POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI)

Sumário

1. Introdução

1.1. Atualmente, o alto de número de vazamentos de dados em todos os segmentos da sociedade digital é uma consequência do acesso fácil, que ao mesmo tempo, gera um aumento na complexidade para armazenar tais informações.

Como sabemos, a Segurança da informação é o pilar principal para a continuidade de um negócio e apresentamos neste documento orientações, normas, ações e responsabilidades relativas à Proteção da informação.

1.2. As regras aqui estabelecidas serão observadas em todos os seus detalhes por todos os colaboradores, Infocart TI e solicitada documentação de prestadores de serviços. Desta forma, quando divulgada e entregue a cópia deste documento, todos os que receberem se comprometem a respeitar todos os tópicos abordados e ficam cientes da repercussão de tais regras no seu dia-a-dia.

1.3. São princípios para o Sistema de Gestão de Segurança da Informação a Confidencialidade, a Integridade e a Disponibilidade, conforme norma de mercado para a Segurança da Informação (NBR/ISO 27001-2013). Esses devem ser preservados, controlados e auditados para garantir que as informações estejam protegidas nas medidas exigidas para sua utilização.

1.4. Esta Política de Segurança da Informação (PSI), aprovada, compreende as diretrizes e normas que servem de base para atender aos princípios fundamentais da Segurança da Informação.

1.5. A Política de Segurança da Informação tem por princípio a proteção dos dados, informações e conhecimento, classificados como sigilosos, além da preservação dos dados Cartorários.

1.6. Dessa forma, a Infocart TI estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

2. Propósito

2.1. Constituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação e a conformidade com a LGPD (Lei Geral de Proteção de Dados) juntamente com o Provimento 74/2018 CNJ;

2.2. Promover ações necessárias à implementação e à manutenção da segurança da informação;

2.3. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal ao sistema de informação mantido pela Infocart TI;

2.5. Combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem da Infocart TI;

2.6. Esta PSI se aplica a todos os responsáveis, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informação e de processamento no ambiente da Infocart TI;

2.7. Estabelecer as competências e atribuições dos responsáveis envolvidos nesta política;

2.8. Tornar a segurança da informação como um dos elementos fundamentais no planejamento estratégico da Infocart TI, conforme seus princípios básicos:

• **Integridade:** garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

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

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

3. Diretrizes

3.1 Objetivo

3.1.1 O objetivo da gestão de Segurança da Informação da Infocart TI é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos.

3.2 Gestores de Segurança da Informação

3.2.1. Os Gestores de Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na Infocart TI. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades da Infocart TI.

3.3. Proteção de Recursos

3.3.1. Proteger os recursos de Tecnologia da Informação e Comunicações, as informações e sistemas contra a modificação, destruição, acesso ou divulgação não autorizada, garantindo sua confidencialidade, integridade e disponibilidade.

3.4. Utilização de Informações e Recursos

3.4.1. Assegurar que informações e recursos tecnológicos sejam tornados disponíveis para Órgãos devidamente autorizados, e que sejam utilizados apenas para finalidades lícitas, éticas e administrativamente aprovadas.

3.5. Nível de Segurança

3.5.1. Garantir que na criação de novos serviços, a seleção de mecanismos de segurança e a aquisição de bens e contratação de serviços, levem em consideração o balanceamento de aspectos tais como: riscos, tecnologia, austeridade no gasto, qualidade, velocidade e impacto no negócio, possuindo sistema de proteção redundante para fazer detecção de intrusos.

3.6. Conscientização

3.6.1. Tomar medidas para que Órgãos com acesso às informações, ambientes e recursos tecnológicos da Infocart TI, sejam devidamente conscientizados quanto à Segurança da Informação, face às suas responsabilidades e atuação.

3.7. Gestão de Ativos

3.7.1. Assegurar a análise periódica dos ativos da informação (bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade de negócios, procedimentos de recuperação, trilhas de auditoria e informações armazenadas) de forma que estejam devidamente inventariados, protegidos, tenham um usuário responsável e tenham mapeadas suas vulnerabilidades e ameaças de segurança.

3.8. Monitoramento

3.8.1. Garantir o monitoramento do tráfego de informações efetuado em ambientes e recursos de Tecnologia de Informação e Comunicações, rastreando e identificando possíveis ocorrências de eventos críticos, no estrito interesse da administração da Infocart TI, obedecendo a legislação aplicável.

3.9. Gerenciamento das Operações e Comunicações

3.9.1. Garantir a operação segura e corrente dos recursos do processamento da informação por intermédio da implementação de controles internos de segurança considerando as pessoas, procedimentos, ambientes e tecnologia.

3.10. Desenvolvimento, Manutenção e Produção de Sistemas

3.10.1. Assegurar que o desenvolvimento, manutenção, aquisição e adaptação de produtos de mercado e sistemas internos e/ou externos, sejam providos dos requisitos de Segurança necessários para garantir informações confiáveis, íntegras e oportunas.

3.11. Continuidade das Atividades

3.11.1. Garantir a continuidade das atividades da Infocart TI, reduzindo a um período aceitável e factível, a interrupção causada por desastres ou falhas de segurança, por intermédio da combinação de ações de administração de crises, prevenção e recuperação dos serviços.

3.12. Terceirização ou Prestação de Serviços

3.12.1. Manter nível de segurança da informação adequado, quanto aos aspectos desta política, naquilo que se refere a responsabilidade pelos procedimentos, sistemas e recursos, terceirizados no todo ou em parte, promovendo auditorias periódicas, buscando o cumprimento dos requisitos de segurança da informação.

3.13. Conformidade

3.13.1. Garantir o cumprimento das leis, regulamentos e normas que regem as atividades da Infocart TI, de forma a obter máxima aderência aos instrumentos legais e normativos, garantindo que os requisitos de segurança sejam cumpridos.

3.14. Administração da Segurança da Informação

3.14.1. Assegurar que a administração da segurança da informação da Infocart TI, seja feita pelo Administrador, por intermédio de área específica, com responsabilidades de estabelecer, implementar, manter e coordenar a elaboração e revisão da Política de Segurança da Informação, bem como avaliar e analisar assuntos a ela pertinentes.

3.15. Prevenção e Resposta a Incidentes

3.15.1. Assegurar que medidas preventivas sejam tomadas com o objetivo de diminuir o risco de ocorrência de fraudes e/ou incidentes que comprometam a segurança da informação, devendo existir canal de comunicação adequado para esse fim.

3.16. Gestão de Risco

3.16.1. Fundamentar-se em atividades coordenadas para direcionar e controlar a Infocart TI no que se refere aos riscos (risco deve ser entendido como perigo ou possibilidade de perigo, ou seja, a possibilidade de perda ou exposição à perda). Deve ser avaliado como uma combinação da probabilidade de um evento e a sua consequência, portanto, um compromisso entre a probabilidade de um evento e o seu impacto.

3.17. Propriedade da Informação

3.17.1. Garantir que toda informação armazenada e em trânsito pela Infocart TI por meio de tecnologia, procedimentos e ambientes é de sua propriedade, e será usada apenas por usuários devidamente autorizados para fins profissionais, no estrito interesse da Associação.

3.18. Backup

3.18.1. Os backups devem ser realizados por sistemas de agendamento. Além dos backups normalmente realizados no servidor, deverá ser feito backup adicional mantido em dispositivo externo com as informações codificadas (criptografadas) em ambiente seguro para armazenagem fora da Infocart TI. A rotina implementada de backup deve estar formalmente documentada para consultas e auditorias.

4. Papéis e Responsabilidades

4.1. Compete à área de Segurança da Informação:

4.1.1. Propor controles e melhorias relacionados ao tema de segurança da informação;

4.1.2. Definir e documentar as políticas e procedimentos relacionados à operacionalização da segurança da informação;

4.1.3. Monitorar e analisar os alertas e informações relacionados à segurança das informações;

4.1.4. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

4.1.5. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;

4.1.6. Disseminar a cultura de Segurança junto às demais áreas da Instituição;

4.1.7. Participar dos projetos em que a área estiver envolvida, acompanhando e sugerindo questões relacionadas ao tema da área;

4.1.8. Proteger as informações contra acessos indevidos e divulgação não autorizada;

4.1.9. Zelar para que os recursos tecnológicos sejam utilizados de forma eficaz, dentro das finalidades da Infocart TI e de Conhecimento do Gestor;

4.1.10. Não compartilhar ou divulgar credenciais de acesso ou equipamentos, sem a autorização explícita;

4.1.11. Cumprir as regras estabelecidas na PSI, normas e procedimentos de segurança da informação, bem como as demais leis, regulamentos e normas aplicáveis;

4.1.12. Estar atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do Gestor sempre que estiver com dúvidas;

4.1.13. Não criar, adquirir ou realizar uso de softwares não homologados ou não autorizados pelo Gestor;

4.1.14. Realizar as cópias de segurança do ambiente tecnológico;

4.1.15. Configurar os equipamentos, ferramentas e sistemas como todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta PSI e normas adicionais;

4.1.16. Planejar, implantar, fornecer e monitorar a capacidade de armazenamento, processamento e transmissão, necessárias para ambiente computacional.

4.2. Compete ao Gestor da área de Segurança

4.2.1. Aprovar juntamente e revisar periodicamente a PSI;

4.2.2. Determinar as diretrizes de Segurança da Informação;

4.2.3. Apresentação de assuntos relevantes quando cabível;

4.2.4. Reforçar junto à equipe de Segurança da Informação, o cumprimento das diretrizes desta PSI, bem como servir como replicador das boas práticas e controles;

4.2.5. Propor ajustes e ferramentas à área de Segurança da Informação que auxilie nos processos de negócio da área;

4.2.6. Informar, à área de Segurança da Informação, sobre o encerramento de contratos em que os prestadores de serviços possuam qualquer tipo de acesso físico ou lógico às informações;

4.2.7. Contribuir nos processos de revisão periódica de acessos ou em outras situações em que forem acionados pela área de Segurança da Informação.

4.3. Compete à área Jurídica da Infocart TI

4.3.1. Requerer a inserção de cláusulas que obriguem o cumprimento desta PSI e demais leis, regulamentos e normas aplicáveis aos prestadores de serviços, cujos

contratos tenham sua análise requerida ao departamento, assegurando que as informações sejam utilizadas apenas para sua finalidade dentro da Infocart TI e preservando sua confidencialidade.

5. Sanções e Punições

5.1. Na hipótese de violação desta PSI ou das normas de segurança da informação, o Gestor determinará as sanções administrativas que serão aplicadas ao infrator, sendo que:

5.2.1. Para os colaboradores, pode acarretar na aplicação de advertência e/ou suspensão ou desligamento formal conforme previsto na Matriz de Penalidades;

5.2.2. Para os prestadores de serviços, pode acarretar na aplicação rescisória imediata do respectivo contrato estabelecido violado.

5.3. A aplicação de sanções e punições será realizada conforme a análise do Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas pelas devidas Leis, podendo, no uso do poder, disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave, conforme termo descrito no item 5.1;

5.4. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano a Infocart TI, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

6. Casos Omissos

6.1. Os casos omissos serão avaliados pelo Gestor de Segurança da Informação para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação da área de Segurança da Informação da Infocart TI, adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações.

7. Aprovação e atualização da PSI

7.1. Os controles de segurança da informação devem ser planejados, aplicados, implementados e, periodicamente, avaliados de acordo com os objetivos e os riscos;

7.2. Alteração da PSI realizada conforme as seguintes regras;

7.2.1. Ordinariamente a cada 2 anos;

7.2.2. Extraordinariamente sempre que identificada a necessidade;

7.2.3. Por encaminhamento do Gestor de Segurança da Informação e aprovação.

8. Glossário

8.1. Ameaça: ameaça pode ser considerada um agente externo ao ativo de informação, pois, se aproveita de suas vulnerabilidades para quebrar os princípios básicos da informação – a confidencialidade, integridade ou disponibilidade, que pode vir a prejudicar a Infocart TI;

8.2. Integridade: Corresponde à preservação da precisão, consistência e confiabilidade das informações e Sistemas da Infocart TI ao longo dos processos ou de seu ciclo de vida, fazendo com que circulem ou sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los, comprometê-los ou danificá-los;

8.3. Disponibilidade: Está relacionada ao tempo e acessibilidade que se tem aos dados e Sistemas da Infocart TI, ou seja, se eles podem ser consultados a qualquer momento;

8.4. Confidencialidade: Relacionado com a privacidade dos dados da Infocart TI. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas do Sistema por meio de *ciberataques*, espionagem, entre outras práticas. Além disso, a confidencialidade está relacionada ao princípio do "menor privilégio" ou hierarquização, que estabelece acesso apenas a poucas pessoas, no caso, dados para os Órgãos integrados que tenha autorização, conforme a necessidade de conhecimento e o nível de responsabilidade por ele instituído;

As ameaças podem ser naturais: são aquelas que se originam de fenômenos da natureza; involuntárias: são as que resultam de ações desprovidas de intenção para causar algum dano, e intencionais: são aquelas deliberadas, que objetivam causar danos, tais como *hacker*.

Sendo assim, é um princípio com forte política de classificação e cujas seguintes características conferem maior suporte:

- ✓ Identificação;
- ✓ Autenticação;
- ✓ Autorização;
- ✓ Controles de acesso;
- ✓ Privacidade;

8.5. Ativo de informação: Patrimônio intangível da Infocart TI, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, bem como quaisquer informações criadas ou adquiridas por meio de integrações, aquisição via recebimento de atos, em formato, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional da Infocart TI ou por infraestrutura externa contratada pela organização, além dos

documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física;

8.6. Controle: Medida de segurança adotada pela Infocart TI para o tratamento de um risco específico;

8.7. Gestor da Informação: Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação;

8.8. Incidente de segurança da informação: Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações da Infocart TI;

8.9. Risco de segurança da informação: Efeito da incerteza sobre os objetivos de segurança da informação da Infocart TI;

RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco)

8.10. Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações da Infocart TI;

8.11. Vulnerabilidade: A *NBR ISO/IEC 27002:2005* define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação. Ao terem sido identificadas as vulnerabilidades ou os pontos fracos, será possível dimensionar os riscos aos quais o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção;

8.12. Backup: Significa Cópia de Segurança, para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos;

8.13. Lei Geral de Proteção de Dados: No dia 14 de agosto de 2018, foi sancionada a Lei Geral de Proteção de Dados ("LGPD", Lei n° 13.709/2018, publicada em 15/08/2018), que entrou em vigor em agosto de 2020, após um período de 18 meses para adaptação;

Esta lei irá trazer mudanças significativas que acarretará radicalmente a abordagem da privacidade do indivíduo, empresas e órgãos públicos.

Resumindo, a *LGPD* é um conjunto de regras, designado a dar mais controle sobre dados pessoais aos cidadãos, ou seja, regras que devem ser seguidas por empresas em relação à coleta, armazenamento e utilização de dados pessoais do usuário. A empresa, Órgão ou Associação que seguir as boas práticas da LGPD terá punições mais brandas em incidentes de vazamentos de dados. A legislação vale para qualquer negócio que opere no país, mesmo se for sediado no exterior.

8.14. Proteção redundante: Manter sistemas duplicados ou triplicados para garantir a disponibilidade de processos e equipamentos críticos;

9. Gestão da Política

9.1. A Política Geral de Segurança da Informação é aprovada pelo Gestor Infocart TI;

9.2. A presente política foi aprovada no dia 02/08/2021.

Jaciara – MT, 02 de Agosto de 2021.