POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

PROPÓSITO: Estabelecer os **princípios**, os **aspectos** e as **diretrizes** para a proteção de um dos principais ativos da Minutrade, a informação, prevenindo, detectando e reduzindo as vulnerabilidades relacionadas com o ambiente cibernético.	**PL-013**

Conteúdo

1. Índice de revisões

Versão	Data	Descrição	Autor	Verificador	Aprovador
1.0	03/02/2017	Criação do documento	Ricardo Moreira	Robson José Pinto Ferreira	Alexandre Bogliolo Sirihal
2.0	28/12/2018	Revisão anual do documento	Carine Alves de Carvalho	Robson José Pinto Ferreira	Alexandre Bogliolo Sirihal
3.0	30/12/2019	Revisão anual do documento	Carine Alves de Carvalho	Robson José Pinto Ferreira	Alexandre Bogliolo Sirihal
4.0	31/12/2020	Revisão do documento contemplando a segurança cibernética. Inclusão de diretrizes específicas para o tratamento de dados. Inclusão de responsabilidades do proprietário do ativo e do custodiante do ativo.	Carine Alves de Carvalho	Paulo Roberto Whyte	Robson José Pinto Ferreira

2. Abrangência

Esta política se aplica a todos os colaboradores e prestadores de serviços da Minutrade, devendo ser também considerada nas relações com clientes corporativos, aliados e fornecedores.

3. Vigência

Esta política deve ser analisada criticamente pelo Gestor de Segurança da Informação em conjunto com o Comitê Gestor de Segurança da Informação, pelo menos uma vez ao ano ou quando mudanças significativas ocorrerem.

4. Princípios e aspectos

Nosso compromisso com a proteção das informações da Minutrade e de nossos clientes e aliados está fundamentado nos seguintes princípios e aspectos:

- Confidencialidade: Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas

autorizadas; incluindo meios para garantir a privacidade e a proteção de informações proprietárias.

- Integridade: Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
- Disponibilidade: Toda informação deve estar disponível aos seus usuários de forma oportuna e confiável.
- Autenticidade: Toda informação trocada tem garantia da identidade de usuário ou sistema de informações com o qual se vai estabelecer comunicação (ser autêntico, ser quem diz ser).
- Conformidade: Toda informação deve cumprir obrigações empresariais com *stakeholders* e com aspectos legais e regulatórios relacionados à administração empresarial, dentro de princípios éticos e de conduta estabelecidos com a alta direção.

5. Conceitos

- Ativo: Qualquer coisa que tenha valor para a organização. Para a Minutrade, a informação é considerada um dos principais ativos, denominado ativo de informação.
- Ativo de informação: Qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. São exemplos de ativos de informação: bases de dados, documentações, equipamentos computacionais, infraestrutura, pessoas, reputação, locais físicos e softwares.
- Inventário de ativos de informação: Registro de identificação, localização e funcionalidade dos ativos de informação de valor relevante, para que a organização possa avaliar os controles de segurança adequados. Para a Minutrade, os ativos de informação mais relevantes devem ser inventariados como Itens de Configuração no BDGC.
- Controle de Segurança da Informação: Forma de gerenciar o risco, incluindo políticas, procedimentos, diretrizes, práticas ou estruturas organizacionais, que podem ser de natureza administrativa, técnica, de gestão ou legal. É um processo, política, dispositivo, prática ou outras ações que modifiquem o risco.
- Incidente de Segurança da Informação: evento único de Segurança da Informação ou uma série de eventos indesejados e inesperados que tem uma probabilidade significativa de comprometer as operações do negócio e ameaçam a Segurança da Informação.
- Perfil de acesso: É um conjunto de direitos pré-autorizados que o usuário possui para que execute suas funções. Cada ativo de informação possui um perfil de acesso para cada usuário, conforme necessidade própria.

- Perímetros de segurança: Áreas que contêm informações críticas ou sensíveis usadas para guarda ou processamento da informação.
- Proprietário da informação: É um gestor, formalmente indicado pela diretoria, responsável por qualificar o ciclo de vida do ativo, sendo responsável também por assegurar que os ativos de informação sejam inventariados, adequadamente classificados e protegidos conforme descrito na Política de Classificação, Rotulação e Tratamento da Informação.
- Segregação de funções: Princípio básico que consiste na separação de atribuições ou responsabilidades entre diferentes pessoas, especialmente nas funções ou atividades-chave de autorização, aprovação, execução, registro e auditoria, de tal maneira que ninguém detenha o conhecimento e/ou privilégios necessários para executar ou controlar todo o processo sozinho.
- Segurança cibernética: É a disciplina que concentra os esforços para a proteção dos ativos de informação no ambiente cibernético.
- Ambiente cibernético: É o ambiente resultante da interação de pessoas, softwares e serviços por meio de dispositivos tecnológicos e redes conectadas a estes dispositivos.

6. Disposições gerais

Esta política segue as seguintes disposições gerais:

- Esta política deve estar disponível e ser divulgada para todos os colaboradores e prestadores de serviços da Minutrade.
- Na Minutrade, a Segurança da Informação abrange também a segurança cibernética concentrando, principalmente, na informação no formato digital e nos sistemas interconectados que a processam, armazenam ou transmitem.
- Outras políticas devem ser geradas para tratar assuntos específicos da Segurança da Informação. Exemplos: Política de Controle de Acesso e Política de Desenvolvimento Seguro
- Procedimentos de Segurança da Informação devem ser estruturados para instruírem a prática dos princípios, aspectos, diretrizes e responsabilidades estabelecidas nesta política.
- Os Procedimentos de Segurança da Informação destinam-se a um público mais restrito e devem estar disponíveis de acordo com sua classificação da informação.
- A informação pode estar presente em diversas formas, tais como: sistemas de informação, diretórios de rede, bancos de dados, mídia (impressa, magnética ou ótica), dispositivos eletrônicos, equipamentos portáteis, microfilmes e até mesmo por meio da comunicação oral.
- Toda informação de propriedade da Minutrade pode ser monitorada através dos seus recursos de processamento da informação.

- Esta política está em *compliance* com a ABNT NBR ISO/IEC 27001:2013, ABNT NBR ISO/IEC 27002:2013 e com as leis e regulamentações aplicáveis.

7. Diretrizes principais

1. As informações da Minutrade, dos seus clientes e dos seus aliados devem ser tratadas de forma ética e sigilosa e de acordo com as leis, regulamentações vigentes e normas internas, evitando-se mau uso e exposição indevida.
2. Toda informação relacionada às operações da Minutrade constitui ativo dessa instituição, essencial à condução e à continuidade dos negócios, e em última análise, à sua existência. Independentemente 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.
3. Convém que funções conflitantes e áreas de responsabilidade sejam segregadas para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido das informações, durante todo seu ciclo de vida.
4. A identificação de qualquer colaborador ou prestador de serviço deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas. Sua senha deve ser mantida secreta, sendo proibido o seu compartilhamento.
5. A concessão de acessos deve obedecer ao critério de menor privilégio, na qual os usuários têm acesso somente aos recursos de informação imprescindíveis para o pleno desempenho de suas atividades.
6. Toda informação, processada internamente ou transmitida para organizações externas, deve estar protegida por meio de uma operação segura e pela correta utilização dos ativos de informação.
7. Os requisitos de Segurança da Informação para aquisição, desenvolvimento e manutenção de software devem ser estabelecidos e aplicados no ambiente Minutrade.
8. Os riscos associados aos ativos de informação ou a um grupo de ativos de informação, comprometendo a confidencialidade, a integridade ou a disponibilidade das informações da Minutrade, devem ser reportados ao Comitê Gestor de Segurança da Informação.
9. Todos os incidentes de Segurança da Informação devem ser registrados e tratados.
10. A Política de Segurança da Informação deve ser aprovada e divulgada pela Alta Direção e, suas diretrizes e responsabilidades devem ser entendidas e asseguradas de forma ampla pelos colaboradores e prestadores de serviço.

8. Responsabilidades

8.1. Alta Direção

- Aprovar a Política de Segurança da Informação e suas revisões.
- Tomar decisões e medidas em caso de descumprimento das políticas de Segurança da Informação.
- Garantir que todos os envolvidos com as informações da Minutrade tenham acesso a esta Política de Segurança da Informação.

8.2. Comitê Gestor de Segurança da Informação (CGSI)

- Promover melhorias nas políticas de Segurança da Informação e procedimentos relacionados.
- Aprovar os processos, políticas e procedimentos derivados da Política de Segurança da Informação, através de pelo menos um de seus representantes.
- Analisar os casos de irregularidade ou violação das políticas de Segurança da Informação e, quando for o caso, encaminhá-los à Alta Direção.
- Propor projetos e iniciativas relacionadas à melhoria da Segurança da Informação da Minutrade.
- Participar da elaboração de relatórios, levantamentos e análises que deem suporte à Gestão de Segurança da Informação e à tomada de decisão.
- Realizar reuniões trimestrais ou em convocação extraordinária, sempre que necessário.
- Definir os objetivos de Segurança da Informação na Minutrade.

8.3. Gestor da Gestão de Segurança da Informação (GGSI)

- Redigir as políticas de Segurança da Informação e suas revisões.
- Redigir os procedimentos de Segurança da Informação e suas revisões.
- Definir e registrar os proprietários da informação.
- Convocar e coordenar as reuniões do Comitê Gestor de Segurança da Informação.
- Prover as informações solicitadas pelo Comitê Gestor de Segurança da Informação.
- Receber e avaliar projetos relacionados ao aperfeiçoamento da Segurança da Informação.
- Analisar os incidentes de Segurança da Informação e acompanhar o seu tratamento e a sua solução.
- Solicitar e acompanhar a análise de vulnerabilidades para monitoramento dos níveis de Segurança da Informação.

- Gerenciar os riscos de Segurança da Informação, incluindo, quando necessário, os riscos relacionados à segurança cibernética.
- Promover a divulgação das políticas e procedimentos de Segurança da Informação.
- Promover treinamentos e orientações sobre as políticas e procedimentos de Segurança da Informação.
- Estabelecer mecanismos de registro e controles de não conformidades às políticas e procedimentos de Segurança da Informação.
- Compor o Comitê de Crise, sempre que ele for instaurado.

8.4. Gestores

- Quanto às equipes sob sua responsabilidade:
    - Ser referência quanto à Segurança da Informação.
    - Garantir que as diretrizes e os aspectos aqui definidos sejam seguidos.
    - Assegurar que as suas equipes tenham conhecimento das políticas e dos procedimentos de Segurança da Informação.
    - Ao requisitar a concessão de acesso físico ou lógico, sempre optar por conceder somente aquilo que seja necessário para execução da função.
    - Autorizar o trabalho remoto, quando necessário.

- Quanto às rotinas de Segurança da Informação:
    - Contribuir para a melhoria dos processos e procedimentos sob sua responsabilidade para que atendam às políticas de Segurança da Informação.

8.5. Colaboradores e prestadores de serviços

- Seguir as diretrizes e aspectos estabelecidos nesta política.
- Conhecer e cumprir as políticas e procedimentos de Segurança da Informação.
- Ser responsável pelo uso adequado e seguro dos ativos de informação e das informações a que tenha acesso.
- Buscar orientação sempre que não estiver absolutamente seguro quanto ao manuseio das informações.
- Comunicar ao Comitê Gestor de Segurança da Informação casos de violação ou falhas relacionadas à Segurança da Informação.
- Manter a confidencialidade de suas senhas, não compartilhá-las e criá-las obedecendo os requisitos de complexidade exigidos na Política de Controle de Acesso.

- Devolver o ativo de informação após o encerramento de suas atividades, do contrato ou acordo.

8.6. Proprietário da informação

- Autorizar o acesso às informações que são de sua responsabilidade.
- Fiscalizar os registros e controles de todos os acessos concedidos às informações sob sua responsabilidade.
- Participar, sempre que convocado, das reuniões do Comitê Gestor de Segurança da Informação.
- Revisar periodicamente os perfis de acesso.

8.7. Proprietário do ativo

- Assegurar que a informação relacionada ao ativo esteja gerenciada e protegida.
- Abrir requisição de serviço para solicitar criação ou alterações dos ativos.
- Definir a classificação do ativo e definir as restrições de acesso.
- Designar o custodiante do ativo.

8.8. Custodiante do ativo

- Operar o ativo e se responsabilizar pela sua guarda.
- Zelar pelo armazenamento, operação, administração e preservação do ativo que está sob sua custódia.
- Abrir requisição de serviço para solicitar a manutenção dos ativos.

9. Diretrizes específicas

9.1. Políticas de Segurança da Informação

- A Minutrade deve elaborar, manter e divulgar políticas de Segurança da Informação para proteger a informação de acordo com os princípios, os aspectos e as diretrizes de Segurança da Informação e, também, em total alinhamento com os requisitos do negócio.
- As políticas de Segurança da Informação devem ser desenvolvidas e analisadas criticamente levando em consideração os resultados da análise crítica pela alta direção.

9.2. Organização da Segurança da Informação

9.2.1. Segregação de funções

- Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe.
- Os ambientes de produção devem ser segregados e rigidamente controlados, garantindo o isolamento necessário em relação aos ambientes de desenvolvimento e homologação.
- O mau uso dos sistemas, feito de forma acidental ou deliberada, deve ser combatido pela segregação das funções de administração do sistema das funções de execução de certas atividades, ou entre áreas de responsabilidade. Tal segregação de funções visa criar controles para evitar fraudes ou conluios no desempenho de atividades críticas do sistema.
- As funções gerenciais e operacionais devem ser segregadas para restringir ao mínimo necessário os poderes de cada indivíduo e eliminar, ou ao menos reduzir, a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.
- Quando a segregação de funções for difícil ou impraticável a implementação, devem ser aplicados controles de compensação.

9.2.2. Contato com autoridades e grupos especiais

- A Minutrade deve elaborar procedimentos que especifiquem quando e quais autoridades serão contatadas e como os incidentes de Segurança da Informação identificados serão reportados em tempo hábil. Exemplo: no caso de suspeita de que uma lei foi violada, acionar a autoridade competente.
- A Minutrade deve manter contatos apropriados com grupos especiais, associações profissionais ou outros fóruns especializados em Segurança da Informação para ampliar o conhecimento sobre as melhores práticas e manter-se atualizado com as informações relevantes sobre Segurança da Informação.

9.2.3. Segurança da Informação em Gestão de Projetos

- A Segurança da Informação é um requisito não funcional em Gestão de Projetos que deve ser considerado, pelo gestor do projeto, em cada projeto.

9.2.4. Dispositivos móveis

- A Minutrade deve estabelecer e implementar uma Política de Uso de Dispositivos Móveis para definir as diretrizes de segurança das informações no trabalho remoto e no uso de dispositivos móveis.

9.2.5. Trabalho remoto (home office e teletrabalho)

- Os usuários devem utilizar somente os ativos da Minutrade para a execução das suas atividades profissionais durante o trabalho remoto ou o teletrabalho.
- Em casos de acesso remoto ao ambiente de produção, o acesso deve ser realizado através de VPN criptografada.
- Para o acesso aos demais serviços em nuvem, a estação cliente deve ter o mínimo de controles instalados, como antivírus e conexão confiável.
- O período de trabalho remoto ou teletrabalho deve estar em conformidade com o contrato de trabalho ou prestação de serviço e a utilização dos ativos fora do horário normal do expediente, incluindo, mas não se limitando a, correio eletrônico institucional, aplicativos e comunicadores instantâneos, por si só, não configuram sobrejornada, sobreaviso ou plantão do colaborador.
- A Minutrade deve estabelecer medidas de proteção voltadas para os ativos utilizados no trabalho remoto ou teletrabalho, como criptografia, dupla autenticação e proteção por senhas.
- A Minutrade não é responsável pela infraestrutura física de rede e pela conexão de internet contratada pelo colaborador para a execução das suas atividades no trabalho remoto ou teletrabalho.

9.3. Segurança em recursos humanos

- Durante a seleção de colaboradores, a Minutrade deve implementar atividades que diminuam os riscos e atenda aos requisitos de negócio quanto à vaga a ser preenchida.
- Os contratos de trabalho ou prestação de serviços devem incluir declarações de responsabilidade do indivíduo com relação à Segurança da Informação.
- A Minutrade deve assegurar que os colaboradores e prestadores de serviços estejam conscientes sobre as responsabilidades pela Segurança da Informação, por meio da assinatura do Termo de Confidencialidade e Declaração de Ciência e Adesão à Política de Segurança da Informação para os colaboradores e do Termo de Confidencialidade e Responsabilidade para os prestadores de serviço.

- No encerramento ou alteração de funções de um colaborador ou prestador de serviço, deve-se levar em consideração a Segurança da Informação e desativar ou modificar todos os seus acessos, de forma a garantir a proteção das informações da Minutrade.
- A Minutrade, através de um plano de treinamento de Segurança da Informação, deve garantir que todos os colaboradores sejam orientados quanto à Segurança da Informação e suas políticas.
- Todos os usuários devem ser treinados quanto à Segurança da informação antes de obter acesso aos ativos de informação.
- O acesso a esta política deve ser garantido a todos os colaboradores, respeitando a classificação da informação.
- O não cumprimento dessa política e/ou demais políticas e procedimentos que a complementam constitui falta grave e o usuário estará sujeito a penalidades definidas pela Diretoria Executiva.
- A Minutrade deve realizar procedimentos para a disseminação da cultura de segurança da informação e cibernética, incluindo, a implementação de programa de treinamento para colaboradores e prestadores de serviço.
- Qualquer situação de exceção, ou não prevista, deve ser analisada e autorizada pelo Comitê Gestor de Segurança da Informação (CGSI).

9.4. Gestão de ativos de informação

9.4.1. Responsabilidade pelos ativos

- A Minutrade deve estabelecer e implementar um processo de Gestão da Configuração e Ativos de Serviço para identificar todos os ativos com requisitos de controle, monitoramento e uso de licenças, mídias de instalação e manuais.
- O inventário dos ativos de informação, assim como sua manutenção, deve ser realizado no BDGC, sendo de responsabilidade da Gestão da Configuração e Ativos de Serviço.
- Cada ativo de informação deve possuir um responsável (custodiante) e um proprietário.
- O uso aceitável do ativo deve ser garantido através de termos da Segurança da Informação e ferramentas do Sistema de Gerenciamento de Configuração (SGC).
- Independentemente da forma de armazenamento ou de reprodução (impresso, eletrônico, mídia removível, vídeo, áudio e outros), toda a informação deve ser protegida durante seu ciclo de vida (manuseio ou utilização, armazenamento ou estocagem, transmissão ou transporte e descarte ou exclusão) de forma a evitar acessos, alteração ou destruição indevida.

9.4.2. Classificação da informação

- A Minutrade deve estabelecer e implementar uma Política de Classificação, Rotulação e Tratamento da Informação para definir as diretrizes para classificação, rotulação e tratamento das informações.
- É de responsabilidade do proprietário do ativo classificar as informações como:
    - Pública: Informações públicas, que podem ser divulgadas publicamente, com acesso irrestrito.
    - Interna: Informações internas, que podem ser divulgadas a todos os colaboradores e a prestadores de serviços (quando necessário e desde que estes estejam comprometidos com a confidencialidade da informação).
    - Restrita: Informações restritas, que devem ser divulgadas somente a determinados grupos, áreas ou cargos.
    - Confidencial: Informações confidenciais, que sua divulgação não autorizada ou acesso indevido pode gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação, imagem ou estratégia da Minutrade. A informação deve ser divulgada somente a determinados indivíduos.
- A rotulação e o tratamento da informação devem ser desenvolvidos e implementados de acordo com o esquema de classificação da informação na Minutrade.
- A classificação da informação deve orientar os usuários quanto ao tratamento da informação durante seu ciclo de vida, independentemente da forma de armazenamento, principalmente quanto ao uso de controles como criptografia ou descarte seguro de mídias.

9.4.3. Tratamento dos ativos e das mídias

- O uso de ativos específicos e/ou particulares de TI para fins pessoais é permitido desde que não prejudique os interesses da Minutrade e não cause impacto no tráfego da rede.
- Todos os recursos de processamento da informação disponibilizados pela Minutrade são de sua propriedade e os usuários possuem sua custódia para realização de suas atividades profissionais. Seu uso pessoal é permitido, desde que não prejudique suas atividades e não vá contra essa política, regulamentos e leis aplicáveis.
- A utilização de software nos recursos de processamento de informação deve estar homologada e autorizada pela área de TI. O uso de software não autorizado será classificado como incidente de Segurança da Informação e estará sujeito às penalidades pertinentes.
- A Minutrade deve estabelecer e implementar controles para que sejam protegidos os direitos de propriedade intelectual da Minutrade e de terceiros, de forma a permitir instalar e/ou utilizar somente recursos tecnológicos autorizados e com as respectivas licenças de uso válidas.

- A Minutrade disponibiliza acesso à Internet em suas instalações para uso nas atividades profissionais de seus usuários, que devem utilizá-lo com responsabilidade, evitando sites suspeitos e que vão contra o bom costume e/ou a legislação vigente. O ambiente de Internet pode ser monitorado para garantir a Segurança da Informação.
- O correio eletrônico disponibilizado pela Minutrade deve ser utilizado de forma profissional, ou seja, suas mensagens devem ser escritas com linguagem formal, respeitando os regulamentos internos e a legislação vigente, sem infringir o código de ética da Minutrade. A conta de correio eletrônico é de responsabilidade do usuário ao qual foi disponibilizada.
- O conteúdo de cada conta de correio eletrônico pode ser monitorado e acessado pela Minutrade quando detectadas situações de risco à Segurança da Informação, não garantindo ao usuário sigilo das mensagens da conta de correio eletrônico disponibilizada pela Minutrade.
- O uso de redes sociais é permitido desde que não prejudique os interesses da Minutrade. Em caso de usuários que possuem acesso às redes sociais da Minutrade, qualquer comunicação deve respeitar o código de ética, bem como as autorizações pertinentes.
- O acesso e utilização dos ativos disponibilizados pela Minutrade ou de ativos específicos e/ou particulares, inclusive de forma remota, fora do horário normal do expediente, incluindo, mas não se limitando a, correio eletrônico institucional, aplicativos e comunicadores instantâneos, por si só, não configuram sobrejornada, sobreaviso ou plantão do colaborador, visto que isso pode ocorrer por ato de liberalidade e/ou conveniência do próprio colaborador sem expressa e prévia requisição da Minutrade.

9.5. Controle de acesso

9.5.1. Requisitos do negócio

- A Minutrade deve estabelecer e implementar uma Política de Controle de Acesso alinhada com os requisitos do negócio.
- Os colaboradores e prestadores de serviço devem receber acesso à rede e aos serviços de rede que tenham sido especificamente autorizados a usar.
- A Minutrade deve adotar controles que garantam o acesso autorizado e diminua o risco de acesso não autorizado aos ativos de informação.

9.5.2. Gestão do acesso do usuário

- Todos os usuários devem ser identificados de forma única.
- As solicitações para concessão e revogação de acessos físicos e lógicos devem ser registradas formalmente.
- Os acessos físicos e lógicos devem ser revisados, periodicamente, através de processos e procedimentos formais de Gestão de Acesso.
- O acesso deve ser retirado logo após o encerramento/mudança das atividades, contratos ou acordos com colaboradores e prestadores de serviço.
- A concessão de acesso e o uso de acessos privilegiados devem ser restritos e controlados.

9.5.3. Gestão de acesso ao sistema e à aplicação

- Qualquer acesso à informação e às funções do sistema deve ser autorizado, registrado e restrito, podendo até mesmo ser rastreado.
- Onde aplicável pela Política de Controle de Acesso, o acesso aos sistemas e aplicações devem ser controlados por um procedimento seguro de entrada no sistema (*logon*).
- Os sistemas para gerenciamento de senhas devem ser interativos e assegurar a criação de senhas de qualidade.
- O acesso ao código-fonte de programas deve ser restrito e controlado.

9.6. Criptografia

- Ao utilizar criptografia, a Minutrade deve identificar e gerenciar o uso de chaves criptográficas.
- A Minutrade deve implementar uma política sobre o uso, proteção e tempo de vida das chaves criptográficas ao longo de todo o seu ciclo de vida.
- O uso de controles criptográficos deve estar em conformidade com todas as leis, acordos, legislação e regulamentações aplicáveis.

9.7. Segurança física e do ambiente

9.7.1. Perímetros e controle de entrada física

- Os perímetros de segurança devem ser protegidos com controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso permitido.
- O acesso físico ao ambiente da Minutrade deve ser controlado e segregado de acordo com a criticidade da informação armazenada em cada perímetro.

- A Minutrade deve implementar controles que garantam a proteção adequada para todos os ativos de informação.
- Em todos os ambientes físicos, os colaboradores, visitantes e prestadores de serviço devem portar identificações visuais de forma a garantir que estão autorizados a estarem naquele local.
- A Minutrade deve diminuir os riscos relacionados à mídia em papel, armazenamento removível e recurso de processamento da informação sem monitoramento.

9.7.2. Remoção de ativos

- Os recursos da Minutrade, sendo eles equipamentos, informações ou software não devem ser removidos sem autorização prévia do gestor responsável pelo colaborador ou prestador de serviço.
- Os softwares de segurança, como antivírus e *patches* de segurança, não devem ser desinstalados sem a autorização prévia do Gestor de Segurança da Informação.

9.7.3. Reutilização ou descarte seguro de ativos

- A Minutrade deve ter mecanismos para que as mídias de armazenamento que contêm informações confidenciais sejam destruídas fisicamente, ou as informações sejam destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis.

9.7.4. Mesa limpa e tela limpa

- As informações da Minutrade sensíveis ou críticas, em papel ou em mídia de armazenamento eletrônicas, devem ser guardadas em lugar seguro quando não estiver em uso, especialmente quando o escritório estiver desocupado.
- Os recursos de processamento de informação (computadores, notebooks, servidores, etc) devem ser mantidos desligados ou protegidos com mecanismo de tecla de bloqueio, senhas ou outros controles, quando não usados.
- Os documentos que contêm informação sensível ou classificadas como restrita ou confidencial devem ser removidos das impressoras e digitalizadoras imediatamente após o uso ou impressão.

9.8. Segurança nas operações

9.8.1. Responsabilidades e procedimentos operacionais

- A Minutrade deve implementar processos de Gestão de Mudança e Gestão de Capacidade para garantir a operação segura dos recursos de processamento da informação.
- Os procedimentos operacionais de ambientes críticos devem ser documentados e disponibilizados para todos os usuários que necessitam deles.

9.8.2. Separação de ambientes

- A Minutrade deve separar os ambientes de desenvolvimento, homologação e produção para reduzir os riscos de acessos ou modificações não autorizadas no ambiente de produção.

9.8.3. Cópias de segurança

- A Minutrade deve estabelecer e implementar Política de Backup alinhada com os requisitos do negócio relativos às cópias de segurança das informações, dos softwares e dos sistemas.
- Os proprietários dos ativos de informação devem definir as regras e características das cópias de segurança a serem realizadas para as informações de sua responsabilidade.
- A área de TI, em conjunto com a Gestão da Segurança da Informação, deve apoiar os proprietários dos ativos de informação na definição do tipo, periodicidade, armazenamento, replicação e tempo de retenção das cópias de segurança.
- As cópias de segurança de ambientes devem passar por testes de *restore*, garantindo a integridade das mídias.

9.8.4. Registros e monitoramento

- A Minutrade deve registrar e monitorar os eventos (*logs*) necessários para garantir a rastreabilidade de forma a atender necessidades de auditoria e regulamentação.
- O acesso aos registros de eventos (*logs*) deve ser restrito, controlado e monitorado.
- A Minutrade deve manter controle de forma a garantir a sincronização dos relógios de todos os seus ativos críticos.

9.8.5. Gestão de vulnerabilidades técnicas

- A Minutrade deve implementar controles de detecção, prevenção e recuperação para proteção contra vulnerabilidades, como, por exemplo, *malwares*.
- As informações sobre vulnerabilidades técnicas dos sistemas de informação em uso devem ser obtidas em tempo hábil e, caso ocorra a exposição destas vulnerabilidades, a Minutrade deve tomar as medidas apropriadas para lidar com os riscos associados.

9.8.6. Controles de auditoria de sistemas de informação

- A Minutrade deve implementar atividades de auditoria e definir requisitos para verificar os sistemas de informação de forma a minimizar as interrupções dos processos de negócio.

9.9. Segurança nas comunicações

- Qualquer comunicação que trafegue informações para o negócio deve adotar mecanismos para que a Segurança da Informação seja garantida.
- O ambiente de rede da Minutrade deve ser gerenciado, controlado e monitorado de forma a proteger as informações trafegadas.
- A Minutrade deve implementar acordos de níveis de serviço para os serviços de rede internos e terceirizados.
- A infraestrutura de rede nos ambientes de processamento de informação deve ser segregada em desenvolvimento, homologação e produção.
- Qualquer troca de informações deve ser regida por acordos que considerem os princípios de Segurança da Informação.
- O compartilhamento de informações da Minutrade deve respeitar sempre o sigilo da informação, atender aos requisitos de segurança previstos nesta política e respeitar as leis nacionais em vigor para evitar riscos desnecessários relacionados ao vazamento da informação ou que comprometam a instituição.
- A Minutrade deve estabelecer requisitos para confidencialidade ou acordos de não divulgação que reflitam as necessidades da organização para a proteção da informação junto aos colaboradores e prestadores de serviço.
- As informações trafegadas em mensagens eletrônicas devem ser adequadamente protegidas.

9.10. Aquisição, desenvolvimento e manutenção de Sistemas

- A aquisição, desenvolvimento e manutenção de sistemas e/ou aplicações devem estar aderentes às normas e às melhores práticas de mercado de Segurança da Informação.
- As mudanças nos sistemas devem ser controladas através de processos e procedimentos formais de Gestão de Mudança.
- Os dados do ambiente de produção não devem ser utilizados nos ambientes de desenvolvimento e/ou teste sem o devido tratamento. Exemplos: mascaramento dos dados sensíveis e/ou criptografia.
- Caso seja necessária a utilização de dados operacionais, deve-se implementar controles que garantam a sua confidencialidade e protejam contra remoção ou modificação da informação.

9.11. Desenvolvimento seguro

- A Minutrade deve implementar uma Política de Desenvolvimento de Produtos de Software para os sistemas desenvolvidos pela organização.
- O desenvolvimento e a manutenção dos sistemas desenvolvidos pela Minutrade devem atender aos requisitos de segurança em todo o ciclo de vida, a fim de garantir a confidencialidade, integridade, legalidade, autenticidade e disponibilidade das informações.
- As informações envolvidas em transações devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alteração não autorizada da mensagem, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
- Os dados de teste devem ser selecionados com cuidado, protegidos e controlados.

9.12. Relacionamento na cadeia de suprimentos

- A Minutrade deve manter um processo de Gestão do Fornecedor que considere os riscos de Segurança da Informação quanto a acordos, entrega e qualidade dos serviços, bem como sua disponibilidade.
- A Minutrade deve implementar requisitos de Segurança da Informação no acesso dos fornecedores aos ativos de informação para mitigar os riscos associados.
- Os requisitos de Segurança da Informação relevantes devem ser estabelecidos e acordados com cada fornecedor para que possa acessar, processar, armazenar, comunicar ou prover componentes de infraestrutura de TI para as informações da Minutrade.

9.13. Gestão de incidentes de Segurança da Informação

- A Minutrade deve implementar o processo de Gestão de Incidente e Requisição de Serviço e de Gestão de Evento para garantir o tratamento, a comunicação, o monitoramento, a detecção, a análise e notificação de incidentes e eventos de Segurança da Informação.
- O manuseio de evidências de incidentes de Segurança da Informação deve seguir procedimentos específicos para esse fim.
- A Minutrade deve implementar um ponto de contato para notificação e registro de incidentes de Segurança da Informação.

9.14. Gestão de Continuidade do Negócio

- Os proprietários dos ativos devem definir os níveis adequados de disponibilidade dos ativos de sua responsabilidade e, em conjunto com a área de TI, definir os recursos necessários para implementação de um Plano de Continuidade e de Disponibilidade de Serviço.
- O Plano de Continuidade e de Disponibilidade de Serviço deve ser testado e revisado ao menos uma vez ao ano, com contribuição da Gestão da Segurança da Informação.
- A Minutrade deve manter um processo de gestão de riscos de Segurança da Informação de forma a prover insumos para a Gestão de Riscos e para a Gestão da Continuidade e Disponibilidade de Serviço.

9.15. Tratamento de dados

- As informações pessoais devem ser protegidas quanto à sua privacidade, conforme requerido por legislação e regulamentação pertinente, quando aplicável.
- A Minutrade deve estabelecer e implementar uma Política de Tratamento de Dados com diretrizes para o planejamento, desenvolvimento e desempenho de atividades que envolvam tratamento de dados pessoais, de forma a respeitar os direitos e interesses dos titulares de dados pessoais e cumprir com a legislação e regulamentação relacionadas à proteção de dados pessoais.

9.16. Conformidade

- A Minutrade deve implementar controles de Segurança da Informação de forma a garantir conformidade com exigências de leis, regulamentações e contratos vigentes.
- A Minutrade deve analisar criticamente, de forma independente, ao menos uma vez no ano, a implementação da Segurança da Informação de acordo com as políticas e procedimentos da empresa, conforme direcionamentos da Melhoria Contínua.