COAGRU COOPERATIVA AGROINDUSTRIAL UNIÃO

PSIPD

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS

VERSÃO 1.0

Parábola do Semeador

Um semeador saiu a semear e, semeando,
Parte da semente caiu ao longo do caminho;
os pássaros vieram e a comeram.

Outra parte caiu em solo pedregoso,
onde não havia muita terra e nasceu logo,
porque a terra era pouco profunda.

Logo, porém, que o sol nasceu,
queimou-se por falta de raízes.

Outras sementes caíram entre espinhos;
Os espinhos cresceram e as sufocaram.
Outras, enfim, caíram em terra boa:
deram bons frutos.

(Mt. 13,3-8)

Coagru, a semente que deu certo.

PALAVRA DO PRESIDENTE

LEI GERAL DE PROTEÇÃO DE DADOS

A segurança e a privacidade de dados pessoais sempre foram uma preocupação na Coagru. Agora, a cooperativa está reforçando e intensificando seu trabalho de proteção de informações e documentos, motivada pela Lei Geral de Proteção de Dados, nº 13.709/2018, que trata da coleta, armazenamento, tratamento e compartilhamento de dados pessoais.

Essa lei nos atribui um papel muito importante, que é o de preservar a privacidade dos dados pessoais por nós coletados, sejam de cooperantes, colaboradores ou outras pessoas, físicas ou jurídicas, com as quais nos relacionamos no dia a dia.

Essa proteção não se restringe unicamente aos dados que possuímos armazenados em nossos sistemas informatizados, mas também a todo e qualquer registro físico disponível na cooperativa.

Buscando a adequação a essas exigências legais, adaptamos nossas rotinas e procedimentos internos e estabelecemos uma Política de Segurança da Informação e Proteção de Dados (PSIPD), que deve ser seguida por todos os detentores de informações, a fim de orientar e estabelecer as diretrizes que utilizaremos para tratar os dados pessoais que estão sob nosso controle de forma tão importante quanto a entrega de serviços de qualidade ímpar.

O objetivo é, de forma gradativa e estratégica, preparar todos os colaboradores para as mudanças decorrentes da LGPD, engajando-os para que a governança de dados esteja em conformidade com a lei.

Cavalini Carvalho
Diretor Presidente

CONSELHO DE ADMINISTRAÇÃO DA COAGRU (Gestão 2022-2026)

Cavalini Carvalho	Diretor Presidente	Ubiratã
Áureo Zamprônio	Diretor Vice-Presidente	Ubiratã
Valdir Batista	Diretor Secretário	Ubiratã
Alberto Ribeiro Marques		Ubiratã
Clari Luiz de Lazari		Nova Cantu
Jefferson Luiz dos Santos Cunha		Yolanda
José Luiz Caldeira		Anahy
Jurandir Leonildo Zampieri		Ubiratã
Luiz Carlos Canola		Rio Verde
Maria de L. Ribeiro de Souza		Yolanda
Nelson Negretti Stranhieri		Nova Cantu
Nelson Vieira de Andrade		Campina da Lagoa
Neusa Pontelo		Ubiratã
Rogério Saran de Alencar		Ubiratã
Rubens Gomes Reis		Campina da Lagoa
Vinicius Saran Leviski		Rio Verde

CONSELHO FISCAL DA COAGRU

Adalberto Simões	Anahy
Antonino Romangnoli	Nova Cantu
Inivaldo Pinheiro de Freitas	Campina da Lagoa
Moacir Nuto de Lacerda	Rio Verde
Sônia de Campos Jumes	Ubiratã
Waldeir Souza de Oliviera	Yolanda

SUMÁRIO

1 INTRODUÇÃO

O propósito deste documento é estabelecer e apresentar diretrizes de condutas adequadas de Segurança da Informação e Proteção de Dados da **COAGRU COOPERATIVA AGROINDUSTRIAL UNIÃO**.

A Política de Segurança da Informação e Proteção de Dados (PSIPD), atende às boas práticas de mercado, visa orientar os colaboradores, cooperantes, clientes, fornecedores e demais que se relacionem com a Coagru, bem como define as diretrizes, as normas e os procedimentos de segurança das informações institucionais.

2 OBJETIVO

A Política de Segurança da Informação e Proteção de Dados (PSIPD) tem por objetivo instituir diretrizes estratégicas, mecanismos e controles que visam garantir atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos e armazenados, sob guarda ou transmitidos, por qualquer meio ou recurso, contra ameaças e vulnerabilidades.

Desse modo, a PSIPD busca preservar os ativos de informação, reduzir riscos de ocorrência de perdas e alterações destes, bem como de acessos indevidos a informações da Coagru e, sobretudo, preservar a sua imagem institucional.

A finalidade desta Política é preservar as informações no que diz respeito à:

- **Confidencialidade:** garantia de que o acesso à informação seja obtido somente por pessoas autorizadas;
- **Integridade**: garantia de fidedignidade e autenticidade das Informações. Propriedade que garante a não violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão indevida, acidental ou proposital.
- **Disponibilidade**: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

3 REQUISITOS PARA IMPLEMENTAÇÃO DA PSIPD

- Ter o apoio da Diretoria executiva da Coagru para implantação desta PSIPD;
- Criar grupo de trabalho ou Comissão multidisciplinar para dirimir questões relacionadas à PSIPD;
- Alinhar a PSIPD à natureza e finalidade institucionais;
- Dar plena publicidade à PSIPD, seja para o público interno (conselheiros, dirigentes, colaboradores) quanto ao público externo (cooperantes, clientes, fornecedores e demais titulares de dados).

4 ABRANGÊNCIA

A presente Política de Segurança da Informação e Proteção de Dados (PSIPD), alcança todos os processos que tratam ativos de informação da Coagru, digitais e analógicos, que se relacionam à Coagru e a dados dos seus titulares.

Portanto aplica-se a todas as pessoas que trabalham na Coagru, sejam colaboradores, estagiários, dirigentes, bem como a qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Coagru mantém relacionamento, dentre os quais: cooperantes, clientes, fornecedores e prestadores de serviço.

5 REFERÊNCIAS

Esta Política foi desenvolvida tendo como suporte normativo as seguintes normas:

- Norma ABNT NBR ISO/IEC Família 27000: Sistema de Gestão de Segurança da Informação (SGSI);
- Decreto-Lei nº 5.452, de 1º de maio de 1943: aprova a Consolidação das Leis do Trabalho (CLT);
- Lei Geral de Proteção de Dados Pessoais (LGPD): Lei nº 13.709/2018;
- Lei de Diretos Autorais: Lei nº 9.610/1998;
- Normativos próprios da Coagru.

Esta Política deverá ser lida e interpretada juntamente com as seguintes normas da Coagru:

- Manual do colaborador.
- Regulamento Interno de Conduta Aplicável ao Quadro de Colaboradores da Coagru.
- Instrução Normativa Nº 362.

6 DIRETRIZES GERAIS

6.1 Comissão de Segurança da Informação e Proteção de Dados

A Comissão **de Segurança da Informação e Proteção de Dados** é o órgão responsável pela aplicação desta Política na Coagru, autônomo em decisões de sua alçada, de caráter multiprofissional, vinculado diretamente à Diretoria Executiva. Sua composição, organização e funcionamento estão previstos na Resolução da Diretoria Nro. 2085 de 01/11/2021.

6.2 Proteção da Informação

As diretrizes de segurança da informação e proteção de dados estabelecidas nesta PSIPD se aplicam às informações originadas em papel e em meio digital, as convertidas para papel e meio digital, faladas, armazenadas, acessadas, produzidas, utilizadas, editadas, recebidas e transmitidas pela Coagru. Essas diretrizes devem ser seguidas pelos usuários, os quais deverão atuar com responsabilidade e de acordo com o previsto nesta PSIPD.

Toda informação relacionada às operações da Coagru, gerada ou desenvolvida nas dependências da Coagru, físicas e virtuais, constitui ativo desta, independente da forma apresentada ou do meio pelo qual é compartilhada ou armazenada.

A informação deve ser utilizada unicamente para a finalidade para a qual foi autorizada e estritamente para o propósito institucional.

É diretriz que toda informação de propriedade da Coagru deve ser protegida de riscos e ameaças, que possam comprometer a confidencialidade, integridade, disponibilidade ou autenticidade destas, através de medidas técnicas e administrativas tais como: perfis de acesso, controle de senhas, troca de senhas, armários com chaves, dentre outros.

Para consolidar a proteção da informação, garantir sua disponibilidade e segurança das informações tratadas, a Coagru, por meio das respectivas áreas responsáveis pelos procedimentos, sistemas, serviços e utilização destes, deve estabelecer, cumprir e fazer cumprir os procedimentos da PSIPD e demais normativos internos.

6.3 Confidencialidade de Dados e Informações

A COAGRU obriga-se a preservar a confidencialidade dos dados cadastrais e pessoais dos colaboradores, cooperantes, clientes, fornecedores e parceiros, e os utilizará tão e somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas para proteger tais dados, de acordo com a presente Política de Segurança da Informação e Proteção de Dados e pela Lei Geral de Proteção da Dados (LGPD).

São consideradas informações confidenciais, para os fins desta Política, as descritas no parágrafo anterior, bem como quaisquer informações não disponíveis ao público ou reservadas, tais como dados, especificações técnicas, desenhos, manuais, esboços, modelos, amostras, materiais promocionais, projetos, estudos, documentos e outros papéis de qualquer natureza, tangíveis ou em formato eletrônico, arquivos em qualquer meio, programas e documentação de computador, comunicações por escrito, verbalmente ou de outra forma reveladas para a Coagru.

O usuário que receber informações confidenciais deverá mantê-las e resguardá-las em caráter sigiloso, bem como limitar seu acesso, controlar cópias de documentos, dados e reproduções que porventura sejam extraídas da mesma, sob pena de se responsabilizar pelo seu uso indevido. Dados considerados sensíveis e de menores devem ter atenção redobrada.

Nenhum dado ou informação confidencial pode ser compartilhado com terceiros, interna ou externamente à Coagru, sem consentimento por escrito, sob pena de aplicação das sanções previstas no item 6.5, desta Política.

6.4 Responsabilidades

É missão e responsabilidade de cada colaborador, estagiário, dirigente, bem como de qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Coagru mantém relacionamento: fornecedores, prestadores de serviço, cooperantes, clientes, dentre outros, observar e seguir as políticas, padrões, procedimentos e orientações estabelecidas para o cumprimento da presente PSIPD.

É imprescindível que cada envolvido compreenda o papel da segurança da informação e proteção de dados pessoais em todas as suas atividades prestadas para a Coagru, que devem respeitar a legislação vigente e a normatização proposta por órgãos e entidades reguladoras, com relação à segurança dos dados e informações.

É também obrigação de cada usuário se manter atualizado em relação a esta PSIPD e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso, tratamento e/ou descarte de informações.

Para auxiliar todos os envolvidos, a Comissão de Segurança da Informação e Proteção de Dados da Coagru é responsável por gerenciar as políticas e padrões que apoiam a todos na proteção dos ativos de informação e proteção de dados, além de auxiliar na resolução de problemas relacionados ao tema e disseminação do conteúdo desta PSIPD.

6.5 Descumprimento e Sanções

As violações de segurança devem ser imediatamente informadas à Comissão de Segurança da Informação e Proteção de Dados da Coagru, as quais serão apuradas nos termos dos normativos internos, garantida a ampla defesa e contraditório de todos os envolvidos, com vistas a adoção das medidas necessárias, inclusive a correção da falha, se houver, ou reestruturação de processos.

O descumprimento das diretrizes desta PSIPD e a violação de normas, sujeitam os envolvidos, além das sanções disciplinares cabíveis, inclusive a rescisão do contrato de trabalho, se colaborador for, à eventual responsabilização civil e criminal.

7 DIRETRIZES ESPECÍFICAS

7.1 Gestão de Ativos

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho ou atividade, respeitando as recomendações técnicas, comportamentais e de sigilo específicas aplicáveis.

Como condições gerais para a gestão e o uso aceitáveis dos ativos de informação e dados dos titulares, esta PSIPD considera:

7.1.1 Acessos e Recursos de Rede

I. O acesso e o uso de todos os sistemas de informação, pastas de rede, bancos de dados e demais recursos (computadores, servidores de documentos e arquivos, impressoras, câmeras de vídeo, telefones, sistemas de videoconferência e áudio conferência) devem ser restritos a pessoas expressamente autorizadas, de acordo com a necessidade para o cumprimento de suas atividades laborais e durante o exercício das mesmas nos ambientes da Coagru (físicos ou virtuais) ou externos a ela.
II. O acesso a dados, informações, sistemas, serviços e redes, seja nos ambientes da Coagru (físicos ou virtuais) ou externos a ela, via VPN, ou rede particular quando se aplicar, deve ser solicitado e/ou revogado conforme regras estabelecidas pelo Departamento de Tecnologia da Informação.
III. Todo acesso será monitorado e se verificada a ocorrência de acessos desnecessários ou com poder excessivo, estes serão imediatamente revogados. A concessão de acesso às informações e sistemas deve ser autorizada com base na regra de mínimo acesso necessário para o desempenho da função.
IV. Acessos fornecidos sob a forma de *login* (usuário e senha), seja para acesso à rede corporativa, e-mail, sistemas entre outros, sempre deverão ser realizados através de uso de senhas sigilosas. Senhas são de uso pessoal e intransferível, tendo sua divulgação e compartilhamento vedados sob qualquer hipótese, devendo ser alterada conforme as regras estabelecidas pelo Departamento de Tecnologia da Informação da Coagru.
V. O Departamento de Tecnologia da Informação da Coagru poderá bloquear o *login* de qualquer usuário, no caso de suspeitas de vazamento de senhas ou de tentativas consecutivas de violação de acesso.
VI. Concessão e revogação de acessos para colaboradores, estagiários, dirigentes, bem como qualquer pessoa física ou jurídica, de Direito Público ou Privado, com quem a Coagru mantém relacionamento: fornecedores, prestadores de serviço, cooperantes e clientes, deverá ser registrada pelo Departamento de Tecnologia da Informação da Coagru através de chamado técnico.

7.1.2 Correio Eletrônico (e-mail) e Sistemas de Mensageria

I. A Coagru fornecerá, a seu critério exclusivo, o acesso às plataformas digitais e correio eletrônico (e-mail) ao colaborador, com o respectivo domínio, em sua admissão através de perfis de acessos previamente definidos, baseados em cargos e funções.
II. Por quaisquer meios de correio eletrônico, e-mail, mensageria e correspondência, o usuário é responsável pelas informações recebidas, enviadas e compartilhadas, bem como pela sua guarda, confidencialidade e publicidade.
III. As plataformas de colaboração, correio eletrônico e mensageria disponibilizadas pela Coagru, deverão ser utilizadas para fins corporativos e relacionados às atividades do colaborador, enquanto se mantiver o vínculo empregatício.
IV. As mensagens de correio eletrônico sempre deverão incluir assinatura conforme o padrão estabelecido pela Coagru.
V. É obrigatória a manutenção da caixa de e-mails pelo respectivo usuário, evitando acúmulo de e-mails e arquivos desnecessários.

VI. O uso dos recursos de correio eletrônico, bem como o conteúdo das mensagens poderão ser vistoriadas por amostragem, estando a Coagru autorizada a ler, copiar, e/ou bloquear mensagens que violem as normas estabelecidas nesta PSIPD e demais normativos da Coagru.
VII. É importante verificar o uso da ferramenta para que o envio de mensagens não seja caracterizado como SPAM, lixo eletrônico ou malware, abstendo-se de:
- Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização concedida pelo proprietário desse ativo de informação;
- Produzir, transmitir ou divulgar mensagem que não estejam de acordo com os demais normativos internos da Coagru e/ou com a legislação vigente;
- Enviar mensagens contendo material protegido por direitos autorais sem a permissão do detentor dos direitos;
- Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas na legislação vigente ou ato normativo interno.

7.1.3 Internet (Rede Mundial)

I. Qualquer informação que for acessada, transmitida, recebida ou produzida na internet estará sujeita a divulgação e auditoria. Portanto, a Coagru reserva-se o direito de monitorar e registrar todos os acessos à internet.
II. Os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de responsabilidade da Coagru, que analisará e, se necessário, bloqueará qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em unidade de armazenamento de dados local, na estação de trabalho, ou em áreas privadas da rede, visando assegurar o cumprimento desta PSIPD.
III. É proibido o acesso a sites da internet ou quaisquer arquivos digitais, bem como sua produção e propagação, que estejam em desacordo ao estabelecido nos demais normativos internos da Coagru, possuam conteúdo ilegal, pornográfico, preconceituoso, racista, bem como objetos, fatos, imagens, conceitos, opiniões e outros que possam disseminar o ódio e a violência e influenciar atitudes alheias aos interesses da Coagru, expondo pessoas físicas ou jurídicas, produtos, marcas ou assemelhados à exposição pública, calúnia, injúria e/ou difamação.

7.1.4 Dispositivos de Acesso (Computadores, Notebooks, Smartphones e ou dispositivos similares), Móveis e Mídias Removíveis

I. A Coagru, na qualidade de proprietária dos dispositivos fornecidos aos usuários, reserva-se o direito de inspecioná-los a qualquer tempo, sendo de incumbência da Departamento de Tecnologia da Informação da Coagru realizar o controle e supervisão do uso dos mesmos dispositivos.
II. O usuário do dispositivo mantido pela Coagru e utilizado para fins corporativos, é responsável por sua conservação, segurança, bloqueio de acesso por meio de senhas e/ou outros recursos, cópia de segurança dos dados, e notificação do seu gestor imediato, Departamento de Tecnologia da Informação e área patrimonial da Coagru em caso de extravio, furto, roubo ou danos.
III. Não é permitida, em nenhuma hipótese, a alteração da configuração dos sistemas operacionais dos equipamentos, em especial os referentes à segurança e à geração de logs,

sem a devida comunicação e a autorização da Departamento de Tecnologia da Informação da Coagru.

IV. Os dispositivos móveis devem ser controlados e supervisionados pela Coagru, sendo ao usuário confiado o correto uso, guarda e segurança do mesmo.
V. O uso de mídias removíveis (cartões de memória, disquetes, pen-drive, pen USB e similares) não é recomendado, pois, trata-se de uma das maiores fontes de ameaças a vulnerabilidades, tanto no sentido de injetar ataques cibernéticos na Rede Corporativa, bem como fontes de vazamento de informações. Contudo, caso seja imprescindível a utilização das mesmas, atuar com toda a cautela possível e, quando estas não forem mais necessárias, deverão ser descartadas de forma segura e protegida.

7.1.5 Computação em Nuvem

O uso das "plataformas de nuvem" para transmissão e armazenamento de informações, só poderá ocorrer nas plataformas formalmente contratadas pela Coagru e disponibilizadas pela Departamento de Tecnologia da Informação.

7.1.6 Redes e Mídias Sociais

I. O uso das redes e mídias sociais institucionais, por parte dos colaboradores, deve ser regido pelas determinações contidas nesta PSIPD, e por demais normativas a ela complementares.
II. A gestão dos perfis institucionais da Coagru nas redes sociais deve ser realizada por colaboradores competentes e/ou por terceirizados contratados para tal, devidamente autorizados, identificados e instruídos de forma a preservar a imagem institucional, sendo vedado aos demais colaboradores a criação de perfis em nome da Coagru.
III. Quanto ao conteúdo das publicações nas redes e mídias sociais fica vedado divulgar informações sigilosas e internas da Coagru ou da vida pessoal e profissional de qualquer pessoa física sem a devida autorização; difamar pessoas ou divulgar assuntos que venham prejudicar a imagem da Coagru ou de terceiros; discriminar e compartilhar temas que venham prejudicar pessoas ou grupos de pessoas, por qualquer motivo.
IV. A Coagru detém legalmente a propriedade intelectual e os direitos autorais de suas obras e criações, composta sobretudo por bens imateriais, tais como marcas, obras intelectuais, nomes empresariais, fotografias e obras audiovisuais, as quais somente podem ser divulgadas nas redes e mídias sociais ou em quaisquer outros meios, para fins profissionais, sendo vedado o uso para fins particulares.

7.1.7 Dados e Informações

I. A Coagru preservará a confidencialidade dos dados cadastrais e pessoais dos seus titulares e os utilizará tão somente para propósitos legítimos e específicos, de modo adequado e conforme as necessidades institucionais, utilizando-se das medidas técnicas e administrativas aptas a proteger tais dados pessoais de acordo com a Lei Geral de Proteção de Dados (LGPD).
II. A Coagru decidirá sobre o compartilhamento ou restrição de acesso aos dados e informações, sob sua gestão, bem como adotará meios de monitoramento do uso dos seus dados.
III. Cabe ao usuário da informação tratar as informações que estejam sob seus cuidados com zelo e de acordo com os princípios desta PSIPD e jamais, sob qualquer fundamento, tentar acessar

informações e dados sem autorização para fazê-lo e sem correlação com suas funções laborais.

IV. Cabe ao usuário da informação documental proceder a guarda dos documentos que estejam sob seus cuidados em locais seguros durante o expediente, enquanto estiver manuseando e ao final do dia de trabalho.
V. Cabe à Coagru adotar e manter Inventário de Dados e/ou Ativos de Informações, bem como os normativos internos relacionados.
VI. Cabe à Coagru estabelecer condições para transferência segura de informações a partes externas, prevendo responsabilidades aos usuários que exercerem atividades de tratamento de dados pessoais, observando os seguintes processos:
    - Controle e notificação de transmissões de dados pessoais;
    - Procedimentos para assegurar a rastreabilidade dos eventos e o não-repúdio;
    - Normas para identificação de portadores;
    - Notificação e registro de incidentes de segurança da informação, como perda de dados;
    - Utilização de um sistema acordado de identificação para informações críticas e sensíveis, garantindo que a informação esteja devidamente protegida.

7.1.8 Guarda de Informações Digitais (Backup) e Documentação Física

I. Rotinas sistemáticas de backup e guarda de informações devem ser realizadas por colaboradores da Departamento de Tecnologia da Informação da Coagru.
II. Cópias dos dados de produção, backup local e backup off-site, devem ser produzidas aplicando-se as melhores práticas de mercado com relação à segurança e proteção de dados.
III. Documentos imprescindíveis para as atividades da Coagru deverão ser salvos em drives de rede corporativa, viabilizando a produção de backup e guarda da informação.
IV. Documentações Físicas devem ser guardadas/arquivadas de forma segura, quer seja em ambiente interno ou externo, de acordo com os prazos previstos em lei para guarda e arquivamento de referidos documentos.
V. As cópias de segurança devem ser armazenadas em uma localidade remota, a uma distância suficiente para escapar dos danos de um eventual desastre ocorrido no local principal, bem como as mídias de backup devem ser regularmente testadas para garantir que sejam confiáveis no caso do uso emergencial.

7.1.9 Instalação de Programas (Softwares)

I. Os softwares instalados e utilizados nos equipamentos da Coagru e externos, devem ser legalmente adquiridos e/ou autorizados pela Departamento de Tecnologia da Informação, mesmo que supostamente de livre uso, como aqueles usualmente classificados como “freeware”, “shareware”, “demoware”, sendo todos utilizados somente dentro do seu período de validade de licenciamento.
II. A Departamento de Tecnologia da Informação deverá realizar a gestão dos softwares instalados nas estações de trabalho e servidores da Coagru, mantendo o devido registro das licenças disponíveis.
III. O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização deste na segurança da informação da Coagru e o suporte para o mesmo.
IV. É vedado efetuar réplicas dos softwares adquiridos pela Coagru, bem como promover esta prática com outros programas.

V. É vedado utilizar softwares que, por algum motivo, descaracterizem os propósitos da Coagru ou danifiquem de alguma forma o ambiente instalado.
VI. A Departamento de Tecnologia da Informação poderá remover programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa norma.
VII. O usuário deverá manter a configuração do equipamento disponibilizada pela Coagru, seguindo os devidos controles de segurança exigidos por esta PSIPD, pelas normas específicas da Coagru, assumindo a responsabilidade como custodiante de informações.

7.1.10 Antivírus

I. Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente de forma automática pela Departamento de Tecnologia da Informação.
II. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar imediatamente a Departamento de Tecnologia da Informação.
III. O usuário não pode, em hipótese alguma, desabilitar o programa de antivírus instalado no computador.
IV. Todo arquivo proveniente do ambiente externo (internet, e-mail, pen-drive, etc.), deverá ser verificado pelo antivírus, antes de ser aberto.
V. É proibida a instalação de outros sistemas de antivírus, que não sejam os fornecidos pela Departamento de Tecnologia da Informação.

7.1.11 Datacenter

I. O ambiente do Datacenter é de acesso restrito, visto que abriga equipamentos computacionais e guarda de dados pessoais e institucionais, em funcionamento ininterrupto.
II. Situações emergenciais que venham a ocorrer no extra horário, finais de semana e feriados deverão ser comunicados a Departamento de Tecnologia da Informação imediatamente.
III. O Datacenter deve contar com proteção física contra perturbações da ordem pública, desastres naturais ou causados pelo homem. Os equipamentos devem ser protegidos contra falta e oscilações de energia elétrica e outras interrupções.
IV. Todo acesso físico ao ambiente do Data Center deve ser controlado e monitorado.
V. Somente será permitido acesso de pessoas externas ao ambiente do Datacenter por ocasião de manutenções preventivas ou corretivas, desde que acompanhadas por colaborador da Departamento de Tecnologia da Informação.

7.1.12 Dispositivos de Impressão, Cópia e Digitalização

I. Todos os ativos de informação devem ser devidamente guardados, especialmente documentos em papel ou mídias removíveis da Coagru. Documentos não devem ser abandonados após a sua cópia, impressão ou utilização. Ao usar uma impressora coletiva, o usuário deverá recolher o documento impresso imediatamente.
II. As impressoras e seus respectivos suprimentos são de uso exclusivo para as atividades da Coagru.

III. Os usuários devem recolher imediatamente suas impressões, sejam elas corretas ou impressões com falhas. No caso de impressões com falhas, deverão ser descartados de forma adequada.
IV. Impressões com falhas contendo informações sigilosas devem ser inutilizadas tornando-as ilegíveis.

7.2 GESTÃO DE OUTROS RECURSOS DE INFORMAÇÃO

7.2.1 Estação de Trabalho

I. Nenhuma informação confidencial deve ser deixada à vista, seja em papel ou em quaisquer dispositivos, eletrônicos ou não, devendo ser adequadamente armazenadas em local provido com chaves/fechaduras.
II. No caso dos computadores, notebooks ou similares, os mesmos devem ficar bloqueados, mesmo quando o usuário se ausentar por curto período de tempo, assim como os dispositivos móveis, quando necessário, devem ser guardados em local provido com chaves/fechaduras.
III. Os usuários devem devolver todos os ativos de informação da organização que estejam em sua posse, após o encerramento de suas atividades, do respectivo contrato ou acordo.
IV. No caso de baixas patrimoniais ou uso do próprio equipamento pessoal pelo colaborador, deverão ser adotados procedimentos para assegurar que toda a informação relevante seja transferida para a organização e que seja apagada de forma segura do equipamento.

7.2.2 Controle de Acesso Físico

I. Todos os colaboradores da Coagru que transitem por ambientes administrativos, devem possuir identificação pessoal visível por crachás.

7.2.3 Serviços Postais e de Envelopes Vai e Vem

I. Os serviços de correspondências e malotes da Coagru, estão disponíveis aos colaboradores, estagiários, dirigentes e prestadores de serviços, na proporção das respectivas autorizações pessoais de uso e deverão atender, exclusivamente, às finalidades e os objetivos da Coagru, respeitando as medidas técnicas para proteger os dados pessoais.

7.2.4 Riscos de Segurança da Informação

I. A Coagru compromete-se a adotar e manter processo contínuo de Gestão de Riscos de Segurança da Informação.
II. Os processos de segurança da informação deverão ser revistos periodicamente pela Comissão de Segurança da Informação e Proteção de Dados da Coagru, com a participação da Departamento de Tecnologia da Informação, a fim de aperfeiçoar e agir proativamente contra riscos advindos de novas tecnologias e ameaças, objetivando a constante elaboração de planos de ação apropriados para a proteção dos seus ativos de informação.

8 REVISÃO

A Comissão de Segurança da Informação e Proteção de Dados da Coagru, deverá, de ofício, avaliar a necessidade de se revisar esta política, ao menos uma vez por ano, expressando seu entendimento e sugestões no relatório de prestação de contas anual à Diretoria Executiva.

9 TERMO DE CIÊNCIA

O Termo de Aceite à PSIPD, deve ser assinado por todos os empregados e estagiários, devendo passar a constar, inclusive, como documento do processo de admissão ou de adaptação.

Os usuários devem entender os riscos associados ao aceite à PSIPD da Coagru e cumprir rigorosamente o que está previsto neste documento.

Nos contratos em que se fizer necessário a concessão de acesso a ativos de informação da Coagru, o aceite à PSIPD da Coagru será condição imprescindível para que o tal acesso seja concedido, o que será instrumentalizado por intermédio de Termo de Aceite à PSIPD, contendo cláusula de Confidencialidade das informações.

10 GLOSSÁRIO E LISTA DE SIGLAS

Os principais termos e siglas citados nesta Política incluem:

Ativo	Qualquer recurso físico ou digital que tenha valor para a Coagru.
Ativos de Informação	Podem ser tangíveis ou intangíveis. Ativos intangíveis são ativos físicos, como documentos em papel, servidores, discos rígidos, laptops, profissionais qualificados, dentre outros. Já os ativos intangíveis, são os ativos não físicos, como dados armazenados em computadores e banco de dados, arquivos de dados, informações pessoais, arquivos de áudio, imagens e vídeos digitalizados, dentre outros.
Backup	Cópia de segurança, na qual são armazenados dados e informações importantes isoladamente do ambiente de produção, para recuperação futura no caso de algum problema, necessidade ou sinistro. É uma fotografia do ambiente na linha do tempo. *Backup local: armazenado nas instalações da Coagru. *Backup off-site: armazenado em instalações externas à Coagru, como por organizações terceiras em ambiente físico e/ou em nuvem.
CLT	Consolidação das Leis do Trabalho.
Comissão de Segurança da Informação e Proteção de Dados	Grupo multifuncional, responsável por gerenciar as políticas e padrões que apoiam a todos na proteção dos ativos de informação na Coagru, além de auxiliar na resolução de problemas relacionados ao tema e divulgação do conteúdo dessas políticas e padrões.
Cookies	Arquivos de texto baixados em seu dispositivo quando você visita um site. São úteis para gravar algumas preferências de acesso e para oferecer um serviço mais eficiente quando ocorrer um acesso posterior pelo titular.

Correio Eletrônico, e-mail, sistemas de mensageria	Plataformas digitais que permitem compor, enviar, receber e gerenciar mensagens por meio de sistemas eletrônicos de comunicação.
Datacenter	Ambiente no qual estão instalados servidores, equipamentos de rede como roteadores e switches, e equipamentos de armazenamento de dados.
Demoware	Versão de demonstração ou de teste, de determinado software.
Dispositivos de Impressão, Cópia, Digitalização e Gravação	Equipamentos contendo softwares que permitem reproduzir de forma idêntica, documentos físicos e/ou digitais, incluindo sons/voz, imagens e afins quando se aplica.
Dispositivos Móveis	Quaisquer equipamentos eletrônicos portáteis para processamento de dados, armazenamento e comunicação, tais como: notebooks, tablets, smartphones, consoles portáteis, câmeras fotográficas e similares.
Estação de Trabalho	Local destinado ao colaborador para a execução de suas atividades laborais e contempla, além de todos os mobiliários, os equipamentos e materiais de expediente necessários para a execução das atividades de forma organizada e segura.
Freeware	Software distribuído gratuitamente aos usuários.
Internet (Rede Mundial)	Várias redes de computadores interligados que utilizam um conjunto de protocolos próprios de comunicação, com o propósito de servir progressivamente o mundo inteiro, permitindo que usuários tenham acesso a vários conteúdos e informações, de outras redes corporativas e ou instituições, sendo estes conteúdos públicos, autênticos ou não.
Malware	Software malicioso projetado para se infiltrar em dispositivos sem o conhecimento do usuário, causando danos ao sistema ou comprometendo a segurança das informações.
PSIPD	Política de Segurança da Informação e Proteção de Dados.
Rede Corporativa	Sistema de transmissão de dados e informações entre equipamentos de uma mesma corporação, tais como computadores e similares, servidores de documentos e arquivos, impressoras, câmeras de vídeo, telefones, sistemas de videoconferência, web conferência e áudio conferência, podendo ou não possuir acesso à internet.
Redes e Mídias Sociais	Ecossistema composto por pessoas e/ou instituições que se conectam digitalmente por diferentes tipos de interesses, formando ou fortalecendo relações, e que compartilham valores, objetivos comuns e conteúdo de diferentes formatos, buscando uma identidade entre as partes, sendo as mídias sociais as plataformas onde esse compartilhamento ocorre.
Segurança da Informação	Esforços contínuos para a proteção dos ativos de informação, em todo o seu ciclo de vida.
Shareware	Software comercial distribuído gratuitamente aos usuários, seja em um formato limitado ou como uma avaliação, que expira após um determinado número de dias.
SPAM ou Lixo Eletrônico	E-mails não solicitados e/ou que podem conter malware.
Titular de dados	Pessoa natural a quem se referem os dados pessoais que são objeto das tratativas em questão.
Usuário(s)	Colaboradores, terceirizados, consultores, auditores, conselheiros, estagiários e visitantes que obtiveram autorização do responsável pela área interessada, de acesso e, quando pertinente, de tratamento dos ativos de informações, formalizada por meio de assinatura de um Termo de Compromisso, Sigilo e Confidencialidade.

VPN	"Virtual Private Network" (Rede Virtual Privada, em tradução livre). Trata-se de um mecanismo capaz de delimitar a comunicação entre celulares, computadores e outros aparelhos que têm acesso restrito à rede em questão, mediante uso das credenciais necessárias.
DADOS PESSOAIS	É considerado dado pessoal qualquer informação que permita identificar, direta ou indiretamente, uma pessoa que esteja viva, tais como: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial, localização via GPS, retrato em fotografia, prontuário de saúde, cartão bancário, renda, histórico de pagamentos, hábitos de consumo, preferências de lazer, dentre outros;
DADOS PESSOAIS SENSÍVEIS	Dados pessoais que revelem a origem racial ou étnica, opiniões políticas e convicções religiosas ou filosóficas, filiação sindical, dados genéticos, dados biométricos tratados simplesmente para identificar um ser humano, dados relacionados com a saúde, dados relativos à vida sexual ou orientação sexual da pessoa.

EQUIPE TÉCNICA

Anderson Sanchez

Edilson Ferreira

Gilberto Dias Martins

Giovane Candido Kubaski

Mario Sérgio Bedeu