1.0 Objetivo

Definir os processos da política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, bem como a conduta dos colaboradores aos recursos tecnológicos disponibilizados aos seus colaboradores.

2.0 Alcance

Este documento aplica-se a CooperJohnson.

3.0 Definições

3.1 Segurança da Informação

A Segurança da Informação deve proteger a informação como um todo, quer seja físico ou digital. Na verdade, precisa proteger tecnologia, procedimento e pessoas sendo contínua e visando sempre a confidencialidade, integridade e a disponibilidade.

3.2 Segurança Cibernética

Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado em resumo preocupa-se com a parte digital.

3.3 Segurança Sigilosa

É qualquer informação ou conhecimento que sua divulgação possa resultar em uma perda no nível de segurança ou financeiro ou moral para a cooperativa, caso revelada (divulgada) a terceiros impactando seus colaboradores ou associados.

3.4 Informação Privilegiada

Entende-se por Informação Privilegiada qualquer informação que não tenha sido autorizada a ser divulgada ao público externo.

4.0 Responsabilidades

4.1 Diretoria e Superintendência: Aprovação da política.

4.2 Diretor Administrativo: Responsável pela política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes.

4.3 TI Infraestrutura e Negócios: Responsáveis pela capacitação do time, pelos testes e o cumprimento da Política de Segurança da Cibernética;

4.4 Estrutura Organizacional: Verificar aderência desta política na prática.

5.0 Diretrizes

5.1 Campo de aplicação

O cumprimento da Política de Conduta dos Processos de Segurança da Informação, Segurança Cibernética é de responsabilidade de todos os conselheiros, diretores, gestores, colaboradores e prestadores de serviços da cooperativa, os quais devem obedecer às seguintes diretrizes:

5.1.1 Proteger as informações contra acesso, modificações, destruição ou divulgação não autorizada;

5.1.2 Prover a adequada classificação da informação, sob os critérios de confidencialidade, disponibilidade e integridade;

5.1.3 Assegurar que os recursos utilizados para o desempenho de sua função sejam utilizados apenas para as finalidades aprovadas pela gestão da cooperativa;

5.1.4 Garantir que os sistemas e as informações sob sua responsabilidade estejam adequadamente protegidos;

5.1.5 Garantir a continuidade do processamento das informações críticas de negócios;

5.1.6 Selecionar os mecanismos de segurança da informação, balanceando fatores de riscos, tecnologia e custo;

5.1.7 Comunicar imediatamente o departamento de TI ou seu gestor imediato, quaisquer descumprimentos da Política Segurança da Informação, Segurança Cibernética.

5.2 Objetivo

5.2.1 A definição de diretrizes para a segurança do espaço cibernético, relacionadas à capacidade da cooperativa de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético;

5.2.2 A proteção das informações sob responsabilidade da cooperativa preservando sua confidencialidade, integridade, disponibilidade e autenticidade;

5.2.3 A prevenção de eventual interrupção, total ou parcial, dos serviços de TI acessados pela cooperativa e pelos cooperados e, no caso de sua ocorrência, a redução dos impactos dela resultantes;

5.2.4 O tratamento e prevenção de incidentes de segurança cibernética.

5.3 Introdução

A Política de Segurança Cibernética foi criada com a finalidade de servir como guia prático de conduta profissional a todos os seus colaboradores visando o compromisso formal da Gestão da cooperativa em relação a Segurança da Informação e Cibernética.

E, em razão da responsabilidade das atividades desenvolvidas pela cooperativa com seus associados, que está sujeita a um rigoroso controle de suas operações e fiscalizado pelo conselho fiscal, auditorias, controles internos e atender a Resolução 4.658 do Banco Central é dever de todos os colaboradores informar a respeito de inconsistências em procedimentos e práticas definidas nesta política, com a finalidade de zelar pelo cumprimento das regras aqui expostas.

5.4 Segurança Cibernética

5.4.1 Para reduzir a vulnerabilidade da instituição a incidentes cibernéticos e atender aos demais objetivos de segurança cibernética, a cooperativa adota procedimento e controle ou que sejam relevantes para a condução das atividades, conforme porte e perfil de risco, tais como:

5.4.1.1 Regras para controlar complexidade e qualidade das credenciais utilizadas para acesso aos sistemas e aos dados sob responsabilidade da cooperativa;

5.4.1.2 Critério de autenticação nos ambientes em que o recurso está disponível;

5.4.1.3 Recursos criptográficos adequados para garantir a privacidade, integridade e não-repúdio dos dados mantidos pela cooperativa;

5.4.1.4 Solução de prevenção e detecção de intrusão, solução de proteção de dispositivos, monitoramento de tráfego na rede, monitoramento de atividades em bancos de dados, monitoramento de atividade de usuários privilegiados;

5.4.1.5 Testes de invasão realizados por equipe interna e por empresa contratada e processo de gestão de vulnerabilidades de ativos de TI;

5.4.1.6 Solução de proteção contra ameaças em e-mail e no acesso a sites na internet, solução de proteção de dispositivos, antivírus;

5.4.1.7 Gerenciador de eventos e incidentes em segurança que mantém registro dos eventos do ambiente, permitindo a rastreabilidade de vários tipos de ocorrências;

5.4.1.8 Segmentação de rede, com isolamento de ambientes (como produção e homologação) e áreas;

5.4.1.9 Manutenção de cópias de segurança dos dados (local e cloud) e das informações.

5.4.2 As informações de propriedade ou sob custódia da cooperativa, mantidas em meio eletrônico ou físico, são classificadas de acordo com os requisitos de proteção esperados em termos de sigilo, valor, requisitos legais, sensibilidade e necessidades do negócio, de modo que busquem assegurar a

confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informações utilizados.

São adotados mecanismos para disseminação da cultura de segurança cibernética na instituição, incluindo:

5.4.3 Implementação de programas de capacitação e de avaliação periódica de colaboradores;

5.4.4 Prestação de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros.

Para manter o processo de Segurança Cibernética a cooperativa possui quatro pilares:

5.4.5 Identificação e avaliação de riscos;

5.4.6 Ações de prevenção e proteção;

5.4.7 Monitoramento e testes;

5.4.8 Plano de ação;

5.4.9 Identificação e avaliação de riscos.

5.4.10 A cooperativa deverá avaliar e identificar os seguintes Riscos Cibernéticos no qual está sujeita:

5.4.10.1 Malwares: software que causa danos a máquina, rede, softwares e banco de dados;

5.4.10.2 Cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;

5.4.10.3 Spyware: software malicioso para coletar e monitorar o uso de informações;

5.4.10.4 Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido;

5.4.10.5 Fraudes Externas e invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico;

5.4.10.6 Ataques DDoS e Botnets: Ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviço.

5.4.11 Ações de prevenção e proteção

5.4.11.1 Treinamento e Divulgação da Política

Todos os colaboradores deverão ter conhecimento desta política, ser capacitado para a compreensão dela, assinar os termos que constituem esta política e anexar em seu dossiê no RH.

5.4.11.2 Senhas e Acessos

5.4.11.2.1 Seguir o item desta política 5.6.2 Conduta para Gestão de Acessos de Informação e a Outros Ambientes Lógicos que adota regras para concessão de senhas de acesso aos sistemas e servidor de dados;

5.4.11.2.2 As senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados e criptografados.

5.4.11.3 Equipamentos e Sistemas

5.4.11.3.1 Sempre que incluir novos equipamentos na rede o departamento de TI deverá garantir que sejam feitas configurações seguras de seus recursos;

5.4.11.3.2 Sempre que o departamento de TI adquirir um novo sistema deverá ser feito testes em ambiente de homologação e de prova de conceito antes do envio à produção;

5.4.11.3.3 A cooperativa conta com recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais. Da mesma maneira monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas;

5.4.11.3.4 As empresas fornecedoras deverão identificar por escrito todos os processos e ações que efetuam para os sistemas que controlam da cooperativa, bem como comprovar sua eficácia. Este processo deverá ser concluído no máximo até 31/12 do ano vigente.

5.4.11.4 Processo de backup

5.4.11.4.1 Processo de Backup Servidor de Dados:

5.4.11.4.2 O Backup do servidor é diário, uma vez por dia, no final da tarde, de forma automática, incremental

(backup somente dos arquivos que sofreram alteração) de duas formas: local (onde ficam armazenados em um disco externo e em nuvem. Ressaltamos que o Backup se encontra num provedor apto as normas da Resolução 4.658 e encontra-se na região conforme capítulo III seção 16.

5.4.11.5 Processo de Sistemas de Dados:

Os backups dos sistemas ERP da cooperativa, Atendimento ONLINE e Aplicativos (IOS e ANDROID) estão sob a responsabilidade do fornecedor efetuar o Backup. Neste caso cabe o departamento de TI solicitar mensalmente a restauração do backup no ambiente de homologação.

5.4.11.6 Abertura de chamados para a Equipe de TI

5.4.11.6.1 Todos os problemas relacionados à TI são comunicados diretamente ao departamento de TI, via telefone ou e-mail, onde estes problemas são averiguados por ordem de chamado;

5.4.11.6.2 A TI tem a responsabilidade de retornar com uma solução ao colaborador na seguinte ordem:

5.4.11.6.2.1 Alta: Um dia para retorno para definir a solução;

5.4.11.6.2.2 Média: Dois dias para definir a solução;

5.4.11.6.2.3 Baixa: Três dias para definir a solução.

5.4.11.7 Contratação de serviços em Nuvem

5.4.11.7.1 Certificar se a há a existência de um acordo para a troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços estão sendo prestados;

5.4.11.7.2 A fornecedora deverá garantir com ferramentas e processos que a prestação dos serviços não cause danos à operação regular da instituição, nem as obrigações que a cooperativa tenha com o Banco Central do Brasil;

5.4.11.7.3 A cooperativa deve dar preferência que os serviços fiquem locados nos EUA ou Brasil;

5.4.11.7.4 Deverá ter no contrato com o Fornecedor uma cláusula de confidencialidade de informações.

5.4.12 Monitoramento e testes

5.4.12.1 Monitoramento das Informações/Equipamentos

A cooperativa em seus treinamentos a colaboradores e/ou integrações a novos colaboradores deverá conscientizar que todas as ações, sistemas, serviços, dados, informações disponíveis não devem ser interpretadas como sendo de uso pessoal, portanto, todos devem ter ciência de que o uso está sujeito à monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pelo departamento de TI, gestores ou por prestador de serviços externo.

5.4.12.2 Testes para Novas Versões de Sistema

5.4.12.2.1 Todos os testes deverão ser feitos em um ambiente de homologação;

5.4.12.2.2 O departamento de TI deverá gerar um relatório comprovando a Eficácia da atualização;

5.4.12.2.3 Deverá participar dos testes além do departamento de TI um colaborador responsável pelo processo para que o mesmo seja validado;

5.4.12.2.4 O gestor ou o departamento de TI deverá treinar os responsáveis e preencher a Lista de Presença/Eficácia desta política.

5.4.12.3 Testes Segurança Informação e Equipamentos

5.4.12.3.1 A cooperativa deverá ter um roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade;

5.4.12.3.2 A cooperativa deverá manter inventários atualizados de hardware e software atualizados, bem como os sistemas operacionais e softwares de uso atualizados;

5.4.12.3.3 A cooperativa realiza testes de segurança no seu sistema de segurança da informação e proteção de dados, dentre as medidas, incluem-se:

5.4.12.3.4 Verificação dos logs dos colaboradores;

5.4.12.3.5 Alteração periódica de senha de acesso dos Colaboradores;

5.4.12.3.6 Segregação de acessos;

5.4.12.3.7 Manutenção bimestral de todo os hardwares;

5.4.12.3.8 A cooperativa deverá solicitar para os fornecedores testes e eficácia dos processos utilizados para evitar e revelar as principais vulnerabilidades dos sistemas que estão sob a responsabilidades deles, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real;

5.4.12.3.9 Os fornecedores relevantes deverão apresentar na forma descrita o Plano de Contingência e Continuidade de Negócios da cooperativa, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

5.4.13 Plano de ação

5.4.13.1 Os eventos ou incidentes de segurança cibernética deverão ser comunicados ao departamento de TI por e-mail, para tomar as devidas providências;

5.4.13.2 São executados anualmente testes de Continuidade de Negócio a contar da construção e efetivação desta política, considerando cenários de indisponibilidade causada por incidentes cibernéticos;

5.4.13.3 Os empregados e prestadores de serviço terceirizados são orientados e instruídos sobre o comportamento correto de não tomar nenhuma ação própria, mas informar imediatamente o evento ou incidente ao departamento de TI, responsável pelo tratamento;

5.4.13.4 Existe processo disciplinar formal estabelecido para lidar com empregados, fornecedores ou profissionais terceirizados que cometam violações de segurança da informação;

5.4.13.5 Existe orientação formal para que os empregados, fornecedores e profissionais terceirizados notifiquem o departamento de TI qualquer observação ou suspeita de fragilidade tempestivamente, de forma a prevenir incidentes de segurança cibernética;

5.4.13.6 Os contratos firmados com empresas terceirizadas que suportam atividades críticas devem dispor de cláusula informando que elas precisam disponibilizar Plano de Continuidade de Negócios, bem como evidência de realização de testes deste plano.

5.4.13.7 Referente aos Sistemas da cooperativa sob a responsabilidade de Terceiros:

5.4.13.7.1 Havendo indícios ou de suspeita fundamentada os colaboradores deverão comunicar o departamento de TI que imediatamente deve acionar o fornecedor responsável para realizar os procedimentos necessários de modo a identificar o evento ocorrido;

5.4.13.7.2 O fornecedor deverá esclarecer por escrito o ocorrido qual o plano de ação que foi tomado e os danos causados;

5.4.13.7.3 Na hipótese de vazamento de informações sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível;

5.4.13.7.4 Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado;

5.4.13.7.5 Referente a sistemas da cooperativa atendimento online ou aplicativo;

5.4.13.7.6 Em caso de suspeita de necessidade de fraude na solicitação de empréstimos via Sistema ONLINE o colaborador deverá;

5.4.13.7.7 Impedir o cooperado de efetuar empréstimos ONLINE;

5.4.13.7.8 Trocar sua senha de acesso;

5.4.13.7.9 Relatar no cadastro do cooperado o fato que as atualizações deste cooperado deverão ser feitas pessoalmente no posto de atendimento até a verificação e validação do processo;

5.4.13.7.10 Relatório do Plano de Ação e de Resposta;

5.4.13.7.11 É elaborado relatório anual sobre a implementação do Plano de Ação e de Resposta a Incidentes de acordo com o anexo I, com data-base de 31 de dezembro, contemplando;

5.4.13.7.12 A efetividade da implementação das ações desenvolvidas pela cooperativa para adequação das

estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética;

5.4.13.7.13 O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes;

5.4.13.7.14 Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

5.4.13.7.15 Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes cibernéticos.

5.4.13.7.16 O relatório anual sobre a implementação do plano de ação e de resposta a incidentes é submetido ao comitê de risco, quando existente, e apresentado ao conselho de administração, ou, na sua inexistência, à diretoria até 31 de março do ano seguinte ao da data-base.

5.4.13.7.17 No caso de não incidência será efetuado o registro em ata de reunião de diretoria não sendo necessário a elaboração do relatório de plano de ação e de resposta.

5.4.14 Sobre contrações de terceiros

5.4.14.1 A contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, devem adotar procedimentos que contemplem:

5.4.14.1.1 A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado, aos riscos a que estejam expostas e a verificação da capacidade do potencial prestador de serviço de assegurar;

5.4.14.1.2 O cumprimento da legislação e da regulamentação em vigor;

5.4.14.1.3 A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço.

5.4.14.1.4 A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço.

5.5 Divulgação da Política

A política de segurança cibernética deve ser divulgada aos colaboradores e às empresas prestadoras de serviços a terceiros.

A cooperativa deve divulgar ao público um resumo contendo as linhas gerais da política de segurança cibernética através de seu site institucional.

5.6 Segurança da Informação

5.6.1 Processo de Conduta Pessoal

5.6.1.1 Independentemente do meio ou da forma em que as Informações da CooeprJohnson, sigilosas ou não, podem ser encontradas seja em dependências ou servidor de dados ou sistemas da CooperJohnson, estas fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamentos seguro e consistente, com destaque para os seguintes itens:

5.6.1.1.1 Os Colaboradores devem assumir atitude proativa e engajada no que diz respeito à proteção das Informações Sigilosas;

5.6.1.1.2 Os Colaboradores devem compreender as ameaças externas que podem afetar a segurança das Informações Sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, gravações telefônicas, etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;

5.6.1.1.3 Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da CooperJohnson;

5.6.1.1.4 Documentos impressos e arquivos contendo Informações Sigilosas ou não devem ser adequadamente armazenados e protegidos, sendo vedada a retirada dos ambientes da CooperJohnson sem a autorização de seu Gestor imediato.

5.6.2 Todo colaborador da CooperJohnson é responsável pela exatidão das informações contidas nos relatórios pelos quais é responsável. É dever dos colaboradores repassar aos gestores ou clientes internos, imediatamente após

o recebimento, todas e quaisquer correspondências enviadas pelos órgãos fiscalizadores:

5.6.2.1 Os colaboradores devem zelar pela confidencialidade de quaisquer informações a que tiverem acesso, que tenham obtido ou tomado conhecimento em função das atividades que desempenham ou desempenharam para a CooperJohnson, por prazo indeterminado;

5.6.2.2 Não deve ser transmitida nenhuma informação relativa a operações em andamento ou não concretizadas, ou informações recebidas de pessoas que sejam especialistas nos mercados que atuam na CooperJohnson;

5.6.2.3 Todos os papéis e documentação digital relacionados a CooperJohnson e seus associados/fornecedores deverão ser mantidos em local seguro, de modo a minimizar o risco de que pessoas não autorizadas venham a ter acesso a informações confidenciais;

5.6.2.4 Os colaboradores não estão autorizados a discutir informações confidenciais em locais públicos ou através de um telefone celular ou viva-voz;

5.6.2.5 De acordo com a legislação brasileira, a divulgação de informações confidenciais ou privilegiadas causando danos a outrem, constitui crimes especificados nos artigos 153, 154 do Código Penal e artigo 12 da Lei 7.492/86;

5.6.2.6 É vedado aos colaboradores qualquer tipo de operação ou serviço no mercado que atua a CooperJohnson que seja realizada de posse de informação privilegiada para seu uso próprio;

5.6.2.7 Os colaboradores que detiverem qualquer informação privilegiada obtida no exercício de suas atividades estão estritamente proibidos de divulgá-las a pessoas não relacionadas às suas atividades da CooperJohnson;

5.6.2.8 Os Colaboradores devem bloquear seus computadores sempre que se ausentarem de suas estações de trabalho;

5.6.2.9 Toda informação em papel não deve ser jogada em lixo. Esta deve ser destruída.

5.6.3 Conduta para Gestão de Acessos de Informação e a Outros Ambientes Lógicos

Senhas:

5.6.3.1 As senhas de acessos dos Colaboradores aos sistemas da CooperJohnson são pessoais e intransferíveis, não podendo ser

compartilhadas, divulgadas a terceiros (inclusive a outros Colaboradores);

5.6.3.2 As senhas não poderão ser anotadas em papel ou em sistema visível ou de acesso não protegido;

5.6.3.3 Todo colaborador após sua contratação receberá do RH suas senhas para acesso aos Sistemas da CooperJohnson, E-mail. Será obrigação do Colaborador efetuar imediatamente a troca destas senhas por uma senha forte composta de números, letras e caracteres especiais. Logo após efetuar este processo caberá a Equipe de TI validar e verificar se as senhas foram corretamente trocadas;

5.6.3.4 É extremamente proibido a todo colaborador salvar senhas em sistemas, servidor e e-mail para facilitar seu acesso;

5.6.3.5 Os sistemas de Controles e ERP da CooperJohnson deverão ter um controle de expiração de senha parametrizado para expirar as senhas. Caso algum sistema não tenha esta finalidade terá que efetuar uma customização até o dia 30/06/2022;

5.6.3.6 A base de dados de senhas deve ser armazenada com criptografia;

5.6.3.7 O usuário poderá solicitar alteração de sua senha, caso não se recorde da mesma, mediante solicitação formal;

5.6.3.8 Todo colaborador deve obrigatoriamente sair do sistema (efetuar LOGOFF) corretamente não deixando seu usuário aberto (logado) no servidor ou no ambiente de nuvem.

5.6.4 Acesso Rede e a Sistemas da CooperJohnson

5.6.4.1 O acesso a rede, as Informações Sigilosas e aos sistemas da CooperJohnson somente será permitido mediante autorização do Gestor, e desde que seja estritamente necessário para o desempenho das funções do Colaborador. O Colaborador será corresponsável pela segurança do acesso remoto aos sistemas e Informações Sigilosas da CooperJohnson;

5.6.4.2 Os colaboradores da equipe de TI, para o desempenho de suas atribuições, poderão ter permissão de acesso a todos os recursos computacionais da CooperJohnson necessários inclusive a máquinas dos demais colaboradores;

5.6.4.3 Os serviços de acesso devem ser cancelados sob as seguintes condições:

5.6.4.3.1 Finalização do período especificado na solicitação ou contrato;

5.6.4.3.2 Perda da necessidade de utilização do serviço;

5.6.4.3.3 Identificação de vulnerabilidade, risco ou uso indevido no acesso concedido.

5.6.4.4 As conexões à rede da CooperJohnson devem ocorrer da seguinte maneira:

5.6.4.4.1 Utilização de autenticação;

5.6.4.4.2 As senhas e as informações que trafegam entre a estação remota e a rede da CooperJohnson devem estar criptografadas;

5.6.4.4.3 Cada usuário deve manter suas credenciais de acesso (login e senha) em sigilo absoluto e não o fornecer a outra pessoa, não deixar gravada a informação da senha, garantindo assim, a impossibilidade de acesso indevido por pessoas não autorizadas;

5.6.4.4.4 É vedada a utilização do acesso para fins não relacionados às atividades da instituição.

5.6.5 Acesso dos Colaboradores no Sistema ONLINE ou Aplicativos:

5.6.5.1 Todo associado possui uma senha criptografada de acesso para o ambiente contendo suas informações de capital, empréstimos, serviços etc.;

5.6.5.2 Todo associado no momento de solicitar um serviço o sistema gerará uma nova senha exclusiva e randômica para aquele serviço. No qual o associado receberá a mesma via SMS/e-mail no qual deverá digitá-la no sistema para confirmar a solicitação;

5.6.5.3 O sistema registra LOG de todos os pedidos e ações do sistema.

5.7 Conduta para utilização da Internet

5.7.1 Os colaboradores deverão utilizar os recursos disponíveis de Internet apenas para assuntos corporativos;

5.7.2 A CooperJohnson possui um servidor de Internet na qual mantém o controle total das informações e sites acessados pelos seus colaboradores;

5.7.3 Os Gestores da CooperJohnson poderão a qualquer momento solicitar um relatório para a Equipe de TI para saber como está sendo utilizado os recursos de internet, a seu exclusivo critério, em casos específicos.

5.7.4 A CooperJohnson possui dois grupos de acesso para a Internet que deverá ser definido pelo seu Gestor:

5.7.4.1 Semi-restrito: Neste grupo o colaborador terá acesso igual ao Restrito incluindo sites de notícias e Redes Sociais;

5.7.4.2 Full: Acesso a todos os sites.

5.7.5 A responsabilidade de informar a Equipe de TI a qual Grupo de acesso o colaborador pertencerá é do Departamento de RH no momento de sua contratação;

5.7.6 Comprovada a utilização irregular, o usuário envolvido terá o seu acesso à Internet bloqueado pela Equipe de TI, sendo comunicado o fato ao seu Gestor, podendo incorrer em processo administrativo disciplinar e nas sanções legalmente previstas, assegurados o contraditório e a ampla defesa.

5.8 Conduta para utilização de e-mail (correio eletrônico)

5.8.1 Os colaboradores deverão utilizar os recursos disponíveis de serviço de e-mail apenas para assuntos corporativos;

5.8.2 Os Gestores da CooperJohnson poderão acessar os e-mails enviados e recebidos pelos Colaboradores, a seu exclusivo critério, em casos específicos. As informações envolvidas constituem em propriedade exclusiva da CooperJohnson, cabendo à mesma as decisões acerca de sua comercialização, reprodução e utilização.

5.8.3 O acesso indevido às informações tramitadas por meio de e-mail corporativo da CooperJohnson, ou contidas em seus ambientes, será punido na forma da lei;

5.8.4 É vedado ao usuário o uso do serviço de e-mail da CooperJohnson com o objetivo de:

5.8.4.1 Praticar crimes e infrações de qualquer natureza;

5.8.4.2 Executar ações nocivas contra outros recursos computacionais da CooperJohnson ou de redes externas;

5.8.4.3 Distribuir material obsceno, pornográfico, ofensivo, preconceituoso, discriminatório, ou de qualquer forma contrário à lei e aos bons costumes;

5.8.4.4 Disseminar anúncios publicitários, mensagens de entretenimento e mensagens do tipo “corrente”, vírus ou qualquer outro tipo de programa de computador que não seja destinado ao desempenho

de suas funções ou que possam ser considerados nocivos ao ambiente de rede da CooperJohnson;

5.8.4.5 Emitir comunicados gerais com caráter eminentemente associativo, sindical ou político-partidário;

5.8.4.6 Enviar arquivos de áudio, vídeo ou animações, salvo os que tenham relação com as funções institucionais desempenhadas pela CooperJohnson;

5.8.4.7 Divulgar, no todo ou em parte, os endereços eletrônicos corporativos constantes do catálogo de endereços do serviço;

5.8.4.8 Executar outras atividades lesivas, tendentes a comprometer a intimidade de usuários, a segurança e a disponibilidade do sistema, ou a imagem institucional;

5.8.4.9 Se o colaborador precisar enviar uma mesma mensagem para vários usuários, como exemplo serviços de divulgação de produtos, cobrança etc. deverá comunicar a Equipe de TI ou MKT para utilizar a ferramenta de envio de e-mail MKT;

5.8.4.10 Todo e-mail enviado pelo colaborador deverá ter a assinatura digital conforme criado e estabelecida pelo Departamento de Comunicação e Marketing.

5.9 Conduta para utilização dos sistemas de informática

5.9.1 Os colaboradores deverão utilizar os softwares para desenvolvimento de Aplicativos e Sistemas ou Softwares adquiridos pela CooperJohnson ou documentos (planilha, documentos textos etc.), apenas para assuntos corporativos. Os Gestores da CooperJohnson poderão acessar o conteúdo das informações, a seu exclusivo critério, em casos específicos. Os sistemas desenvolvidos, em desenvolvimento ou que venham a ser elaborados pelos colaboradores constituem propriedade exclusiva da CooperJohnson, cabendo à mesma as decisões acerca de sua comercialização, reprodução e utilização;

5.9.2 É vedada a cópia, venda, uso ou distribuição de informações, software e outras formas de propriedade intelectual, sem o consentimento prévio e por escrito de no mínimo dois Diretores responsáveis pela CooperJohnson;

5.9.3 Os colaboradores deverão utilizar somente softwares homologados e previamente aprovados pelos Gestores para serem instalados e usados nas estações de trabalho, o que deve ser feito com exclusividade pela equipe de serviços de informática da Gestora;

5.9.4 Havendo a necessidade de utilização de software não homologado, o Gestor imediato deverá solicitar formalmente a Equipe de TI a homologação do mesmo contendo os seguintes itens:

5.9.4.1 Especificações detalhadas do software solicitado;

5.9.4.2 Quantidade de licenças;

5.9.4.3 Suporte ao software (necessidade de suporte);

5.9.4.4 Justificativa.

5.9.5 O processo de homologação de software deve avaliar, sobretudo, o impacto da utilização deste na segurança da informação da CooperJohnson e o suporte para ele;

5.9.6 A instalação e a utilização de software estão sujeitas ao cumprimento dos seguintes requisitos:

5.9.6.1 Quantidades de licenças de uso adquiridos;

5.9.6.2 Custo X Benefício;

5.9.6.3 Conformidade com a área de atuação do setor interessado;

5.9.6.4 Compatibilidade com os softwares utilizados;

5.9.6.5 Desempenho do ambiente computacional;

5.9.6.6 Impacto entre a necessidade de instalação e a demanda de outros setores;

5.9.6.7 A todos os Colaboradores é proibido utilizar softwares que, por algum motivo, descaracterizem os propósitos da CooperJohnson ou danifique de alguma forma o ambiente instalado, tais como jogos eletrônicos e outros, com exceção feita na Área Social da CooperJohnson devido suas particularidades;

5.9.6.8 A instalação de software de outras categorias, tais como freeware (software gratuito), de domínio público (não protegido por copyright) e/ou cópias de demonstração que não sofram ação de direitos autorais, deve ser previamente requerida, homologadas pela Equipe de TI;

5.9.6.9 A Equipe de TI deverá remover qualquer programa de computador instalado em estação de trabalho que não se enquadre nos critérios estabelecidos nessa política.

5.10 Condutas em relação aos Computadores e Notebooks da empresa

5.10.1 Todo colaborador é responsável pela proteção e conservação do patrimônio da CooperJohnson, no caso em questão os Computadores e Notebooks e que estejam sob sua responsabilidade;

5.10.2 Os computadores devem ser utilizados exclusivamente para fins profissionais;

5.10.3 Os Gestores da CooperJohnson poderão acessar os dados nas máquinas a seu exclusivo critério, em casos específicos;

5.10.4 Para os colaboradores que utilizam notebooks deverão deixá-los na CooperJohnson em períodos de férias ou afastamentos com exceção de uma autorização de seu Gestor;

5.10.5 A equipe de TI não é responsável por efetuar backup nas máquinas sendo total responsabilidade do colaborador. Qualquer informação (documento, planilha, relatórios) deve ser armazenada no servidor conforme detalhada nesta política;

5.10.6 Quando encerrar seu contrato com a CooperJohnson o colaborador deverá deixar seu Notebook com o responsável da Equipe de TI;

5.10.7 É vedado aos Colaboradores utilizarem equipamentos próprios nas instalações, bem como efetuar download de qualquer programa;

5.10.8 Todo colaborador deve ligar/desligar de forma adequada e segura o equipamento;

5.10.9 Todo colaborador ao deparar com um Computador ou Impressora desligada da corrente elétrica antes de ligá-la deve comunicar imediatamente a Equipe de TI para verificar voltagem correta;

5.10.10 Todos os computadores e notebooks da CooperJohnson deverão possuir o programa de antivírus homologado pela Equipe de TI;

5.10.11 Todo colaborador deve obrigatoriamente executar o antivírus nos dispositivos removíveis antes de sua abertura quando inseridos na estação de trabalho.

5.10.12 Todo colaborador que possuir notebook deve obrigatoriamente assinar o Termo de Responsabilidade pela guarda e uso do Equipamento.

5.11 Condutas em relação a Impressoras

5.11.1 Somente os colaboradores poderão ter acesso aos recursos de impressão;

5.11.2 A configuração da impressora nos Equipamentos da CooperJohnson deverá ser realizada ou orientada pela Equipe da TI;

5.11.3 Todo colaborador não deve deixar informações sigilosas ou sensíveis da instituição nas impressoras, de tal forma que pessoas não autorizadas possam obter acesso a elas;

5.11.4 Todo colaborador sempre que possível deve utilizar o recurso de impressão frente e verso.

5.12 Condutas em Relação ao Servidor de Dados

5.12.1 A CooperJohnson manterá um servidor de dados nas dependências de sua sede;

5.12.2 Este servidor deverá ficar os documentos (planilhas, textos, políticas, normas) da CooperJohnson;

5.12.3 Seus dados ficarão divididos por departamento sendo proibida a criação de pastas pessoais ou com nome de colaboradores;

5.12.4 Na pasta “Area de Transferência” deve ser utilizada para arquivos temporários sendo que sua limpeza será diária e não haverá backup dela;

5.12.5 As permissões de acesso deverão ser concedidas conforme determinação de seu Gestor mediante solicitação formal;

5.12.6 É proibida a exposição de material de natureza pornográfica, racista, etc., armazenado, distribuído, editado ou gravado através do uso dos recursos computacionais da rede;

5.12.7 Não é permitido criar ou remover arquivos fora da área alocada ao usuário ou que venham a comprometer o desempenho e funcionamento dos sistemas;

5.12.8 É vedada a gravação de dados e informações de natureza particular. Se esta for encontrada será apagada imediatamente pela Equipe de TI;

5.12.9 É obrigatório armazenar os arquivos inerentes ao serviço de cada setor em suas respectivas pastas para garantir o backup dos mesmos.

5.13 Condutas em Relação à Rede CooperJohnson

5.13.1 Rede Sede CooperJohnson

5.13.1.1 Os Racks com o servidor de Dados e Internet (Firewall) e switches deverão estar numa sala fechada, onde terão acesso somente pessoas acompanhadas de um responsável pela a Equipe de TI, com a refrigeração compatível com a necessidade dos equipamentos;

5.13.1.2 As portas dos switches somente devem estar ativas se utilizadas e inventariadas;

5.13.1.3 Os switches e access points devem possuir controle de acesso;

5.13.1.4 Todos os equipamentos só podem ser instalados na rede da CooperJohnson após a sua adequação aos padrões de segurança definidos pela CooperJohnson;

5.13.1.5 Os ativos de rede somente devem ser liberados para uso após a efetiva homologação, realizada em ambiente apropriado, distinto do ambiente de produção, e devidamente documentado;

5.13.1.6 As intervenções no ambiente de rede somente serão permitidas mediante supervisão pela Equipe de TI;

5.13.1.7 Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede ou conta, pois todo o equipamento (computador, notebook, celular ou impressora) deve ser previamente cadastrado no Firewall da CooperJohnson pela Equipe de TI com suas permissões e liberado sua porta nos switches;

5.13.1.8 A CooperJohnson reserva o direito de realizar investigações em qualquer dos equipamentos que integrem a sua rede local;

5.14 Condutas acesso a Rede WiFi:

5.14.1 A CooperJohnson possui duas redes Wifi distintas em sua sede: Uma Coorporativa e outra para visitantes/eventos.

5.14.1.1 Rede WIFI Coorporativa segue os mesmos padrões da rede física;

5.14.1.2 Rede WIFI Visitantes/Eventos: Para seguir os padrões de segurança tanto de dados, como criminal o sinal de WIFI será liberado pela Equipe de TI mediante solicitação formal com as senhas e prazo de validade. O responsável pelo evento deverá cadastrar as pessoas que receberam a senha com Nome, CPF e e-mail.

5.15 Condutas em relação ao uso de telefones e celulares coorporativos

5.15.1 Os colaboradores deverão utilizar os recursos telefônicos, apenas para assuntos corporativos;

5.15.2 Detectando abusos de ligações particulares fica autorizado os Gestores a descontarem os valores das ligações em folha de pagamento de seu Colaborador;

5.15.3 Todo colaborador deve atender ou “puxar” uma ligação no Terceiro toque;

5.15.4 Os Colaboradores que utilizam celulares corporativos deverão assinar um termo de recebimento.

6.0 Referências

6.1 Internas

6.1.1 Termo de Responsabilidade pela guarda e uso do Equipamento de Trabalho disponível no diretório: Termo de Responsabilidade pela guarda e uso do Equipamento de Trabalho.

6.2 Externas

6.2.1 Resolução Nº 4.658 - Banco Central do Brasil;

6.2.2 Lei n. 7.492 – Planalto

7.0 Anexos

7.1 Relatório – Pano de Ação e de Resposta a Incidentes

RELATÓRIO - PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

PERIODO	xx/xx/xxxx a xx/xx/xxxx
DATA DA EMISSÃO	xx/xx/xxxx

CONTEÚDO DO RELATÓRIO

Incidente	Plano de ação	Resultado Obtido	Testes

São José dos Campos, xx, xxxxxxx, xxxx

*****FIM DO DOCUMENTO*****

Histórico de Revisão do Documento			
N° da Versão	**Seção**	**Descrição da mudança**	**Justificativa da Mudança**
4.0	5.10.12	Inclusão assinatura termo	Complemento de informação
	6.1.1	Inclusão diretório do termo	
HISTÓRICO ANTERIOR ENCONTRA-SE NA VERSÃO: 3.0_10/2022			

ELABORADORES	CARGO
JOSÉ D. GUILHEME NETO	Especialista de TI Infraestrutura
PAULO LAVEZO	Gerente de Negócios

APROVADORES	CARGO
FLÁVIO A. S. MARQUES	Diretor Presidente
FABYANO SOUSA MELLO	Diretor Administrativo
EDVALDO NOBILE	Diretor Operacional
IVO LARA RODRIGUES	Superintendente