GUIA ORIENTATIVO DE

SEGURANÇA DA INFORMAÇÃO NA PROTEÇÃO DOS DADOS PESSOAIS

Câmara Técnica sobre a Lei Geral
de Proteção de Dados Pessoais
Conselho Nacional de Controle Interno

Conaci
CONSELHO NACIONAL DE CONTROLE INTERNO

SUMÁRIO

1. APRESENTAÇÃO

A Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018) estabelece um conjunto de regras para o tratamento de dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Na LGPD foram elencadas uma série de disposições relacionadas à segurança da informação com foco na proteção dos dados pessoais, desde a definição da segurança como princípio (art. 6), até o estabelecimento de regras relacionadas à segurança e ao sigilo dos dados (art. 46 a 49).

art. 6, VII

Define a **segurança** como princípio a ser observado por meio da utilização de medidas técnicas e administrativas aptas a **proteger os dados pessoais de acessos não autorizados** e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

art. 46

Estabelece que os agentes de tratamento devem adotar **medidas de segurança**, técnicas e administrativas aptas a **proteger os dados pessoais de acessos não autorizados** e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

art. 47

É determinado que os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a **segurança da informação** prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término.

art. 48

Também trata sobre o tema da segurança no aspecto relacionado a comunicação de **incidentes de segurança** a Autoridade Nacional de Proteção de Dados – ANPD e aos titulares dos dados pessoais, estabelecendo a necessidade de comunicação por parte do controlador à autoridade nacional e ao titular a ocorrência de **incidente de segurança** que possa acarretar risco ou dano relevante aos titulares.

art. 49

Por fim, o art. estabelece que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos **requisitos de segurança**, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Lei Geral de Proteção de Dados, nº 13.709/2018

Nesse contexto, a segurança da informação desempenha um papel crucial na proteção dos dados pessoais, uma vez que estabelece uma série de boas práticas e estratégias direcionadas para garantir a integridade dos dados. Seu foco reside em prevenir ataques cibernéticos, bem como diversas outras ameaças e riscos que possam comprometer uma organização.

O Conselho Nacional de Controle Interno – CONACI, por meio da Câmara Técnica sobre LGPD, disponibiliza o Guia Orientativo de Segurança da Informação na Proteção de Dados Pessoais que apresenta uma série de boas práticas de segurança com foco na proteção dos dados pessoais.

2. SEGURANÇA DA INFORMAÇÃO

A segurança da informação é uma disciplina abrangente que engloba diversas áreas, tais como tecnologia da informação, gerenciamento de riscos, conformidade regulatória, governança corporativa e conscientização do usuário. Ela demanda a implementação de uma série de controles e práticas para salvaguardar os ativos de informação de uma organização. Isso inclui desde a avaliação de riscos e o estabelecimento de políticas de segurança até a adoção de medidas técnicas, como criptografia, firewalls, sistemas de detecção de intrusão e autenticação multifatorial, entre outras.

A preservação da confidencialidade, integridade e disponibilidade dos dados é fundamental para garantir a segurança da informação em qualquer organização. A confidencialidade garante que apenas indivíduos autorizados tenham acesso aos dados, protegendo as informações sensíveis de serem divulgadas a pessoas não autorizadas.

A integridade dos dados assegura que eles permaneçam íntegros e precisos ao longo do tempo, impedindo modificações indevidas que possam comprometer sua veracidade e confiabilidade. Por fim, a disponibilidade dos dados garante que eles estejam acessíveis quando necessários, evitando interrupções não planejadas que possam prejudicar as operações da organização.

Portanto, para alcançar essa proteção abrangente, é essencial implementar medidas de segurança que protejam contra acessos não autorizados, modificações indevidas e interrupções não planejadas, garantindo a integridade e a continuidade das operações. Muitas regulamentações, como a LGPD (Lei Geral de Proteção de Dados), exigem que as organizações implementem medidas de segurança da informação. Investir em medidas de segurança da informação ajuda a garantir que a organização esteja em conformidade com as leis e regulamentos aplicáveis.

Em resumo, a Segurança da Informação desempenha um papel fundamental na proteção dos dados pessoais, garantindo que eles sejam mantidos seguros, confidenciais e íntegros, ao mesmo tempo em que são processados de acordo com as leis e regulamentações aplicáveis. Essa abordagem proativa não apenas protege os indivíduos contra o uso indevido de suas informações pessoais, mas também promove a confiança do público e a reputação das organizações que lidam com esses dados.

3. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação (PSI) é um documento que estabelece diretrizes, normas e procedimentos que a organização deve seguir para proteger suas informações e garantir a segurança dos dados.

A PSI estabelece medidas preventivas e corretivas, ajudando a identificar e mitigar riscos relacionados à segurança da informação. Ao antecipar possíveis ameaças, a organização estará mais preparada para enfrentar desafios, protegendo-se contra potenciais prejuízos e danos à reputação.
Uma PSI robusta engloba uma ampla gama de normas e procedimentos elaborados. Dentro desse conjunto, alguns assumem uma relevância ainda maior no contexto da proteção de dados pessoais, uma vez que contêm diretrizes específicas de segurança destinadas a salvaguardar esses ativos vitais. Estas diretrizes não apenas estabelecem os padrões e protocolos necessários para proteger os dados pessoais de forma eficaz, mas também delineiam as responsabilidades dos colaboradores, os processos de monitoramento e auditoria, além das medidas corretivas a serem tomadas em caso de violação ou incidente de segurança.

Essas normas internacionais trazem uma série de diretrizes e boas práticas que devem ser considerados em uma PSI, sobretudo, para as questões relacionadas a proteção dos dados pessoais como:

1. gestão de acessos;
2. backup;
3. prevenção de incidentes de segurança;
4. plano de resposta a incidentes;
5. proteção de ativos críticos;
6. criptografia.

3.1. GESTÃO DE ACESSOS

A gestão de acessos, abrangendo tanto os aspectos físicos quanto lógicos, desempenha um papel crucial na garantia da segurança da informação e no controle de acesso em qualquer organização. Suas diretrizes são projetadas para garantir que apenas pessoas autorizadas tenham permissão para acessar ativos específicos, fortalecendo assim a segurança e a confidencialidade das informações corporativas.

3.1.1. GESTÃO DE ACESSOS FÍSICOS

A gestão de acessos físicos refere-se ao controle e administração do acesso a espaços físicos dentro de uma organização, como edifícios, instalações, salas ou áreas restritas. Essa gestão é fundamental para garantir a segurança das pessoas, dos bens e dos dados pessoais e sensíveis. Envolve a implementação de medidas de segurança física, como sistemas de fechaduras, cartões de acesso, câmeras de vigilância e controle biométrico, para garantir que apenas indivíduos autorizados tenham acesso aos espaços designados. Além disso, a gestão de acessos físicos inclui o desenvolvimento e a aplicação de políticas e procedimentos para monitorar e controlar o acesso, a fim de prevenir acesso não autorizado e proteger os ativos da organização.

A gestão de acessos físicos, de acordo com a ISO 27001, envolve várias boas práticas, tais como:

- **avaliação de riscos:** identifique e avalie os riscos relacionados à segurança física, como acesso não autorizado a instalações, roubo de equipamentos, entre outros;

- **desenvolvimento de políticas e procedimentos:** estabelecimento de políticas e procedimentos para controlar o acesso físico às instalações da organização. Isso pode incluir políticas de controle de acesso, diretrizes para o uso de dispositivos de identificação, procedimentos de autorização de acesso e protocolos de segurança para visitantes;
- **implementação de controles físicos**: implemente medidas físicas de segurança, como sistemas de fechaduras eletrônicas, câmeras de vigilância, cercas, controle biométrico de acesso, entre outros;
- **equipe especializada em segurança física:** designe uma equipe de segurança ou contrate uma empresa especializada em segurança física;
- **treinamento e conscientização**: capacite os colaboradores sobre as políticas e procedimentos de segurança física, bem como a importância do controle de acesso e da proteção dos ativos da organização;
- **monitoramento e revisão:** monitore continuamente os controles de acesso físico para garantir sua eficácia, além de revisar periodicamente as políticas e procedimentos para garantir que estejam alinhados com as necessidades e requisitos da organização.

3.1.2. GESTÃO DE ACESSOS LÓGICOS

A gestão de acessos lógicos se refere ao controle de acesso a sistemas de computadores, redes, aplicativos e dados digitais de uma organização. As boas práticas de gestão de acessos, de acordo com a série ISO/IEC 27000, envolvem a implementação de controles eficazes.

Esses controles estão relacionados às medidas adotadas para garantir que apenas pessoas autorizadas tenham acesso aos recursos de informação da organização, e que esse acesso seja concedido conforme a necessidade. A gestão de acessos lógicos é implementada por meio de uma série de práticas, tais como:

- **identificação de usuários:** estabeleça processos para identificar e autenticar usuários antes de conceder-lhes acesso aos sistemas e dados da organização. Isso pode incluir o uso de credenciais individuais, como nomes de usuário e senhas, autenticação multifatorial ou outros métodos de autenticação robustos;
- **controle de acesso:** implemente controles de acesso adequados para garantir que os usuários tenham acesso apenas às informações e recursos necessários para realizar suas funções de trabalho;

- **políticas de acesso**: desenvolva políticas claras e abrangentes que estabeleçam quem tem permissão para acessar quais recursos de informação e sob que circunstâncias. As políticas devem ser comunicadas efetivamente a todos os colaboradores e revisadas regularmente para garantir que estejam alinhadas com as necessidades de segurança da organização;
- **monitoramento e auditoria:** implemente sistemas de monitoramento e auditoria para rastrear atividades de acesso aos sistemas e dados da organização. Isso pode incluir a análise de logs de acesso, monitoramento de eventos de segurança, revisões periódicas de permissões de acesso e análise de comportamento de usuários para detectar atividades suspeitas;
- **gerenciamento de identidades:** estabeleça processos eficazes para o gerenciamento de identidades dos usuários, incluindo a atribuição e revogação de credenciais de acesso, a gestão de contas de usuário e a atualização regular das permissões de acesso com base em mudanças de função ou responsabilidade;
- **conscientização e treinamento:** forneça treinamento regular e conscientização aos funcionários sobre as políticas e procedimentos de segurança da informação, incluindo a importância do controle de acesso e as práticas recomendadas para proteger informações sensíveis.

3.2. BACKUP

O procedimento de Backup visa garantir a recuperação eficiente e segura de dados críticos em caso de perda, corrupção ou desastre, estabelecendo mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades. As boas práticas de backup de acordo com a série ISO/IEC 27000 enfatizam a importância de proteger os dados da organização contra perda, corrupção e acesso não autorizado. Abaixo estão algumas práticas recomendadas:

- **política de backup:** estabeleça uma política clara de backup que inclua critérios como frequência de backup, tipos de dados a serem incluídos nos backups, métodos de armazenamento, retenção de backups e procedimentos de recuperação;
- **priorização de dados críticos**: Identifique e priorize os ativos de informação críticos que precisam ser incluídos nos backups. Isso pode incluir dados dos titulares e outros dados essenciais para as operações da organização;
- **definir métodos adequados:** Escolha métodos de backup adequados com base nas necessidades de segurança e disponibilidade dos dados. Isso pode incluir backups completos, diferenciais e incrementais, bem como a utilização de técnicas de criptografia para proteger os dados durante o armazenamento e a transmissão;

- **armazenamento seguro:** armazene os backups em locais seguros e protegidos contra ameaças físicas, como incêndios, inundações e roubo. Além disso, considere a implementação de medidas de segurança, como criptografia e acesso restrito, para proteger os backups contra acesso não autorizado;
- **testes de recuperação:** realize testes regulares de recuperação de backup para garantir a eficácia dos procedimentos de backup e recuperação em caso de emergência. Isso ajuda a identificar e corrigir quaisquer falhas ou problemas antes que ocorram situações reais de perda de dados.

3.3. PREVENÇÃO DE INCIDENTES DE SEGURANÇA

A prevenção de incidentes de segurança é uma parte crucial da gestão da segurança da informação. Os incidentes de segurança podem incluir violações de dados, acessos não autorizados, malware, phishing e outros eventos que comprometem a confidencialidade, integridade ou disponibilidade de informações sensíveis.

As boas práticas de prevenção de incidentes de acordo com a série ISO/IEC 27000 envolvem a implementação de controles e medidas proativas para evitar e mitigar incidentes de segurança da informação. Abaixo estão algumas práticas recomendadas:

- **gestão de riscos:** realize avaliações regulares de riscos de segurança da informação para identificar potenciais vulnerabilidades, ameaças e impactos associados a ativos de informação críticos;
- **implementação de controles**: Implemente controles de segurança adequados para proteger os ativos de informação da organização contra ameaças conhecidas. Isso pode incluir controles técnicos, como firewalls, antivírus, sistemas de detecção de intrusão, criptografia e controles organizacionais, como políticas de segurança da informação, conscientização dos funcionários e procedimentos de gestão de mudanças;
- **monitoramento e detecção de ameaças:** estabeleça sistemas de monitoramento contínuo para detectar atividades suspeitas, intrusões e violações de segurança. Isso pode envolver a análise de logs de eventos, monitoramento de rede e sistemas, e o uso de ferramentas de detecção de ameaças;
- r**esposta a incidentes:** desenvolva planos de resposta a incidentes claros e eficazes para lidar com incidentes de segurança da informação. Isso inclui a designação de responsabilidades, procedimentos de notificação, contenção de incidentes, análise forense e recuperação de sistemas e dados.

3.4. PLANO DE RESPOSTA A INCIDENTES

Um plano de resposta a incidentes é um documento que descreve os procedimentos e as etapas a serem seguidas quando ocorre uma violação de segurança da informação ou outro incidente relacionado à segurança.

As boas práticas de plano de resposta a incidentes na série ISO/IEC 27000 envolvem a implementação de um conjunto de procedimentos e diretrizes para garantir uma resposta eficaz a incidentes de segurança da informação. Aqui estão algumas práticas recomendadas de acordo com a ISO/IEC 27001:

- **equipe de respostas a incidentes:** designe uma equipe multidisciplinar, composta por membros de diferentes áreas, como TI, segurança da informação, jurídico e comunicações, para coordenar a resposta a incidentes;
- **procedimento de notificação:** estabeleça procedimentos claros para relatar incidentes de segurança da informação, incluindo quem deve ser notificado, como fazer a notificação e em que prazos;

- **classificação de incidentes:** defina critérios para classificar e priorizar os incidentes com base em sua gravidade, impacto e urgência, garantindo uma alocação eficiente de recursos durante a resposta;
- **contenção de incidentes:** descreva os procedimentos para conter e mitigar os incidentes, incluindo a interrupção de atividades maliciosas, isolamento de sistemas afetados e implementação de medidas temporárias para reduzir o impacto;
- **comunicação e gerenciamento de crise**: defina os procedimentos de comunicação interna e externa durante um incidente, incluindo como informar as partes interessadas afetadas, autoridades reguladoras, clientes e mídia. Também inclua planos para gerenciamento de crise e coordenação de resposta com outras organizações, se necessário.

3.5. PROTEÇÃO DE ATIVOS CRÍTICOS

A Política de Segurança da Informação desempenha um papel fundamental na proteção dos ativos críticos de uma organização. Estabelecendo diretrizes claras, ela assegura que informações pessoais e sensíveis sejam tratadas com o devido cuidado, impedindo acesso não autorizado e garantindo a integridade e confidencialidade dos dados.

A proteção de ativos críticos é fundamental para garantir a segurança da informação e a continuidade dos negócios em uma organização. Aqui estão algumas boas práticas de acordo com a série ISO/IEC 27000:

- **identificação dos ativos críticos:** realize uma análise detalhada dos ativos de informação e sistemas da organização para identificar aqueles que são críticos para suas operações e objetivos de negócios;
- **gestão de riscos:** realize avaliações de riscos específicas para os ativos críticos, identificando ameaças potenciais, vulnerabilidades e impactos associados a esses ativos;
- **implementação de controles:** implemente controles de segurança adequados para proteger os ativos críticos contra ameaças identificadas. Isso pode incluir controles técnicos, como firewalls, antivírus, criptografia e sistemas de detecção de intrusão, bem como controles organizacionais;

- **monitoramento detecção de ameaças:** estabeleça sistemas de monitoramento contínuo para detectar atividades suspeitas ou anomalias que possam indicar uma ameaça aos ativos críticos da organização;
- **melhoria contínua**: Realize revisões regulares dos controles de segurança dos ativos críticos e identifique oportunidades de melhoria com base nas lições aprendidas com incidentes de segurança e mudanças nas ameaças e no ambiente de negócios.

3.6. CRIPTOGRAFIA

- As boas práticas de criptografia na série ISO/IEC 27000 são essenciais para proteger a confidencialidade, integridade e autenticidade das informações sensíveis de uma organização.

Aqui estão algumas práticas recomendadas:

- **identificação de necessidades de criptografia**: realize uma análise de risco para identificar quais informações e sistemas requerem criptografia para proteção adequada;
- **seleção de algoritmos robustos**: escolha algoritmos de criptografia adequados e robustos, que estejam de acordo com as melhores práticas e padrões reconhecidos, como AES (*Advanced Encryption Standard*) para criptografia simétrica e RSA ou ECC (*Elliptic Curve Cryptography*) para criptografia assimétrica;
- **gerenciamento de chaves:** Implemente práticas adequadas de gerenciamento de chaves para garantir a segurança das chaves de criptografia. Isso inclui a geração segura de chaves, armazenamento seguro, distribuição controlada, rotação periódica de chaves e revogação de chaves comprometidas.
- **revisão e atualização**: Revise periodicamente as práticas de criptografia da organização para garantir que estejam alinhadas com as melhores práticas, padrões e evoluções tecnológicas, fazendo atualizações conforme necessário.

4. SECURITY BY DESIGN E PRIVACY BY DESIGN

O desenvolvimento de sistemas é o processo de criação, implementação e manutenção de sistemas de software para atender às necessidades específicas de uma organização. Esse processo demanda a adoção de práticas relacionadas à segurança da informação, especialmente com a crescente quantidade de dados sensíveis e pessoais que são armazenados, processados e transmitidos digitalmente.

Considerando a necessidade premente de construir sistemas que sejam mais seguros e que respeitem integralmente os aspectos relacionados à privacidade e à proteção dos dados pessoais, o *Security by Design* (Segurança desde o início) e o *Privacy by Design* (Privacidade desde o início) emergem como abordagens fundamentais no desenvolvimento de softwares e arquiteturas de sistemas. Ambas as metodologias destacam a importância de incorporar medidas de segurança e privacidade desde as fases iniciais do projeto, em contraposição à sua adição posterior como uma reflexão tardia.

Essa abordagem proativa envolve a consideração meticulosa de aspectos de segurança e privacidade ao longo de todo o ciclo de vida do desenvolvimento do sistema. Desde a coleta de requisitos até o design, implementação, teste, implantação e manutenção contínua, é essencial integrar práticas robustas de segurança e privacidade para garantir a confiabilidade e a proteção adequada dos dados.

Ao adotar o *Security by Design* e o *Privacy by Design*, as organizações se comprometem a implementar sistemas que não apenas atendam aos requisitos funcionais, mas também incorporem camadas robustas de proteção contra ameaças cibernéticas e garantam a preservação da privacidade dos usuários. Essa abordagem pró-ativa não apenas reduz o risco de exposição a vulnerabilidades de segurança e violações de dados, mas também fortalece a confiança dos usuários e clientes na integridade e segurança dos sistemas que utilizam.

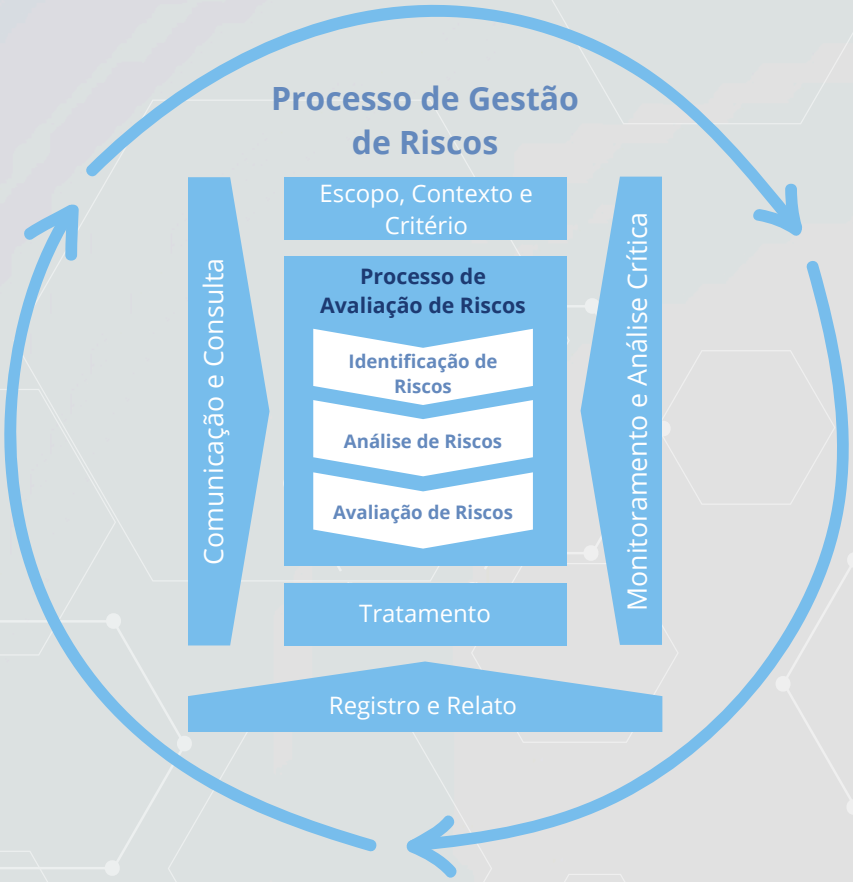
Aqui estão alguns princípios que devem ser observados na adoção dessas práticas:

- **minimizar superfícies de ataque**: limite os recursos que os usuários têm acesso para minimizar as possibilidades de vulnerabilidades e ataques, reduzindo as áreas que podem ser exploradas por potenciais invasores;
- **princípio do menor privilégio**: conceda apenas as permissões e acessos necessários para que os usuários e processos executem suas funções. Isso reduz a exposição de sistemas a possíveis ataques, limitando o acesso a recursos críticos apenas a indivíduos autorizados;
- **princípio da defesa em profundidade:** implementa várias camadas de defesa para mitigar riscos de segurança em diferentes níveis do sistema, ao invés de criar apenas camadas primárias de validação de inputs ou regras de negócio;

- **serviços de terceiros:** cheque e valide os serviços desenvolvidos por terceiros que serão utilizados pelas suas aplicações. Apesar de conveniente, a prática pode criar vulnerabilidades. Então é necessário checar a validade dos dados e restringir suas permissões;
- **testes de segurança regulares**: realize testes regulares de penetração e avaliações de vulnerabilidades para identificar e corrigir possíveis pontos fracos no sistema;
- **minimização de dados**: colete e retenha apenas a quantidade mínima de dados pessoais necessária para um propósito específico e limitar o acesso a esses dados a indivíduos ou processos autorizados;
- **privacidade como configuração padrão:** garanta que as proteções de privacidade sejam automaticamente incorporadas aos sistemas, produtos e serviços por padrão, exigindo esforço mínimo dos indivíduos para manter sua privacidade;
- **respeito pela privacidade do usuário**: Empoderar os usuários com controle sobre suas próprias informações pessoais, respeitando suas preferências de privacidade e consentimento;
- **funcionalidade total da privacidade:** Garanta que medidas de privacidade não comprometam a funcionalidade ou a usabilidade do sistema, mantendo um equilíbrio entre privacidade e usabilidade.

5. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

O processo de gestão de riscos é definido como a aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco (ABNT NBR ISO/IEC 31000:2018).



No que se refere à proteção de dados pessoais, o processo de gestão de riscos de segurança da informação é fundamental para identificar, avaliar e mitigar ameaças à segurança dos dados e dos sistemas de uma organização.

Aqui estão os passos essenciais envolvidos na gestão de riscos de segurança da informação.

- **identificação dos ativos de informação**: identifique e documente todos os ativos de informação da organização, incluindo dados, sistemas, redes, dispositivos e aplicativos;
- **avaliação de ameaças e vulnerabilidades**: Identifique as ameaças potenciais que podem afetar os ativos de informação, bem como as vulnerabilidades que podem ser exploradas por essas ameaças;
- **análise de riscos**: avalie a probabilidade e o impacto das ameaças identificadas, combinadas com as vulnerabilidades dos ativos de informação, para determinar os riscos à segurança da informação;
- **priorização dos riscos:** priorize os riscos identificados com base na sua gravidade e impacto potencial na organização, para que os recursos possam ser alocados de forma eficaz para mitigar os riscos mais críticos;

- **estratégias de mitigação**: implemente estratégias de mitigação de riscos para reduzir a probabilidade e o impacto das ameaças à segurança da informação, incluindo medidas técnicas, procedimentais e organizacionais, além dos controles de segurança adequados para proteger os ativos de informação da organização contra ameaças identificadas, incluindo firewalls, antivírus, criptografia, políticas de acesso, entre outros;
- **monitoramento e revisão contínua**: monitore continuamente a eficácia dos controles de segurança implementados e revisar regularmente o processo de gestão de riscos para garantir que os riscos sejam mantidos em um nível aceitável;

6. CONSIDERAÇÕES FINAIS

A segurança da informação é um aspecto fundamental em nosso mundo digital, especialmente quando se trata da proteção de dados pessoais. Este guia orientativo foi desenvolvido com o objetivo de fornecer boas práticas e medidas técnicas relacionadas à segurança da informação com foco na proteção dos dados pessoais.

Ao longo deste guia, abordamos uma variedade de tópicos relacionados à segurança da informação, considerando a necessidade de implementação de medidas técnicas e operacionais com foco na proteção dos dados pessoais. Destaca-se a importância de proteger os dados pessoais contra acessos não autorizados, uso indevido e violações de segurança, bem como a necessidade de conformidade com regulamentações e requisitos legais relevantes.

A proteção de dados pessoais é uma responsabilidade compartilhada por todos os membros das organizações. Portanto, é fundamental que haja plena compreensão da importância da segurança da informação e um comprometimento em seguir as melhores práticas recomendadas neste guia.

7. REFERÊNCIAS

Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados;

Norma ABNT NBR ISO/IEC 27000 Princípios e Vocabulário, define a nomenclatura utilizada nas normas seguintes da família 27000;

Norma ABNT NBR ISO/IEC 27001 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos;

Norma ABNT NBR ISO/IEC 27002 Tecnologia da informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação;

Norma ABNT NBR ISO/IEC 31000:2018 Gestão de Riscos

Conaci

CONSELHO NACIONAL DE CONTROLE INTERNO

Câmara Técnica sobre a Lei Geral de Proteção de Dados Pessoais
Conselho Nacional de Controle Interno (Conaci)