FINALIDADE

Estabelecer conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão da GPAtiva. Definir os princípios fundamentais que formam a base da Política de Segurança Cibernética e da Informação, norteando a elaboração de normas, processos, padrões e procedimentos.

ÁREAS ENVOLVIDAS / RESPONSABILIDADES

Todo Colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações da GPAtiva e deve cumprir as determinações da Política, normas e padrões de segurança da informação.

Administração (Conselho de Administração e Diretoria Executiva)

Responsável por:

- Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação.
- Prover comprometimento e apoio à aderência a Política de Segurança Cibernética e da Informação de acordo com os objetivos e estratégias de negócio estabelecidas para a Cooperativa;
- Fornecer à área de Segurança da Informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário.

Todos os Colaboradores

Responsáveis por:

- Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI;
- Notificar a área de Segurança da Informação do GPA sobre as violações da Política de Segurança Cibernética e da Informação e sobre os incidentes de segurança que venha a tomar conhecimento;
- Manter o sigilo das informações que tenha obtido acesso enquanto Colaborador da GPAtiva, mesmo após seu desligamento da Cooperativa.

Gerente Adm/Financeiro (Controles Internos / Riscos / PLD-FT)

Responsável por:

- Apoiar e incentivar o estabelecimento da Política de Segurança Cibernética e da Informação na GPAtiva;

- Garantir que todos os colaboradores e fornecedores tenham acesso e conhecimento desta Política e demais normas e padrões de segurança da informação;
- Fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações da GPAtiva;
- Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de todas as equipes;
- Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;
- Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem o Código de Conduta Moral, a Política de Segurança Cibernética e da Informação e as normas do GPA e da GPAtiva;
- Autorizar acessos de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de *need to know* e *least privilege*.
- Apoiar a área de segurança da informação e Tecnologia do GPA na execução de suas devidas responsabilidades, disseminação de conteúdos focados em segurança da informação, políticas e códigos de conduta e ética.

Área de Segurança da Informação do GPA

Responsável por:

- Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;
- Desenvolver e estabelecer programas de conscientização e divulgação da Política de Segurança Cibernética e da Informação;
- Conduzir o processo de Gestão de Riscos de Segurança da Informação;
- Conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
- Conduzir os processos de monitoração e segurança da informação;
- Definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;
- Propor projetos e iniciativas para melhoria do nível de segurança das informações do GPA e GPAtiva.

Área Tecnologia da Informação (TI) do GPA

Responsável por:

- Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;

- Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
- Conduzir a gestão dos acessos a sistemas e informações do GPA e GPAtiva;
- Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
- Informar imediatamente a área de Segurança de Informação do GPA, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos do GPA e GPAtiva;
- Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;
- Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio.
- Garantir que todos os ativos críticos de Tecnologia da Informação devem ser instalados em ambientes especializados conhecidos como Datacenters. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.

Recursos Humanos

Responsável por:

- Verificar o histórico de candidatos a emprego, de acordo com a ética e leis vigentes;
- Garantir que a Política, Normas e Procedimentos da Política de Segurança Cibernética e da Informação sejam divulgados no processo de admissão/integração de novos Colaboradores.

Área Jurídica do GPA

Responsável por:

- Apoiar a aplicação de medidas disciplinares referente a violações da Política de Segurança Cibernética e da Informação;
- Identificar requisitos legais pertinentes à segurança da informação;
- Garantir a adoção de clausulas pertinente à segurança das informações nos contratos estabelecidos com o GPA e a GPAtiva.

Segurança Patrimonial do GPA

Responsável por:

- Monitorar o acesso físico de Colaboradores às instalações do GPA e GPAtiva;
- Administrar o controle de acesso físico.

Fornecedores e Parceiros de Negócios

Responsável por:

- Cumprir as determinações da Política, Normas e Procedimentos publicados pelo GPA e GPAtiva;
- Orientar os funcionários da empresa sobre o cumprimento das determinações da Política, Normas e Procedimentos publicados pelo GPA e GPAtiva;
- Cumprir com o acordo de confidencialidade.

CONCEITOS / CRITÉRIOS GERAIS

A informação é um ativo essencial para os negócios de uma organização e sendo assim deve ser adequadamente protegida. Isto é especialmente importante em um ambiente de negócios cada vez mais interconectado.

Segurança cibernética e da informação é a proteção das informações contra diversos tipos de ameaças, para minimizar a exposição da Cooperativa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade. Isso significa proteger a Cooperativa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e da marca da Cooperativa.

A GPAtiva, através do departamento de Segurança da Informação do GPA e de forma alinhada com os objetivos e requisitos do negócio, estabelece nesta Política de Segurança Cibernética e da Informação, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da GPAtiva, de seus cooperados, fornecedores e parceiros de negócios.

1. CONCEITOS

Para efeito deste documento, aplicam-se os seguintes termos e definições:

1.1. Recursos

Qualquer recurso, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade da GPAtiva, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

1.2. Ameaça

Qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

1.3. Boas Práticas de Segurança da Informação

São consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC 31000, OWASP (www.owasp.org), NIST (www.nist.gov), ISACA (www.isaca.com.br), SANS (www.sans.org) e outras internacionalmente reconhecidas.

1.4. Colaborador

Entende-se como Colaborador qualquer pessoa que trabalhe para a GPAtiva, quer seja: Funcionário com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou trainee.

1.5. Controle

Qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros.

1.6. Gestor

Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção.

1.7. Informação

Qualquer conjunto organizado de dados que possua algum propósito e valor para a GPAtiva, seus cooperados, parceiros e colaboradores. A informação pode ser de propriedade da Cooperativa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem.

1.8. Princípios de “Least Privilege” e “Need to Know”

Estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know).

1.9. Política de Segurança Cibernética e da Informação

Estrutura de documentos formada pela Política, normas e padrões de segurança cibernética e segurança da informação.

1.10. Risco

Qualquer evento que possa afetar a capacidade da Cooperativa de atingir seus objetivos e sua estratégia de negócios ou, conforme a ISO 31000, o efeito da incerteza nos objetivos.

1.11. Segurança da Informação (SI)

Segurança da Informação é a proteção das informações, sendo caracterizada pela preservação de:

- **Confidencialidade:** garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;
- **Integridade:** garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade.
- **Disponibilidade:** garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;
- **Conformidade:** Garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

1.12. Segurança Cibernética

Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital.

1.13. Recursos Críticos

Recursos essenciais para o funcionamento da operação da GPAtiva e que possuem informações críticas ou sensíveis.

1.14. Baselines

Requisitos, recomendações e melhores práticas de configurações de segurança da informação para os ativos.

1.15. Nuvem (Cloud)

Infraestrutura, plataforma, aplicação ou serviço localizado na internet. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e parte irrestrita.

1.16. IoT (Internet of Things – Internet das coisas)

Conexão de dispositivos eletrônicos, como aparelhos eletrodomésticos, eletro portáteis, máquinas industriais, meios de transporte, dentre outros utilizados no dia-a-dia à internet.

2. CRITÉRIOS GERAIS

2.1. Aquisição, Desenvolvimento e Manutenção de Tecnologia da Informação.

Aquisições, desenvolvimento, contratações e a manutenções de Tecnologia da Informação devem ser centralizadas e gerenciadas pela área de Tecnologia da Informação do GPA.

Responsáveis pela aquisição de produtos ou serviços de Tecnologia da Informação, assim como o desenvolvimento e manutenção de ativos tecnológicos, devem:

- Garantir a adoção e manutenção dos requisitos previamente definidos nos baselines, padrões e normas de segurança da informação;
- Garantir o envolvimento da área de Segurança da Informação na análise crítica de novas soluções ou para aquelas que sofreram alterações significativas;
- Garantir o atendimento aos requisitos de segurança necessários para assegurar a confidencialidade, integridade, disponibilidade e conformidade de sistemas e informações.
- Garantir que novas soluções sejam devidamente documentadas, assim como mantida documentação para entendimento e rastreabilidade das ações realizadas.

Os Recursos de Tecnologia da Informação utilizados pela GPAtiva devem ser inventariados, controlados e colocados à disposição de acordo com as regras de acesso vigentes e boas práticas de segurança da informação.

Na contratação de serviços, os contratos firmados entre as partes e a GPAtiva devem conter cláusulas de confidencialidade, responsabilidade pela proteção da informação, não divulgação e descarte das informações. Outras cláusulas específicas de Segurança da Informação podem ser requeridas de acordo com o contexto do serviço contratado.

O sigilo necessário com as informações da GPAtiva deve perdurar mesmo após o encerramento da prestação de serviços. Este ponto deve ser previsto no estabelecimento de contratos.

A veracidade das informações contidas em contratos deve ser verificada.

Devem ser seguidas as boas práticas de segurança da informação no ciclo de desenvolvimento de sistemas da empresa.

2.2. Classificação da Informação

As informações devem ser atribuídas a um proprietário formalmente designado.

Toda a informação deve ser classificada, de acordo com seu valor, grau de sigilo, criticidade e sensibilidade perante o negócio, de forma que sejam adotados os mecanismos de proteção adequados, balanceando custo e complexidade do controle.

As informações "legadas" não rotuladas devem ser consideradas por todos como uma Informação com rótulo 'INTERNO', ou seja, com o nível intermediário de classificação da Informação, até o momento de sua reclassificação, não sendo permitido o repasse para qualquer pessoa que não seja pertencente a GPAtiva ou ao GPA. As Informações já existentes a GPAtiva ou GPA e que não estão classificadas, deverão ser classificadas conforme forem sendo utilizadas, sendo que caberá aos gestores responsáveis pelas Informações garantir a sua classificação.

Todos os Colaboradores devem tratar as informações da GPAtiva de acordo com seu nível de classificação de forma a protegê-las contra atos ou acessos indevidos ou divulgação não autorizada, mantendo sua confidencialidade, integridade e disponibilidade.

As classificações e complexidade da Informação estão na Política de Classificação da GPAtiva.

2.3. Comportamento Seguro

Os recursos e as informações de propriedade ou sob custódia da GPAtiva devem ser utilizados de acordo com os interesses da organização, para prestação dos seus serviços, atendendo aos requisitos e respeitando as regras estabelecidas.

Independente dos meios onde a informação esteja armazenada, ou seja, transmitida, cada Colaborador deve assumir um comportamento seguro e proativo impedindo seu vazamento para pessoas ou meios externos da GPAtiva.

O Código de Ética do GPA e o Código de Ética e Conduta Profissional da GPAtiva também detalham aspectos de um comportamento seguro e deve ser de conhecimento de todos os colaboradores.

Aos Colaboradores, sem autorização prévia, é vetado emitir opiniões em nome da GPAtiva ou utilizar informações privadas da GPAtiva em: e-mails, sites, redes sociais, publicações impressas, fóruns de discussão, serviços da Internet e outros ambientes públicos, em face da possibilidade de divulgação inadvertida.

O uso da marca, nome ou citação de qualquer empresa do GPA e da própria Cooperativa deve cumprir os requisitos de autorização por direito de imagem e propriedade.

Os colaboradores são responsáveis por manter as informações da GPAtiva em locais seguros. Isso se aplica a informações impressas, escritas em quadros ou em outras mídias físicas, que não devem ser deixadas desprotegidas em salas de reuniões, mesas ou qualquer local dentro e fora da Cooperativa ou empresas do GPA.

O descarte de informações internas, restritas ou confidenciais, contidas em qualquer meio, quer seja impresso, eletrônico, magnético, ou sob qualquer outra forma, deve ser feito de forma segura, garantindo a destruição dos dados de forma que não possam ser novamente recuperados.

O uso de recursos tecnológicos para gravação, foto e filmagem de qualquer reunião ou evento corporativo não é permitido sem prévia autorização e consentimento de todos os participantes.

2.4. Conformidade

O cumprimento e aderência às leis, regulamentações, Política de Segurança Cibernética e da Informação, normas, obrigações contratuais, Código de Conduta Moral e padrões de segurança, são obrigatórios e devem ser garantidos por todos os Colaboradores da GPAtiva.

Responsáveis por recursos críticos da GPAtiva devem garantir a retenção de evidências da execução de seus controles para fornecimento em casos de auditorias ou necessidade do atendimento a regulamentações.

2.5. Conscientização e Divulgação de Segurança Cibernética e da Informação

A Política de Segurança Cibernética e da Informação, normas e padrões de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos Colaboradores, tanto pelas equipes de Recursos Humanos quanto pelos Gestores.

Programas de conscientização, divulgação e reciclagem do conhecimento da Política de Segurança Cibernética e da Informação devem ser estabelecidos e praticados regularmente para garantir que todos os Colaboradores e terceiros conheçam as diretrizes e responsabilidades relacionadas à segurança das informações.

2.6. Continuidade de Negócios

Deve-se estabelecer, documentar, implantar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para os serviços e processos de negócio da GPAtiva, durante situações adversas. O modelo a ser adotado para a Gestão de Continuidade de Negócios deverá ser baseado na Norma ISO 22301.

2.7. Segurança Física

O acesso físico à sede da GPAtiva deve ser permitido apenas a colaboradores ou visitantes que estejam portando crachá em local visível, sendo controlado por catracas ou outros dispositivos de controle eletrônico de acesso. Na ausência de controles automatizados o responsável pela área deve garantir que o controle seja realizado de forma pessoal através da verificação do porte de crachás por colaboradores e visitantes. Nenhum visitante tem a autorização de circular pelas dependências da Cia sem estar acompanhado por um colaborador GPAtiva.

A identificação e registro de pessoas e equipamentos são obrigatórios, seguindo o procedimento definido pela área de Segurança Patrimonial do GPA.

As recepções e áreas de maior criticidade devem estar sob proteção de um circuito interno de câmeras de vídeo, instaladas em locais estratégicos. Nas referidas áreas haverá sinalização informando sobre o uso de câmeras de vídeo. As imagens obtidas devem ser preservadas com segurança.

2.8. Acesso Lógico

O processo de gestão dos acessos a qualquer sistema da GPAtiva quer seja interno ou em nuvem, deve ser conduzido pelo departamento de Gestão de Acessos do GPA, exceções deverão ser tratadas junto ao departamento de Segurança da Informação do GPA.

O acesso a qualquer sistema tecnológico da GPAtiva deve ser autenticado, ou seja, protegido por credenciais de acesso, certificados, tokens ou qualquer outro método seguro de identificação e autenticação.

Acessos a informações e a sistemas da GPAtiva devem ser permitidos apenas após dois ou mais níveis de autorização, sendo o primeiro do gestor do colaborador solicitante e o segundo do responsável pela informação ou sistema.

Os acessos de colaboradores e terceiros devem ser desativados assim que desligados ou encerrados contratos de prestação de serviços.

As credenciais de acesso a sistemas e informações, compostas por usuário e senha, são concedidas pela GPAtiva aos Colaboradores e Terceiros para uso em atividades relacionadas a seu trabalho, pelo tempo em que perdurar seu vínculo com a Cooperativa.

É proibido transferir, compartilhar, emprestar ou revelar a senha das credenciais de acesso concedidas pela Cia ou GPAtiva a outros colaboradores, assim como é proibido o uso de credenciais de outros colaboradores.

Todos os perfis de usuários e acessos a informações ou sistemas de média e alta criticidade devem ser revisados periodicamente pelo respectivo responsável, seguindo os critérios de segregação da função e observando o princípio de mínimo acesso (least privilege) e necessidade de conhecimento (need to know).

2.9. Gestão de risco de Segurança da Informação

A Gestão de Riscos de Segurança da Informação deve ser realizada através de um processo estruturado que contemple a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoração dos riscos que podem afetar negativamente os negócios da organização e da Cooperativa.

O processo de gestão de riscos deve contemplar novos ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros.

2.10. Incidentes de Segurança da Informação

São considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de SI: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio em risco.

Violações ou tentativas de violação desta Política, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

Colaboradores devem informar imediatamente à segurança da informação todas as violações à Política de segurança da informação, normas, padrões incidentes ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

A identificação de incidentes de segurança pode ocasionar o bloqueio imediato dos acessos dos colaboradores envolvidos até que sejam concluídas as investigações necessárias.

2.11. Monitoração

Todas as ações de colaboradores e visitantes, realizadas nas dependências da GPAtiva ou remotamente, abrangendo o acesso físico e a utilização de recursos de tecnologia da informação e comunicação do grupo, podem ser monitoradas.

A área de Segurança da Informação do GPA é responsável por garantir a privacidade dos registros oriundos da monitoração do acesso e uso de sistemas e serviços de Tecnologia da Informação.

Ao acessarem sistemas e recursos tecnológicos da GPAtiva, Colaboradores e visitantes concordam que suas ações podem ser monitoradas.

Os registros obtidos através de monitoramento poderão ser utilizados em processos de investigação de incidentes e suspeitas de violação de leis e de Normas do Grupo e da GPAtiva, bem como, em processos judiciais e trabalhistas, a critério da GPAtiva.

A Cooperativa deverá elaborar, anualmente, relatório de implementação do plano de ação e de respostas a incidentes, com data base 31 de dezembro.

2.12. Privacidade

Deve-se assegurar a privacidade e a proteção, conforme previsto pela legislação e regulamentação pertinente, todas as informações pessoais de cooperados, colaboradores, parceiros de negócio e outras que venham a ser armazenadas, processadas ou colocadas sob custódia da GPAtiva.

2.13. Propriedade Intelectual

A GPAtiva é proprietária ou custodiante responsável por toda a informação criada, armazenada, transmitida, transportada, processada ou descartada pelos seus recursos ou por aqueles contratados pela Cooperativa em nuvem ou prestados por terceiros devidamente autorizados.

É vetada aos Colaboradores a violação da propriedade intelectual do grupo ou de terceiros, quer seja por meio da utilização indevida de imagens, textos, softwares, marcas ou pela cópia indevida de originais ou conversão do formato destes.

2.14. Utilização de Recursos de Tecnologia da Informação

Para utilização de qualquer recurso de tecnologia da informação é necessária à aprovação prévia do gestor do colaborador/terceiro e do proprietário da informação, sistema ou recurso. Casos onde Segurança da Informação do GPA identificar que possa colocar em risco as informações do grupo, deverá ser analisado e tratado.

Não é permitida aos Colaboradores e Terceiros a instalação de qualquer software ou a alteração de parâmetros de configuração de computadores da GPAtiva. Estas devem ser realizadas por equipes de TI autorizadas, após processos de homologação e obtenção do licenciamento adequado. Softwares instalados indevidamente poderão ser automaticamente excluídos, sem prévio aviso.

É proibido o armazenamento, transmissão, processamento e impressão de conteúdo que contenha pedofilia, pornografia, erotismo, violência, terrorismo, racismo, intolerância, e outros conteúdos proibidos por leis, moral, ética e normas do GPA.

As informações internas, restritas e confidenciais ou sensíveis da GPAtiva não devem ser copiadas, sincronizadas ou replicadas em serviços em nuvem, exceto situações analisadas e aprovadas por SI.

É proibido o uso de computadores de propriedade do colaborador, nas sedes ou em lojas, para atividades profissionais da GPAtiva.

Informações da GPAtiva ou sob sua custódia e responsabilidade, não devem ser transportadas ou processadas em qualquer meio ou serviço pessoal, a exemplo e-mail, Internet, pendrive, redes sociais, CD/DVD, papel, computador dentre outros meios.

O acesso de celulares, smartphones, tablets e qualquer outro dispositivo a serviços e informações da GPAtiva deve ser permitido apenas após o atendimento integral dos requisitos de segurança da GPAtiva definidos nas normas para esta categoria de dispositivos.

Documentos eletrônicos de uso da GPAtiva devem ser armazenados em repositórios centralizados da rede (servidores de arquivos) com as devidas proteções de segurança, dentre elas: controle de acesso e backup. Documentos eletrônicos do grupo não devem ser armazenados em estações de trabalho.

Os colaboradores devem zelar pela segurança de ativos da empresa colocados sob sua responsabilidade, como dispositivos móveis e notebooks.

O uso de recursos de criptografia deve ser autorizado pelo departamento de Segurança da Informação do GPA e estar de acordo com os padrões definidos para o GPA.

2.15. Segurança em Redes

Devem existir controles tecnológicos para proteger o acesso entre redes (incluindo Internet, redes públicas, extranets, acesso remoto, wireless e as diferentes redes de usuários).

Equipamentos com diferentes requerimentos de segurança devem ser segregados em redes diferentes.

Além do controle de acesso entre as redes, deve ser protegida a informação em trânsito, seguindo os requerimentos da Classificação da Informação.

O acesso remoto somente será permitido para situações onde for indispensável e esteja documentado e com mecanismos de autenticação de dois fatores.

Os níveis de segurança (confidencialidade, integridade e disponibilidade) esperados dos serviços de comunicações, devem ser estabelecidos nos contratos firmados com os fornecedores desses serviços.

Deve ser implementado controle tecnológico de Firewall para a proteção das redes mais críticas.

Controles criptográficos devem ser solicitados, estabelecidos e/ou desenvolvidos, para garantir os níveis de confidencialidade das informações trafegadas, segundo a sua classificação (definido pelo proprietário da informação).

2.16. Registros de Auditoria

Todas as ações de usuários, sistemas e qualquer evento de Segurança da Informação devem gerar trilhas de auditoria (logs), que deverão ser mantidos por um período mínimo de 5 anos, em local centralizado e protegido contra acessos não autorizados.

Não deve haver nenhuma modificação na integridade das trilhas de auditoria (logs), ou seja, não pode haver usuários com permissão de alteração.

Todo acesso de consulta, cópia ou tentativa de modificação e exclusão as trilhas de auditoria (logs) devem ser registradas.

As falhas nos registros das trilhas de auditoria (logs) devem ser registradas, analisadas e devem ser tomadas providencias para corrigir o erro de forma imediata.

2.17. Backups, arquivamento e restaurações

A área de TI deve determinar os recursos requeridos para cumprir com os requerimentos mínimos de respaldo dos ativos de informação, conforme definido pelos proprietários da informação.

A área de TI deverá estabelecer um plano de backup para cumprir com esses requisitos e deverá estabelecer mecanismos para a correta execução das rotinas de backup.

Diariamente devem ser validados os resultados da realização dos backups, sendo que as falhas deverão ser reportadas como incidente de segurança.

O processo de backup e restauração para todos os sistemas deve ser testados em intervalos regulares, com o objetivo de assegurar que estejam em conformidade com os requerimentos dos donos da informação e com as exigências do plano de continuidade do negócio do GPA e Cooperativa.

O tempo necessário que a informação deve ser mantida deverá estar de acordo com as necessidades do negócio e deve levar em consideração as exigências das leis vigentes.

2.18. Análise de Vulnerabilidades Técnicas

Periodicamente devem ser realizados testes de vulnerabilidades técnicas dos equipamentos críticos da infraestrutura.

Após os levantamentos, as comparações e identificações dos riscos devem ser executadas, possibilitando o tratamento dos riscos de acordo com seus níveis.

Nos casos em que não for possível a eliminação total da vulnerabilidade, deve ser apresentada aceitação do risco ou a determinação de falso positivo.

Verificações ou auditorias regulares devem verificar a conformidade com as exigências técnicas dos sistemas e das redes.

As auditorias realizadas por terceiros devem identificar claramente as interações com os sistemas em operação.

As auditorias técnicas dos sistemas e das redes devem respeitar as práticas estabelecidas e devem ser realizadas de acordo com as recomendações da organização. Estas auditorias devem ser realizadas por fornecedores reconhecidos e competentes.

2.19. Prevenção, Detecção de Intrusão

Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS.

Sempre que o IDS / IPS detecta ou responde a uma tentativa externa mal-intencionada suficientemente grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada e procedimento de resposta deve ser acionado.

2.20. Proteção contra códigos maliciosos

Deverão ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.

Deve ser verificada a atualização das ferramentas de proteção baseadas em assinaturas, para que estejam nas últimas atualizações disponíveis.

2.21. Controles Criptográficos

Deverão ser utilizados controles criptográficos para proteger as informações segundo os requerimentos da sua classificação.

Somente algoritmos de criptografia aprovados pela área de Segurança da Informação do GPA podem ser utilizados nas soluções e sistemas adotados pela GPAtiva.

O gerenciamento das chaves de criptografia deve prever mecanismos para o armazenamento seguro, geração segura da chave e destruição da chave.

Deverá existir um mecanismo de recuperação da informação caso seja perdida uma chave de criptografia.

As chaves de criptografia devem ser trocadas periodicamente, dependendo da sua frequência de utilização.

Caso seja comprometida uma chave criptográfica, deve ser revogada imediatamente. Se for uma chave para criptografia de arquivos, deve ser trocada.

Mecanismos de autenticação e auditoria devem ser estabelecidos para garantir a segurança do acesso às chaves.

2.22. Aquisição e Desenvolvimento Seguro de Sistemas

Sistemas da informação desenvolvidos ou adquiridos devem contar com atributos e funcionalidades de segurança que protejam adequadamente as informações. Os requerimentos devem ser identificados e documentados na fase de concepção do sistema, para assegurar que as demandas de segurança sejam atendidas.

Deve haver controles que previnam erros de operação, perda, ou vazamento de informações. Todo sistema deve ser documentado, tornando sua implantação e operação independente de conhecimentos informais.

Devem ser estabelecidos controles criptográficos para proteger a confidencialidade, autenticidade ou integridade das informações. Faz-se necessária a documentação do uso de chaves, quando necessário.

Sistemas devem ser protegidos contra alteração indevida, evitando a exposição de dados sensíveis. Devem ser estabelecidos controles para monitorar e corrigir as vulnerabilidades e falhas desses.

2.23. Serviço de Nuvem

A possibilidade de utilização de uma solução de hospedagem externa, e, mais especificamente, uma solução 'cloud computing', depende do nível de sensibilidade dos dados e os processos em questão. Esta escolha deve ser feita com base em uma análise de risco.

Toda e qualquer contratação ou alteração contratual de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá comunicada ao Banco Central do Brasil conforme os seguintes critérios:

i. Quando da existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços serão prestados, a comunicação deverá ser realizada até dez dias após a contratação dos serviços ou alteração contratual.

ii. Quando da inexistência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços serão prestados, a GPAtiva deverá solicitar autorização do Banco Central do Brasil, sendo que a comunicação deverá ser realizada no prazo mínimo de sessenta dias antes da contratação ou alteração contratual.

Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles software como serviço (SaaS) ou armazenamento de base de dados devem possuir acesso seguro através de interfaces HTTPS bem como a autenticação segura e em ambientes segregados.

Os acessos devem ser controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada colaborador/terceiro ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

2.24. Gestão de Incidentes de Segurança

Qualquer evento relacionado a um suposto ou comprovado ataque a segurança de um sistema operacional deve ser resolvido de acordo com um processo de gerenciamento de incidentes.

Os procedimentos envolvidos devem descrever o processo de gerenciamento de incidente, o processo de investigação e o processo de recolhimento de provas. O processo de gerenciamento de incidente deve:

- Permitir a detecção, o mais cedo possível, e a capacidade de responder com a máxima eficácia para limitar os danos causados pelo incidente;
- Limitar as zonas de vulnerabilidade pela remediação de anomalias identificadas em algum ou todos os sistemas operacionais potencialmente afetados;
- Reter informações relevantes para posteriores investigações e coleta de provas;
- Compilar um registro de incidentes de segurança e estatísticas para uso na previsão de possíveis incidentes futuros;
- Identificar pontos de contato apropriados para o nível de severidade do ataque

Uma vez que um incidente mal-intencionado for resolvido, uma análise deve ser feita para identificar a origem do ataque e iniciar procedimentos administrativos ou judiciais apropriados.

2.25. Contratação e Gestão de Fornecedores

Todo serviço de TI deve ser classificado com base em uma análise de risco para se definir a sua criticidade e, assim se avaliar a possibilidade de sua prestação por uma empresa terceira.

Serviços críticos deverão sempre requerer uma homologação prévia do fornecedor, para garantir riscos mínimos com relação a sua prestação no que se refere a segurança e privacidade de dados.

Estabelecer em contrato requisitos mínimos de segurança e privacidade de dados que devem ser cumpridos pelo prestador de serviço.

A intervalos regulares os requisitos de segurança e privacidade de dados de fornecedores críticos devem ser verificados conforme definidos nas cláusulas contratuais estabelecidas entre as partes.

O gerenciamento de fornecedores deverá considerar a avaliação de risco e classificação dos fornecedores (estratégico, tático, operacional).

A intervalos regulares o desempenho dos fornecedores críticos deve ser medido quanto ao cumprimento das metas acordadas e os resultados avaliados. Os resultados devem ser discutidos com o fornecedor para se identificar as necessidades e oportunidades de melhoria.

Cada fornecedor deverá ter um gestor designado que acompanha o seu desempenho, tornando-o responsável pela qualidade dos serviços fornecidos.

2.26. Atualizações desta e demais políticas

Esta Política está sujeita a revisões anuais, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos da organização.

Esta e demais políticas passarão pelo seguinte procedimento de elaboração e revisão:

- Gestor responsável pela alteração solicitada e/ou inclusão de novo procedimento na política;
- Revisão pelo gerente de riscos e compliance, caso pertinente; e
- Avaliação e aprovação da Administração (Conselho de Administração e Diretoria Executiva).

A versão atualizada desta Política será publicada na rede interna da Cooperativa e deverá ser lida por todos os colaboradores.

Além dessa política, a Cooperativa também deve seguir as políticas vinculadas ao programa de governança em privacidade do GPA, conforme listagem abaixo. Esse processo é relevante levando em consideração que a GPAtiva fica dentro da rede do GPA. E o GPA pode atualizar as políticas listadas sempre que necessário, devendo a cooperativa sempre se manter atualizada em relação aos conteúdos:

Governança Privacidade:

- Políticas de Governança de dados;
- Política de retenção e descarte dos dados;
    - Anexo I retenção e descarte de dados pessoais;
    - Anexo II retenção e descarte de dados pessoais;
- Política de privacidade colaboradores;
- Política de privacidade;

Políticas de SI:

- Utilização Aceitável de Recursos Tecnológicos
- Política de Classificação da Informação;
- Política de Segurança de Banco de Dados;
- Política de Aquisição e Desenvolvimento Seguro de Sistemas;
- Política de Segurança Cibernética e da Informação;
- Política de Gestão de Incidentes de Segurança da Informação;
- Gerenciamento de Mudanças de TI

2.27. Aplicabilidade

O Gestor imediato ou o departamento de Segurança da Informação do GPA devem ser consultados sempre que existir alguma dúvida referente à aplicabilidade da Política de Segurança Cibernética e da Informação e demais documentos que a compõe.

Cabe à área de Segurança da Informação do GPA avaliar os riscos de ações não previstas na Política de Segurança Cibernética e da Informação, se necessário levando o assunto para a deliberação do Comitê de Segurança do GPA.

Exceções às diretrizes contidas neste documento e nos demais que compõem a Política de Segurança Cibernética e da Informação devem ser autorizadas pelo departamento de Segurança da Informação do GPA e Administração (Conselho de Administração e Diretoria Executiva) da Cooperativa.

SANÇÕES / PENALIDADES

O Colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração ao Gestor direto ou Canal de Ouvidoria do GPA. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares baseadas na Política de Gestão do Comitê de Ética, Código de Ética GPA e na Política de Consequências e Sanções Disciplinares.

Observação

No caso de Colaboradores terceiros, pode ser solicitada às suas respectivas empresas a troca da equipe alocada na GPAtiva, ou ainda, podem ser aplicadas penalidades a empresa tais como, multas, cancelamento do contrato e ações judiciais.

Disposições Finais

A presente Política tem por finalidade orientar a conduta dos Colaboradores que atuam para a Cooperativa.

Casos não contemplados nesta Política deverão ser comunicados à Administração (Conselho de Administração e Diretoria Executiva) que os apreciará e, caso necessário, fará a deliberação.

As propostas para alteração desta Política deverão ser elaboradas pela gerencia da Cooperativa e aprovadas pela Administração (Conselho de Administração e Diretoria Executiva).

Esta Política deverá ser objeto de avaliação anual pela Administração (Conselho de Administração e Diretoria Executiva) da Cooperativa.