletrônico (e-mails) disponibilizados pela Conasa às pessoas autorizadas devem ser utilizados exclusivamente para mensagens de âmbito profissional e não podem, em hipótese alguma, ser usados para transmitir ou retransmitir mensagens ou seus anexos de qualquer natureza e conteúdo que possam comprometer a Conasa.

A Conasa adota a política de mesas limpas. Todos os Colaboradores devem evitar manter papéis e documentos confidenciais expostos em suas mesas de trabalho. Documentos confidenciais devem ser guardados em local apropriado e com chave, mesmo no decorrer do expediente, para evitar o acesso de terceiros não autorizados. Ao final do expediente, as mesas devem permanecer trancadas e sem papéis ou documentos sobre elas.

As informações confidenciais de clientes enviadas ou entregues à Conasa para execução de transações são protegidas por lei. O compartilhamento destas informações com terceiros depende de expressa autorização dos clientes, por escrito.

Nas operações passivas da Conasa, em especial quando se tratar de distribuição de cotas de fundos a clientes, quando aplicável, os Colaboradores devem firmar documentos específicos com os distribuidores dos fundos sob administração ou gestão, com dispositivos específicos prevendo:

A obrigação de os distribuidores adotarem política de privacidade e Confidencialidade de dados dos clientes;

A garantia aos clientes da devida observância destas políticas pelo distribuidor e pelas pessoas a ele vinculadas;

Minimização de riscos de imagem para a Conasa, evitando que clientes vinculem a Companhia a uma eventual falha do distribuidor na proteção das Informações Confidenciais.

A Conasa poderá revelar as informações confidenciais e restritas nas seguintes hipóteses:

Sempre que estiver obrigada a revelá-las, em virtude de dispositivo legal, ato de autoridade competente, ordem ou mandado judicial;

Aos órgãos de proteção e defesa de crédito e prestadores de serviços autorizados pela Conasa a defender seus direitos e créditos;

Aos órgãos reguladores do mercado financeiro; e

Para outras instituições financeiras, desde que dentro dos parâmetros legais estabelecidos para tanto, podendo, nesta hipótese, o usuário, a qualquer tempo, cancelar sua autorização.

4.3. Utilização de Conteúdo Protegido por Direitos Autorais

A maioria das informações e softwares que estão disponíveis em domínio público (incluindo a internet) está protegida por leis de Propriedade Intelectual, portanto:

Não é permitido obter softwares, mídias e outros conteúdos destas fontes, exceto quando houver permissão explícita por parte do respectivo proprietário e autorização pela Gerência de TI da Conasa;

Deve-se ler e compreender todas as restrições dos direitos autorais do conteúdo e, caso a Conasa não possa cumprir com as condições estipuladas, não faça Download e não utilize o respectivo material;

É proibido o uso de qualquer foto, imagem ou desenho que possua marca registrada de terceiros. Podem ser utilizadas imagens originais do Sistema Operacional ou aquelas não relacionadas a Produtos, Empresas ou Pessoas. Imagens consideradas agressivas também não devem ser utilizadas;

Em caso de dúvidas em relação às licenças ou a quaisquer dos pontos acima, o Colaborador deve entrar em contato com as áreas de Compliance e de TI.

5. RECOMENDAÇÕES DE SEGURANÇA

5.1. Privacidade

A Conasa tem o Direito de Acesso a qualquer informação salva em formato eletrônico em seus equipamentos de rede ou "nuvem", que se encontrem fisicamente no mobiliário do escritório, como, por exemplo, em mesas, estantes, gaveteiros, armários etc. Dessa forma, ainda que o Colaborador possa se utilizar da estrutura de tecnologia da organização para algum uso particular não conflitante, tais informações podem ser acessadas pela Conasa mesmo sem o prévio consentimento do respectivo Colaborador.

Com relação às ligações telefônicas, aos e-mails e outros canais de comunicação internos, a Conasa se reserva o direito de monitorar e armazenar registros das ligações e conversas de texto, bem como consultá-los sem prévio aviso ao Colaborador.

Sem prejuízo ao acima exposto, a Conasa garante que toda escuta a conversas telefônicas e mensagens de texto depende do prévio consentimento da área de Compliance. Além disso, a Companhia se compromete a zelar pelo sigilo de qualquer informação, incluindo de caráter pessoal, que eventualmente se depare nos processos de monitoramento.

5.2. Proteção do Patrimônio Físico e Intangível

Integram o patrimônio físico e intangível da Conasa, seus imóveis, instalações, veículos, equipamentos, estoques, valores, planos, produtos, tecnologia, estratégia de negócio e de comercialização, informações, pesquisas e dados que devem ser protegidos pelos colaboradores, não podendo eles serem utilizados para obtenção de vantagens pessoais e nem fornecidos a terceiros, independentemente do fim.

Não podem ser utilizados equipamentos ou outros recursos da Conasa para fins particulares, salvo se previamente autorizado pelo gestor de área, sendo a referida aprovação vetada nos casos em que interfira no seu trabalho, ou se ainda:

- *Interferir ou concorrer com os negócios da Companhia;*
- *Fornecer informações a terceiros;*
- *Envolver solicitação comercial ou outra solicitação não apropriada ao negócio, e;*
- *Envolver custo adicional para a Conasa.*

5.3. Uso do E-mail

O uso do e-mail na Conasa está baseado nas premissas de civilidade, eficiência e rapidez, sempre objetivando aumentar a produtividade nos trabalhos diários. O e-mail não deve substituir uma conversa presencial ou um telefonema, quando este for mais eficiente. Contudo, pode e deve ser usado como documento de comunicação, interno e externo. Com isso em vista, seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização desta ferramenta:

- *O usuário é o único responsável pelo conteúdo das transmissões feitas através do e-mail a partir de sua conta e senha;*
- *O uso da conta de e-mail corporativo da Conasa é para fins profissionais, sendo permitido seu uso pessoal com bom-senso para assuntos que não sejam conflitantes com as atividades da Companhia nem prejudiquem qualquer lei, regulação ou regulamento e políticas internas da Companhia.*
- *As mensagens de e-mail são confidenciais, somente podendo ser acessadas pelo remetente e seu(s) destinatário(s). É proibida a leitura de mensagens de outros usuários, mesmo que estejam abertas na tela;*
- *Não devem ser abertos arquivos ou executados programas anexados aos e-mails sem antes ter certeza de sua procedência e existência de prévia expectativa do recebimento da mensagem;*
- *Dentro do aplicativo ou visualizador de e-mails, devem sempre estar desabilitadas as opções que permitam abrir ou executar automaticamente arquivos ou programas anexados às mensagens;*
- *Não deve ser utilizado e-mail para fins ilegais;*
- *Não devem ser transmitidos quaisquer materiais ilegais ou de qualquer forma censuráveis através deste serviço;*
- *Não devem ser transmitidos quaisquer materiais que violem direitos de terceiros, incluindo, mas não se limitando aos, direitos de propriedade intelectual;*
- *Não devem ser transmitidos quaisquer materiais que violem leis ou regulamentos locais, estaduais, nacionais ou internacionais aplicáveis;*
- *O Colaborador não pode obter ou tentar obter acesso não-autorizado a outros sistemas ou redes de computadores conectados ao serviço;*
- *Não devem ser utilizados os serviços de e-mail para transmitir quaisquer materiais que contenham Vírus, arquivos do tipo "Cavalo de Tróia" ou outro programa prejudicial;*
- *Não devem ser transmitidas mensagens não-solicitadas, conhecidas como Spam ou Junk mail, correntes, chain letters ou distribuição em massa de mensagens não-solicitadas, salvo mensagens informativas de produtos e serviços da Conasa,*

aprovadas pela diretoria ou área de comunicação, por lista controlada e via Ferramentas oficiais contratas pela Companhia. Quando este envio ocorrer, deve contar com sistema de cancelamento de cadastramento na própria mensagem;

- *Mensagens com assuntos confidenciais não devem ser impressas em impressoras usadas por outros usuários, sem que se esteja cuidando para retirar a impressão antes do acesso físico ao conteúdo impresso, de forma inadvertida, pelos demais usuários;*
- *O e-mail deve estar ativo sempre que o usuário estiver trabalhando no microcomputador. Quando este se afastar de sua estação de trabalho, deve encerrar a sessão ou acionar recurso de proteção de tela com senha pessoal;*
- *É proibido aos administradores de rede ou e-mail ler mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte, salvo por necessidade de apuração de eventos que tenham causado danos, ou tenham sido classificados como potencialmente danosos à Conasa ou a terceiros ou por determinação da área de Compliance, desde que devidamente justificado, ou, ainda, de Reguladores ou Autoridades para apuração de eventos de infração de alguma regulação ou legislação, e;*
- *Não é permitido enviar músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura de rede local ou que violem as leis de direitos autorais.*

5.4. Uso do Telefone Fixo

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização destas Ferramentas:

O uso do telefone fixo na Conasa deve ter uso para fins profissionais. É permitido o uso para fins pessoais desde que com bom-senso, para assuntos que não sejam conflitantes com as atividades da Companhia nem prejudiquem qualquer lei, regulação ou regulamento e políticas internas da Conasa. Vale lembrar também que todas as ligações são gravadas e podem ser ouvidas pela Conasa como determinam suas políticas;

O uso de telefone localizado fora das dependências da Conasa para discussão de assuntos confidenciais internos pode ser necessário, principalmente em situações de contingência, porém pode gerar exposição de segurança. Portanto, deve-se sempre priorizar fazer ligações dentro da Companhia, ou pelos meios eletrônicos de telefonia e comunicação disponibilizados pela empresa via computador e/ou aplicativos aprovados pela Diretoria de TI. Caso não seja possível, deve-se certificar que não existem terceiros ouvindo a ligação;

Não se deve deixar mensagens confidenciais em secretárias eletrônicas, pois essas podem ser resgatadas por pessoas não autorizadas, e;

Ao coordenar uma teleconferência ou videoconferência, deve-se garantir que todos os participantes foram devidamente autorizados antes de começar a reunião.

5.5. Uso da Internet

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização da internet em dispositivos da organização ou na utilização de dispositivos pessoais na rede corporativa da CONASA:

Algumas páginas da internet contêm ou distribuem material não apropriado ao ambiente de trabalho. Portanto, os Colaboradores não devem acessar tais sites nem tampouco distribuir / obter material similar;

Os acessos a sites podem estar sendo monitorados a qualquer tempo, portanto, em caso de dúvida, deve-se verificar junto aos superiores imediatos ou o time de TI se o respectivo site pode ser acessado;

É permitido o uso de serviços de mensagens ou chat (WhatsApp, Hangouts, Skype, Messenger etc.) desde que para fins profissionais. O uso pessoal desses aplicativos deve ser limitado e com bom-senso, nunca com finalidades conflitantes com os interesses da Companhia, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas da Conasa. Vale lembrar também que todas as comunicações feitas em computadores da Companhia ficam armazenadas e podem ser consultadas pela Conasa como determinam suas políticas, bem como que o compartilhamento de qualquer assunto referente à Conasa é expressamente proibido, sendo apenas autorizado com expressa comunicação da Diretoria de Compliance;

É permitido o acesso às redes sociais (LinkedIn, Twitter), desde que com bom-senso, nunca com finalidades conflitantes com os interesses da Conasa, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas da Companhia. Vale lembrar também que todas as comunicações feitas em computadores da Conasa ficam armazenadas e podem ser consultadas pela Conasa como determinam suas políticas. Vale lembrar que o compartilhamento de qualquer assunto referente à Conasa é expressamente proibido, sendo apenas autorizado com expressa comunicação da Diretoria ou da área de Compliance;

O acesso aos e-mails não corporativos nos computares de propriedade da Conasa é vetado, sendo proibido o acesso por qualquer meio, inclusive via Webmail, exceto nos casos em que para viabilizar o uso de alguma ferramenta ou aplicativo autorizado pela área de TI, seja necessário o acesso a alguma conta de e-mail pessoal;

Não é permitido o uso de compartilhadores de informações como redes Peer-to-Peer, também conhecidas como redes P2P dentro das dependências da Conasa;

Não é permitido o Download de músicas, vídeos ou quaisquer outros arquivos que possam comprometer o bom funcionamento da infraestrutura local ou que violem as leis de direitos autorais;

É permitida a utilização de programas de streaming de áudio nos computadores da Conasa, desde que com bom-senso, respeitando e priorizando o uso da infraestrutura de rede para fins profissionais e desde que sejam acessos lícitos e individualizados. Não é permitido o uso de programas de streaming de vídeo, exceto com aprovação expressa e limitada (tipo, tempo etc.) pelo Gestor da área e área de TI.

5.6. Uso das Impressoras

Seguem as regras que devem ser observadas por todos os Colaboradores quando da utilização deste equipamento:

Quaisquer impressões, sobretudo as que contêm informações confidenciais, devem ser imediatamente retiradas da impressora;

Esta ferramenta deve ser utilizada apenas quando o documento físico se fizer imprescindível, evitando desperdícios ou gastos desnecessários;

As impressoras são Ferramentas para fins profissionais, objetivando aumentar a produtividade nas atividades desenvolvidas pela Conasa. Impressões para finalidade pessoal devem ser limitadas e com bom-senso, nunca com finalidades conflitantes com os interesses da Companhia, bem como nunca infringindo nenhuma lei, norma, regulamentação e normas e políticas internas da Conasa, e;

Impressões coloridas devem ser feitas apenas em caráter excepcional, quando a utilização da cor interferir na compreensão do documento ou quando a situação assim exigir.

5.7. Mesa Limpa

A política de mesa limpa consiste em não deixar informações confidenciais ou bens da Conasa, incluindo, mas não se limitando a, papéis, pen-drives ou quaisquer outros tipos de mídias removíveis ou acessíveis a outras pessoas sem a devida proteção, quando o colaborador estiver fora de sua estação de trabalho.

Ao final do dia de trabalho, em relação aos computadores portáteis, os Colaboradores devem seguir uma das seguintes recomendações: serem trancados em gaveta ou armário, serem

presos a cabos de segurança ou serem levados pelo seu responsável, conforme estabelecido pelo respectivo gestor.

5.8. Tela Limpa

Computadores, notebooks e outros dispositivos devem estar protegidos por senha quando não estiverem sendo utilizados. Todos os computadores devem ter proteção de tela automática com senha habilitada para acionamento no tempo máximo de 10 minutos de inativação.

5.9. Senhas

A Conasa adota política de troca obrigatória de senhas com período de uso contínuo de no máximo 90 (noventa) dias.
A senha é o meio de validação de acessos a recursos e serviços, funcionando como a assinatura digital do Colaborador. Portanto, devem ser verificados os seguintes cuidados básicos para sua proteção:

- *Manter sua Confidencialidade;*
- *Criar senhas fortes, respeitando, ao menos, os critérios abaixo:*
- *Evitar senhas óbvias, como aquelas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário), e*
- *Criar senhas que tenham, pelo menos, 8 caracteres, com ao menos um caractere especial e um número.*

Os acessos, validados por meio da utilização de senha, serão limitados aos recursos e serviços necessários para o desempenho das atividades exercidas por cada Colaborador, e poderão ser revogados rapidamente, quando necessário.

6. GESTÃO DA SEGURANÇA CIBERNÉTICA

6.1. Autenticação e Controle de Acesso

A prática de Controle de Acesso tem o objetivo de prevenir o acesso de indivíduos não autorizados ao ambiente e aos sistemas, garantindo a Confidencialidade das informações.

Para garantir um nível aceitável de Controle de Acessos, são executados os seguintes processos:

Controle de Acessos através da matriz de segregação de função. Na matriz estão listadas todas as equipes, Colaboradores e acessos liberados;

Execução de procedimentos formalizados para a Concessão, Alteração, Revogação e Gerenciamento de acessos, sendo que, para todos os procedimentos citados acima, é respeitado o princípio de menor privilégio e perfil mínimo restrito de acesso, conforme a matriz de segregação de função;

Todos os usuários são orientados a possuírem acesso apenas à informação de acordo com as necessidades de negócio;

É de responsabilidade do gestor da equipe o informe do nível de acessos para novos Colaboradores. Os acessos são limitados aos ativos de informação sob domínio da equipe do gestor;

Todos os procedimentos de Concessão e Alteração do Acesso dentro de uma equipe são aprovados pelo gestor responsável e pela área de TI;

Existem casos específicos de Colaboradores que necessitam de acesso aos ativos de informação pertencentes à outras equipes. Para estes casos, todos os procedimentos de Concessão e Alteração são aprovados pelo gestor responsável da equipe do colaborador, gestor da equipe detentora dos ativos de informação, e Gerência de TI;

A Conasa realiza revisão de acessos, no mínimo, anualmente, conforme Política, que tem como objetivo a atualização dos acessos e permissões, procedimento este que é coordenado pela Gerência de TI, sendo o resultado da revisão enviado para a anuência da Diretoria Colegiada.

6.2. Serviços de diretório

Serviços de diretório desempenham um papel importante no desenvolvimento de aplicações intranet e Internet permitindo o compartilhamento de informações sobre usuários, sistemas, redes, serviços e aplicações através da rede.

A Conasa utiliza mais de um servidor de diretório em paralelo para minimizar riscos de falhas. Os diretórios possuem sincronização ativa, logo, compartilham dos mesmos usuários, grupos, senhas e demais informações.

Sempre que possível os sistemas adquiridos e desenvolvidos possuirão login integrado com o serviço de diretório em nuvem (Microsoft 365) da Conasa, mantendo um canal único e centralizado de gestão de acessos.

6.3. Gerenciamento de Senhas e Acessos

A Conasa disponibiliza a todos os Colaboradores um serviço de cofre seguro, que é o meio ideal para armazenar e gerenciar informações confidenciais compartilhadas, como senhas, documentos e identidades digitais.

A ferramenta fornece controles de segurança preventiva e de investigação, através de fluxos para rotinas de aprovação e alertas em tempo real sobre senhas de acesso. Ela permite ainda auditorias de segurança da reunião e conformidade regulamentar, como SOX, HIPAA e PCI.

6.4. Controle Contra Software Malicioso

Os malwares de computador são programas desenhados para causar perda ou alteração de dados do computador. Assim, todo equipamento da Conasa deve ter um programa Antivírus/antimalware instalado. Os softwares Antivírus devem ser atualizados diariamente e de forma automática.

O Colaborador, ao receber alerta de Vírus de qualquer fonte que não seja o Antivírus, não deve acessá-lo ou encaminhá-lo a outras pessoas, pois geralmente estes alertas são falsos. *De toda forma, permanecendo a dúvida, o Colaborador deve entrar em contato com a área de Tecnologia para maiores explicações e suporte técnico.*

6.5. Atualizações

O Sistema Operacional, Antivírus e demais sistemas devem permanecer atualizados. O sistema operacional dos equipamentos de Colaboradores deve permanecer com as atualizações automáticas sempre ativas, salvos os casos específicos de compatibilidade de sistemas defasados ou testes em ambientes simulados.

6.6. Rastreabilidade

Todas as soluções, sejam elas adquiridas ou desenvolvidas, possuem geração ativa de logs de erros, eventos críticos, entrada e saída de informações relevantes, entre outros eventos. Esse registro pode ser utilizado para restabelecer o estado original de um sistema, para que um administrador conheça o seu comportamento no passado ou até mesmo para análise de auditorias internas e externas.

Trilhas de auditoria automatizadas devem ser implantadas para todos os componentes de sistema para reconstruir os seguintes eventos:

- *Autenticação de usuários (tentativas válidas e inválidas);*
- *Acesso a informações; e*
- *Ações executadas pelos usuários, incluindo criação ou remoção de objetos do sistema.*

6.7. Cópias de Segurança (Backup)

A importância dos Backups na administração de sistemas nunca pode ser minimizada. Sem eles, muitos dados são simplesmente irrecuperáveis caso sejam perdidos devido a uma falha acidental ou a um Incidente de Segurança.

Cada departamento/usuário tem acesso a, pelo menos, uma pasta no servidor e/ou serviço de nuvem de arquivos. Todos os documentos relacionados ao negócio devem ser armazenados nestas pastas. Além disso, cada usuário tem uma pasta individualizada para uso profissional no servidor e/ou serviço de nuvem de arquivos.

Qualquer arquivo armazenado em pastas locais nos computadores não é passível de Backup; consequentemente, o armazenamento nesses locais é de total responsabilidade do usuário.

O Backup dos servidores de aplicações e bancos de dados e aplicações críticas e arquivos deve ocorrer várias vezes ao dia, de forma automatizada e terá a retenção seguindo as diretrizes a seguir.

Observar o arquivo POP.TI01R01.DOC em anexo.

Todos os e-mails, anexos e arquivos armazenados no diretório em nuvem possuem um serviço de Backup a parte. O serviço monitora o volume de alterações nestes documentos e cria versões automaticamente, podendo gerar até 6 (seis) Backups por dia. Todas as versões geradas permanecem armazenadas enquanto o serviço estiver contratado, por prazo indefinido.

6.8. Testes de Intrusão

Testes de Intrusão interno e externo nas camadas de rede e aplicação devem ser realizados, no mínimo, anualmente.

6.9. Varredura de Vulnerabilidades

As varreduras das redes internas e externas devem ser executadas periodicamente ou sempre que houver mudança significativa na estrutura tecnológica. As vulnerabilidades identificadas devem ser tratadas e priorizadas de acordo com seu nível de criticidade.

6.10. Segmentação de Rede

As definições de rede estão especificadas no Manual de Infraestrutura e devem seguir as regras para garantia da segurança das informações nela trafegadas:

Computadores conectados à rede corporativa não devem ser acessíveis diretamente pela Internet;

Não é permitida a conexão direta de rede de terceiros utilizando-se protocolos de controle remoto aos servidores conectados diretamente na rede corporativa;

Para solicitação de criação, alteração e exclusão de regras nos firewalls e ativos de rede, o requisitante deve encaminhar pedido à área de TI, que fará a análise, aprovação e execução da configuração.

6.11. Desenvolvimento Seguro

A Conasa mantém um conjunto de princípios para desenvolver sistemas de forma segura, garantindo que a segurança cibernética seja projetada e implementada no ciclo de vida de desenvolvimento de sistemas.

7. RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

7.1. Contexto Geral

As respostas aos incidentes de Segurança da Informação visam assegurar o restabelecimento do nível normal do ambiente tecnológico, após o acontecimento de um sinistro, através do direcionamento na utilização dos recursos e dos procedimentos fundamentais, no intuito de garantir uma resposta efetiva.

7.2. Planejamento

Esta atividade contempla a identificação, a prevenção e a descrição de situações de possíveis sinistros, bem como suas respectivas ações de mitigação, responsáveis, tempos e registros, de forma que, em situações reais, as atividades já estejam previamente mapeadas e as ações já preestabelecidas. Assim, deve constar no planejamento:

A definição de uma equipe de planejamento, suas responsabilidades e papéis predefinidos, para prever situações de sinistro e as possíveis respostas, assim como atuar no monitoramento e na resposta aos incidentes;

A definição do catálogo dos recursos tecnológicos existentes no parque da Conasa, bem como aqueles necessários para possibilitar uma atuação efetiva na resposta aos incidentes, como, por exemplo: cadastro de todos os servidores;

O detalhamento das ações necessárias na resposta a incidentes, conforme o tipo e criticidade, deve abordar o tempo mínimo de resposta e a quem os incidentes devem ser reportados, entre outros.

Os casos que, em virtude de sua relevância, devem ser previamente autorizados pela alta gestão;

O Plano de Continuidade do Negócio ("PCN" ou "Plano" em outras políticas da Conasa) atualizado, envolvendo os ambientes e processos críticos da Conasa, uma vez que o processo de recuperação pode envolver o acionamento de um processo de continuidade do negócio, a fim de restabelecer a operação normal da Conasa.

As implementações para o ambiente tecnológico existente deverão ser adequadas a esta Política no prazo de 1 (um) ano, a partir de sua publicação.

Caso não seja possível a adequação de alguma ferramenta ou componente, a equipe de planejamento deve documentar essa informação, bem como seus motivos, para fins de auditoria interna.

7.3. Identificação

Esta atividade compreende realizar ações para identificação e registro dos sinistros.

Através dos recursos de detecção na rede de monitoramento dos servidores e recursos de tecnologia ou através de problemas reportados pelos usuários, podem ser identificados alertas de segurança que configurem incidentes de segurança. Diante disso, o alerta será analisado e as devidas providências serão tomadas, tanto no tratamento do incidente, quanto no encaminhamento do problema para a gestão.

Algumas situações podem ser consideradas na notificação de um evento de Segurança da Informação:

- *Violação da Disponibilidade, Confidencialidade e integridade da informação;*
- *Inconformidade das políticas e/ou procedimentos;*
- *Alterações de sistemas sem controle;*
- *Funcionamento indevido de software ou hardware; e*
- *Violação de acesso lógico.*

Eventos, mesmo que apenas suspeitos, devem ser analisados e validados rapidamente. Uma vez confirmada a ocorrência de um incidente, a análise de seu escopo deverá ser executada. Essa análise deve prover informações suficientes que permitam identificar e priorizar as atividades subsequentes.

Todos os usuários são responsáveis por relatar qualquer tipo de eventos e fragilidades, que possam causar danos à Segurança da Informação. A notificação do evento ou fragilidades por parte do usuário deverá ser registrada por e-mail para a equipe de tecnologia.

Nenhum Colaborador deve investigar por conta própria ou tomar ações para se defender de eventual ataque, a não ser que seja instruído desta forma pela área de TI.

7.4. Resposta

A atividade de resposta a incidentes de Segurança da Informação compreende reações aos possíveis ataques realizados.

A partir da detecção de um Incidente de Segurança, é importante controlá-lo antes que uma possível extensão comprometa outros recursos. Como exemplo, tem-se uma infecção por Vírus em um computador e que, se não for controlada em tempo, pode comprometer outros computadores da rede;

A estratégia de resposta ao Incidente de Segurança da Informação a ser adotada deve ser baseada no tipo (e.g., Vírus, perda de arquivo, incêndio etc.) e na criticidade do incidente (e.g., impacta na imagem ou nos negócios da Conasa, compromete várias áreas, entre outros).

Após a identificação e a confirmação que o incidente se trata de um evento de Segurança da Informação, ou seja, que viole a Disponibilidade, a Confidencialidade ou a Integridade da informação, a resposta deverá ser realizada a partir das seguintes ações:

Preservar, na medida do possível, todas as evidências, para que seja possível identificar o problema, rastrear a possível causa e servir como evidência em eventuais questionamentos;

Verificar se existem planos de ação em que o sinistro identificado esteja previsto, no intuito de seguir o planejamento;

Agir para que os serviços afetados sejam disponibilizados em seu estado normal de funcionamento no menor tempo possível;

Utilizar todos os recursos necessários para a implementação de uma estratégia de reação, seja permanente ou provisória;

Utilizar atividades de recuperação, tais como: a restauração de Backups de sistemas, a instalação de patches, a alteração de senhas e a revisão da segurança do perímetro da rede da Conasa.

Quando as consequências do incidente estiverem contidas, é necessário que sejam solucionados todos os componentes do incidente, como, por exemplo: remover um código malicioso ou desabilitar contas de usuários violadas.

7.5. Vistoria

A vistoria consiste em ações realizadas após a ocorrência do incidente, como auditorias e análises de vulnerabilidade.

É fundamental assegurar que as atividades envolvidas nas respostas aos incidentes sejam adequadamente registradas para futuras análises. Os registros servirão de banco de conhecimento para resposta em incidentes semelhantes;

De acordo com o incidente, uma análise mais aprofundada deve ser conduzida para identificar a origem do incidente para que o tratamento das fragilidades e/ou não conformidade encontradas contribuam para a resolução do incidente;

Periodicamente, a área de TI deve realizar uma análise no ambiente tecnológico com o objetivo de identificar possíveis vulnerabilidades e, de forma antecipada, eliminá-las;

Após a identificação das possíveis vulnerabilidades, deverá ser aberto uma ocorrência na Central de Serviços e comunicada às áreas responsáveis para as devidas tratativas. Após a resolução, deve ser encerrada a ocorrência e registrada as ações realizadas.

7.6. CONSIDERAÇÕES FINAIS

O desconhecimento em relação a qualquer das obrigações e compromissos decorrentes deste documento não justifica desvios. Portanto, em caso de dúvidas ou necessidade de esclarecimentos adicionais sobre seu conteúdo, favor consultar as áreas de TI e de Compliance.

O descumprimento dos preceitos deste documento ou de outros relacionados pode acarretar medidas disciplinares, administrativas ou judiciais cabíveis, podendo levar à demissão ou outras sanções, inclusive decorrentes da legislação, autorregulação ou regulamentação aplicável.

Este documento é de uso interno, porém, em alguns casos, pode ser disponibilizado a terceiro mediante prévio consentimento da área de Compliance, sendo certo que o respectivo envio deve ser realizado exclusivamente em meio físico ou em formato "pdf" (documento protegido), contendo as diretrizes de Confidencialidade.

7.7. ANEXO I – GLOSSÁRIO

Os termos iniciados com letra maiúscula na Política de Segurança da Informação da Conasa deverão ser interpretados com o significado a seguir:

***Antivírus:** programa que detecta e elimina vírus de computador.*

***Backup:** cópia exata de um programa, disco ou arquivo de dados feito para fins de arquivamento ou para salvaguardar informações.*

***Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.*

***Controle de Acesso:** conjunto de restrições ao acesso às informações de um sistema exercido pela equipe de segurança da informação.*

***Criptografia:** arte/ciência de utilizar matemática para tornar a informação segura, criando um grande nível de confiança no meio eletrônico.*

***Direito de Acesso:** privilégio associado a um cargo, pessoa ou processo para ter acesso a um ativo.*

***Disponibilidade:** garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.*

***Download:** transferência de arquivo de um computador remoto para outro computador através da rede.*

***Ferramentas:** conjunto de equipamentos, programas, procedimentos, normas e demais recursos através dos quais se aplica a Política de Segurança da Informação das entidades.*

***Incidente de Segurança:** qualquer evento ou ocorrência que promova uma ou mais ações que comprometam ou que sejam uma ameaça à integridade, autenticidade, ou disponibilidade de qualquer ativo.*

***Integridade:** salvaguarda da exatidão e completeza da informação e dos métodos de processamento.*

***Junk mail**: e-mails não solicitados por usuários não interessados em recebê-los. Log: registro das transações ou atividades realizadas em sistema de computador.*

Nobreak: *sistema de fornecimento de energia ininterrupta com baterias, que mantém o computador funcionando por um determinado período.*

Peer-to-Peer: *rede por meio da qual usuários compartilham entre si seus recursos, possibilitando a provisão de conteúdo e serviços à rede.*

Política de Segurança: *conjunto de diretrizes destinadas a definir a proteção adequada dos ativos produzidos pelos sistemas de informação.*

Proteção dos Ativos: *processo pelo qual os ativos devem receber classificação quanto ao respectivo grau de sensibilidade. O meio de registro de um ativo de informação deve receber a mesma classificação de proteção dada ao ativo que o contém.*

Segurança da informação: *preservação da Confidencialidade, integridade e disponibilidade da informação.*

Senha Fraca ou Óbvia: *senha que utiliza caracteres de fácil associação ao seu dono, que seja muito simples ou pequena, tais como: datas de aniversário, casamento, nascimento, o próprio nome do usuário, nome de seus familiares, sequências numéricas simples, palavras com significado, dentre outras.*

Spam: *e-mail não solicitado enviado a grande número de endereços eletrônicos, que geralmente visam fazer propaganda de produtos e serviços.*

Vírus: *programa construído para causar danos aos softwares do computador.*
Cavalo de Tróia (Trojan Horse): programa que pode danificar áreas da máquina e torná-la vulnerável ao ataque de hackers.