Política de Segurança da Informação

Proteção de Dados

Elaborado por: Ingrid Martinez – Governança Corporativa - Data: 16/08/2024 - Nº da Revisão: 01

www.digix.com.br

1 – Objetivo

A Política de Segurança da Informação e proteção de dados tem por objetivo estabelecer as regras e orientações bases para a utilização segura e ética dos recursos tecnológicos da Digix, seguindo as normativas da Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018) e demais legislações aplicáveis, visando a proteção dos dados pessoais dos seus colaboradores, clientes e demais envolvidos, considerando todo o ciclo de vida da informação, desde a coleta até a sua efetiva eliminação ou anonimização, independente do meio que foi coletada, seja digital ou no papel.

Além disso, busca atingir os seguintes objetivos específicos:

- Proteger a integridade, disponibilidade e confidencialidade dos dados.
- Promover a transparência no tratamento de dados pessoais.
- Estabelecer responsabilidades claras para a gestão de dados e segurança da informação.

Desta forma, assumimos nosso respeito à privacidade de todas as pessoas e demonstramos que estamos comprometidos em proteger essas informações, mantendo a confidencialidade, disponibilidade e integridade da melhor forma possível, sempre preservando a transparência, autenticidade e auditabilidade dessas informações tão necessárias para a realização do negócio da Digix.

2 – Abrangência

Deve ser cumprida por todos os integrantes da Digix que venham ter acesso a dados pessoais, sensíveis e/ou recursos tecnológicos da Digix.

3 – Princípios

- Transparência: Garantir que os titulares de dados sejam informados sobre como seus dados são coletados, utilizados e protegidos.
- Segurança: Implementar medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, perdas ou danos.
- Responsabilidade: Definir claramente as responsabilidades de todos os colaboradores em relação à proteção e gestão dos dados.
- Minimização de Dados: Coletar e processar apenas os dados necessários para as finalidades específicas.

4 – Conceitos Básicos

Para efeitos de entendimento e fácil compreensão desta política, serão apresentados as definições legais e conceitos que serão utilizados no decorrer do documento:

- Agentes de tratamento: corresponde ao Controlador e Operador em conjunto. Não são considerados controladores ou operadores os indivíduos subordinados, tais como os

colaboradores ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento;

- Anonimização: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- Ataque: evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;
- Autoridade Nacional de Proteção de Dados (ANPD): é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;
- *Bot*: código malicioso o qual permite que o invasor controle remotamente o computador ou dispositivo que hospeda;
- Categoria de dados pessoais: classificação dos dados pessoais de acordo com o contexto de sua utilização, tais como dados de identificação pessoal, dados de autenticação em sistemas, dados financeiros;
- Comunicação de incidente de segurança: ato do controlador que comunica à ANPD e ao titular de dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares;
- Controlador: é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;
- Criptografia: é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.
- Dados pessoais sensíveis: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
- Dados pessoais: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, por conta própria ou quando combinada com outras informações;
- Dado de autenticação em sistemas: de acordo com a ANPD, é qualquer dado pessoal utilizado como credencial para determinar o acesso a um sistema ou para confirmar a identificação de um usuário, como contas de login, tokens e senhas;
- Dado pessoal afetado: de acordo com a ANPD, é o dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em um incidente de segurança;
- Dados protegidos por sigilo legal ou judicial: de acordo com a ANPD, é o dado pessoal cujo sigilo decorra de norma jurídica ou decisão judicial;
- Dado protegido por sigilo profissional: de acordo com a ANPD, é o dado pessoal cujo sigilo decorra do exercício de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem;

- Dispositivo móvel: Entende-se qualquer equipamento eletrônico com atribuições de mobilidade, como: notebooks, smartphones e tablets.
- Encarregado de Dados ou Data Privacy Officer (DPO): pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
- Engenharia social: técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados;
- Expurgo de dados: significa destruição segura e definitiva de informações, ou seja, quando os dados não existem mais ou não podem mais ser acessados pelo Controlador de qualquer forma;
- Incidente: evento, ação ou omissão que tenha permitido ou possa vir a permitir acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou, ainda, apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação.
- Incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.
- Incidente de segurança com dados pessoais: de acordo com a ANPD, incidente de segurança à proteção de dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração, vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares de dados pessoais;
- Incidente com dados em larga escala: de acordo com a ANPD, incidente com dados em larga escala é aquele que abranger número significativo de titulares, considerando, ainda, o volume de dados envolvidos, bem como a duração, a frequência e a extensão geográfica de localização dos titulares;
- IP: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;
- Integrantes: todas as pessoas que trabalham na DIGIX, inclusive gestores, diretores, CEO, colaboradores, estagiários, trainees e jovens aprendizes;
- *Log:* processo de registro de eventos relevantes num sistema computacional;
- *Malware:* é um termo genérico para qualquer tipo de "malicious software" ("software malicioso") projetado para se infiltrar em dispositivos eletrônicos sem o devido conhecimento do usuário. Existem muitos tipos de malware, e cada um funciona de maneira diferente na busca de seus objetivos;
- Medidas de segurança: de acordo com a ANPD, medidas técnicas e/ou administrativas adotadas para proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

- Natureza dos dados pessoais: de acordo com a ANPD, classificação de dados pessoais em gerais ou sensíveis;
- Operador: é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador;
- Porta: uma porta de conexão está sempre associada a um endereço IP de um host e ao tipo de protocolo de transporte utilizado para a comunicação;
- Procedimento de apuração de incidente de segurança: de acordo com a ANPD, é o procedimento instaurado pela ANPD para apurar a ocorrência de incidente de segurança que não tenha sido comunicado pelo controlador;
- Procedimento de comunicação de incidente de segurança: de acordo com a ANPD, é o procedimento instaurado no âmbito da ANPD após o recebimento de comunicação de incidente de segurança;
- Processo de comunicação de incidente de segurança: de acordo com a ANPD, processo administrativo instaurado no âmbito da ANPD que abrange o procedimento de apuração incidente de segurança e o procedimento de comunicação de incidente de segurança;
- Recursos tecnológicos: São todos os recursos físicos e digitais utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar informações. Entre os tipos de recursos podemos destacar: computares de mesa ou portáteis, smartphones, tablets, pen drive, discos externos, mídias, impressoras, scanner, entre outros.
- Relatório de tratamento de incidente: de acordo com a ANPD, é o documento fornecido pelo controlador que contém cópias, em meio físico ou digital, de dados e informações relevantes para descrever o incidente e as providências adotadas para reverter ou mitigar os seus efeitos;
- Relatório final: relatório que contenha todas as evidências e ações realizadas para tratamento do incidente e que deve ser emitido ao final das tratativas;
- Relatório de Impacto a Proteção de Dados (RIPD): conforme a LGPD, o RIPD é uma documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que tem o potencial de gerar riscos às liberdades civis e aos direitos fundamentais dos titulares, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
- *Scripts*: conjunto de instruções para que uma função seja executada em determinado aplicativo;
- Sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados pela Digix para dar suporte na execução de suas atividades;
- *Sniffing*: corresponde ao roubo ou interceptação de dados capturando o tráfego de rede usando um *sniffer* (aplicativo destinado a capturar pacotes de rede);
- *Spam*: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para muitas pessoas;
- *Spyware*: programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;

- Tratamento: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação, organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;
- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
- Transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
- Uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
- Vazamento de dados: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;
- Violação de privacidade: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento;
- Vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;
- *Worm*: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador.

5 – Responsabilidades

- Presidente e Diretoria: Aprovar e apoiar a implementação da Política de Segurança da Informação e Proteção de Dados (PSIPD).
- Encarregado de Proteção de Dados (DPO): Garantir a conformidade com a LGPD e atuar como ponto de contato entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- Operações de TI: Implementar e monitorar as práticas de segurança da informação e proteção de dados em suas respectivas áreas.
- Integrantes: Seguir as diretrizes estabelecidas na política e participar de treinamentos sobre proteção de dados.

6 – Diretrizes Gerais

6.1. Governança e Gestão de Dados

- Nomeação do Encarregado de Proteção de Dados (DPO): A indicação deve ser realizada por ato formal (documento escrito, datado e assinado) do agente de tratamento do qual

constem as formas de atuação e as atividades a serem desempenhadas. Nas ausências, impedimentos e vacâncias do encarregado, a função será exercida por substituto formalmente designado.

- Governança de Dados: Definir claramente como os dados são coletados, armazenados, processados e descartados, garantindo a transparência e a responsabilidade.
- Privacy by Design/Default: incorporação de Privacidade, ou seja, integrar a privacidade e a proteção de dados desde a concepção de novos projetos, produtos ou serviços.

6.2. Mapeamento de Dados

- Identificação e Classificação: Realizar um mapeamento detalhado dos dados pessoais que a Digix coleta, armazena e processa. Classificar os dados de acordo com sua sensibilidade e importância.
- Registro das Operações de Tratamento: Documentação detalhada, mantendo registros detalhados de todas as operações de tratamento de dados, incluindo a base legal e a finalidade de cada operação.

6.3. Relatório de Impacto à Proteção de Dados Pessoais

- Avaliação de Impacto: Elaborar, quando cabível, relatórios de impacto à proteção de dados pessoais para identificar e mitigar riscos associados ao tratamento de dados, conforme orienta o guia para Relatório de Impacto à Proteção de Dados (RIPD) da Digix.

6.4. Anonimização de Dados

- Redução de Riscos: Sempre que possível, anonimizar dados pessoais para reduzir os riscos associados ao tratamento de dados sensíveis.

6.5. Conformidade e Auditoria

- Auditorias Regulares: Conduzir auditorias internas e externas para garantir a conformidade contínua com a LGPD.
- Relatórios de Conformidade: Manter registros detalhados das atividades de tratamento de dados e das medidas de segurança implementadas.

7 – Diretrizes Específicas

7.1. Segurança da Informação

- Controle de Acesso: Implementar controles rigorosos para garantir que apenas pessoas autorizadas tenham acesso aos dados pessoais e/ou sensíveis.
- Criptografia: Utilizar criptografia para proteger dados em trânsito e em repouso.
- *Backup* e Recuperação de Dados: Estabelecer procedimentos regulares de backup e planos de recuperação de desastres.

- Atualizações e *Patches*: Manter todos os sistemas e softwares atualizados com os patches de segurança mais recentes.
- Antivírus e Antimalware: Utilizar soluções robustas de antivírus e antimalware para proteger os sistemas contra ameaças.

7.2. Medidas Técnicas e Administrativas

- Segurança Física: Garantir que os locais onde os dados são armazenados fisicamente sejam seguros.
- Monitoramento e *Log*: Implementar sistemas de monitoramento e registro de atividades para detectar e responder a atividades suspeitas.
- Auditorias e Revisões: Conduzir auditorias regulares e revisões de segurança para identificar e corrigir possíveis falhas ou vulnerabilidades.
- Monitoramento de Atividades: Implementar sistemas de monitoramento contínuo para detectar atividades suspeitas e responder rapidamente a incidentes de segurança.

7.3. Gestão de Riscos

- Avaliação de Riscos: Realizar avaliações periódicas de riscos para identificar e mitigar possíveis ameaças à segurança da informação.
- Plano de Resposta a Incidentes (PRI): Desenvolver e testar regularmente um plano de resposta a incidentes de segurança, conforme orientações regulamentadas no plano da Digix. O incidente de segurança que acarretar risco ou dano relevante aos titulares, afetando significativamente seus interesses e direitos fundamentais devem ser comunicados à ANPD e ao titular, nos moldes estabelecidos no PRI da Digix.

7.4. Treinamento, Educação e Conscientização

- Capacitação dos Integrantes: Oferecer treinamentos regulares sobre segurança da informação e proteção de dados.
- Cultura de Segurança: Promover uma cultura organizacional que valorize a segurança da informação e a proteção de dados.
- Campanhas de Conscientização: Realizar campanhas regulares de conscientização sobre a importância da proteção de dados pessoais e as melhores práticas de segurança.
- Treinamentos Específicos: Oferecer treinamentos específicos para diferentes departamentos, abordando as particularidades de cada área em relação à proteção de dados.

7.5. Direitos dos Titulares de Dados

- Transparência: Informar claramente aos titulares sobre como seus dados são utilizados e garantir que eles possam exercer seus direitos, como acesso, correção e exclusão de dados.
- Consentimento: Obter consentimento explícito dos titulares para o tratamento de seus dados pessoais, quando necessário.

- Facilidade de Acesso: Implementar processos eficientes para que os titulares de dados possam exercer seus direitos, como acesso, correção, exclusão e portabilidade de dados.

7.6. Escolha de Parceiros Confiáveis

- Avaliação de Terceiros: Selecionar parceiros e fornecedores que também estejam comprometidos com a proteção de dados e que cumpram com a LGPD. Monitorar o tratamento de dados por terceiros.
- Contratos com terceiros: Incluir cláusulas de proteção de dados nos contratos.

7.7. Notificação de Incidentes

- Comunicação de Violações: Notificar, conforme exigido em lei, a ANPD e os titulares de dados sobre qualquer violação de segurança que possa resultar em risco ou dano significativo.

7.8. Compartilhamento de Dados

- Compartilhamento Interno: Limitar o compartilhamento de dados pessoais aos colaboradores que necessitam de acesso.
- Compartilhamento Externo: Compartilhar dados com terceiros apenas mediante consentimento ou quando exigido por lei. Manter registros detalhados de todas as transferências de dados pessoais para terceiros. Implementar controles de acesso para restringir quem pode visualizar, modificar ou transferir dados pessoais. Configurar os sistemas e bancos de dados para permitir apenas o acesso autorizado.

8 - Conclusão

A implementação de uma Política de Segurança da Informação e Proteção de Dados robusta é essencial para garantir a proteção dos dados pessoais e a conformidade com a LGPD e demais legislações aplicáveis. Todos os colaboradores têm um papel fundamental na proteção e gestão dos dados, promovendo uma cultura de segurança e responsabilidade dentro da Digix.

9 - Nosso contato

Se você tiver dúvidas ou preocupações em relação à sua privacidade ou ao tratamento de seus dados pessoais pela Digix, entre em contato com a nossa Encarregada de Dados – Ingrid Roberta Martinez, através do e-mail lgpd@digix.com.br.

Telefone: +55 (67) 3345-6500

E-mail: lgpd@digix.com.br

10 – Revisões à política

Eventualmente poderemos fazer alterações nesta "Política de Segurança da Informação e Proteção de Dados". Se fizermos qualquer alteração substancial nesta política e à maneira como tratamos os dados pessoais, publicaremos essas alterações. Consulte também a nossa "Política de Privacidade" regularmente.

Controle de alterações

Revisão	Data publicação	Descrição
00	06/08/2020	Versão Inicial
01	16/08/2024	Versão revisada e atualizada para alteração do título e adequação à legislação aplicável.