METODOLOGIA DE AUDITORIA DE CONFORMIDADE COM A LGPD

JUNHO 2022

Equipe Técnica do Grupo ADX

Adriano Lima Head de Projetos	**Adgenison Nascimento** Head de Negócios
Hendrick Arcanjo Consultor de Tecnologia	**Gessica Alcântara** Gestora de Projetos
Lavínia França Analista de Processos	**Saulo Santos** Advogado

Histórico de revisões			
Versão	**Data**	**Autor**	**Descrição**
1.0	20/06/2021	Grupo ADX	Elaboração do documento

SUMÁRIO

ÍNDICE DE FIGURAS

1 – INTRODUÇÃO

A Lei Geral de Proteção de Dados (LGPD) – Lei 13.709, foi sancionada em agosto de 2018, e trata dos direitos à privacidade e uso de dados pelas organizações brasileiras, sejam públicas ou privadas. Na prática, a lei define regras para coleta e a utilização dos diferentes tipos de dados dos usuários, seja em meios físicos ou digitais. O objetivo é impedir o uso indevido das informações coletadas prejudicando a privacidade da pessoa natural.

2 – OBJETIVO

O objetivo deste documento é definir a metodologia de auditoria de conformidade à LGPD, no âmbito do SENAC AL, para atender às exigências legais previstas na Lei Geral de Proteção de Dados (LGPD), no tocante a gestão de segurança da informação e privacidade.

3 – CONCEITOS IMPORTANTES

- **AUDITORIA** - Auditoria é um exame cuidadoso e sistemático das atividades desenvolvidas em determinada empresa, cujo objetivo é averiguar se elas estão de acordo com as planejadas e/ou estabelecidas previamente, se foram implementadas com eficácia e adequadas à consecução dos objetivos.
- **ANÁLISE DE RISCOS** - uso sistemático de informações para identificar fontes e estimar o risco;
- **ATIVOS DE INFORMAÇÃO -** os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;
- **AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD)** - órgão da APF responsável por zelar, implementar e fiscalizar o cumprimento da Lei 13.709, de 14 de agosto de 2018;

- de um sistema;
- **AVALIAÇÃO DE RISCOS** - processo de comparar o risco estimado com critérios de risco predefinidos para determinar a importância do risco.
- **CONTROLES DE SEGURANÇA** - medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções de hash, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros;
- **DADO PESSOAL** - informação relacionada a pessoa natural identificada ou identificável;
- **DADO PESSOAL SENSÍVEL** - dado pessoal sobre 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;
- **ENCARREGADO DE PROTEÇÃO DE DADOS (DPO)** - pessoa indicada pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados;
- **POLÍTICA DE GESTÃO DE RISCOS** - declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de risco;
- **POLÍTICA DE SEGURANÇA DA INFORMAÇÃO** - documento aprovado pela autoridade responsável pelo órgão ou entidade da APF, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da SI (Este termo substituiu o termo Política de Segurança da Informação e Comunicações);
- **TRATAMENTO DA INFORMAÇÃO** - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
- **VAZAMENTO DE DADOS** - transmissão não-autorizada de dados de dentro de uma organização para um destino ou recipiente externo. O termo pode ser usado para descrever dados que são transferidos eletronicamente ou fisicamente. Pode ocorrer de forma acidental ou intencional (pela ação de agentes internos, pela ação de agentes externos ou pelo uso de software malicioso).

4 – O que é uma auditoria e para que ela serve

O conceito genérico de auditoria relaciona-se com o exame das operações, processos, sistemas e responsabilidades gerenciais de uma entidade ou organização com o propósito de verificar a sua conformidade com os objetivos e políticas organizacionais, orçamentos, normas ou padrões. O termo auditoria, historicamente, esteve vinculado quase que exclusivamente ao campo contábil. Contudo, diversos autores têm um ponto de vista mais amplo e argumentam que ela engloba toda a organização, estendendo seu campo de ação com a comunidade: clientes, fornecedores, instituições públicas e privadas com as quais a empresa se relaciona.

Auditoria é a análise de todas as atividades desenvolvidas por uma empresa de pequeno, médio ou grande porte, que tem como objetivo verificar se as ações dessas organizações estão conforme planejadas por elas, ou se estão de acordo com as normas estabelecidas pelo Governo por Lei. Existem dois tipos de auditoria: Interna e externa.

Auditoria interna é realizada pelos colaboradores da própria empresa e examina a adequação e a eficácia dos controles internos e das informações contábeis, financeiras e operacionais da corporação.

O objetivo é de garantir um maior valor para as operações realizadas pela companhia, ajudando a atingir resultados e metas através de uma abordagem sistemática, como também de concluir sobre a qualidade dos registros e a segurança destes.

O auditor interno não deve estar subordinado aos departamentos que examinarem, deverá ser independente prestar informações apenas aos gestores que o destinarem a execução das atividades.

Vale ressaltar que mesmo sendo funcionário da empresa, é necessário existir imparcialidade do colaborador, serem livres de tendência e conflitos de interesse. Os auditores devem assegurar que as constatações e conclusões de auditoria sejam baseadas somente nas evidências encontradas.

Auditoria externa conhecida também como auditoria independente é executada por outras organizações, por pessoas externas à companhia.

A diferença é a total imparcialidade do auditor com a organização auditada, visto que a auditoria independente atende também aos interesses de investidores, instituições bancárias e ao próprio governo.

O processo de auditoria tem como objetivo examinar de forma transparente se as informações disponibilizadas pela entidade estão de acordo com o que foi concedido e de acordo com as normas aplicáveis.

4 – Auditoria de conformidade à LGPD

A auditoria de conformidade à LGPD deve avaliar se todos os processos, controles, documentos e requisitos de segurança da informação, definidos no Sistema de Gestão da Privacidade dos Dados Pessoais (SGPD), estão sendo devidamente utilizados após a fase de implantação do projeto.

Auditorias isoladas e esporádicas são pouco eficazes, além de dispendiosas. O primeiro passo numa auditoria é estabelecer a gestão do projeto que constitui o programa de auditoria. Auditoria é, em geral, um trabalho de equipe, realizado na forma de um projeto, no qual estão envolvidas pessoas, que executarão uma série de atividades técnicas especializadas, produzindo um resultado demandado pela empresa, dentro de prazos, custos e qualidades esperadas. O escopo da auditoria precisa ser bem delimitado, as comunicações entre os membros do “projeto” e com os clientes precisam ser bem organizadas. É necessário fazer monitoramento da ação e tomada de ações corretivas.

O projeto de uma auditoria, como qualquer outro, é sujeito a desvios e riscos, que precisam ser monitorados e controlados visando à produção de resultados com qualidade. É preciso, então, que haja na equipe de auditoria uma pessoa responsável por planejar e gerenciar a atividade definidas em cada ciclo de auditoria.

5 – Como a auditoria deve ser realizada

A auditoria é feita através da coleta de evidências e entrevistas com os colaboradores da empresa. Ela fornecerá informações para a correção de possíveis procedimentos que não estejam em sintonia com os planos e políticas definidos na empresa. Preferencialmente, os colaboradores envolvidos com os itens a serem auditados não devem ter conhecimento prévio do escopo da auditoria.

Um ponto importante a ser levado em consideração é o escopo da auditoria. Certamente será muito difícil auditar do o SGPD de uma única vez. Dessa forma, será preciso dividir o sistema em partes para realizar a auditoria de forma escalonada.

De forma geral, a auditoria deve ser dívida em 5 passos:

1. Definir os objetivos;
2. Planejar a auditoria;
3. Conduzir o trabalho de auditoria;
4. Relatar os resultados;
5. Tomar as ações necessárias para correção dos desvios encontrados.

1 – Definir os objetivos

Trace os objetivos que a equipe de auditoria almeja ao conduzir a auditoria de conformidade à LGPD. Tenha certeza de clarificar o valor de negócio de cada objetivo para que objetivos específicos da auditoria se alinhem com os maiores objetivos da sua empresa.

Use a lista de questões abaixo como um ponto inicial para se ter ideias e refinas a sua própria lista de objetivos para a auditoria.

- ✓ Quais processos, documentos, sistemas, Infraestrutra de TI ou requisitos da lei você deseja auditar?

- ✓ A avaliação será feita pelos requisitos da LGPD ou de outras normas como a ISO 27001 ou 27701?
- ✓ A auditoria comtemplará a validação dos resultados de planos de ações já implementados?

2 – Planejar a auditoria

Um plano bem pensado e organizado é crucial para o sucesso de uma auditoria. Você deverá definir todos os requisitos necessários para a condução do trabalho. Alguns pontos importantes a serem pensados são:

- ✓ Já foi definido o escopo da auditoria com todos os itens a serem auditados?
- ✓ A auditoria será presencial ou remota e em quais setores da empresa ?
- ✓ Se for presencial, será realizada no ambiente de trabalho ou em uma sala reservada?
- ✓ Se for virtual, qual ferramenta será utilizada? Foram agendados testes prévios para validar o funcionamento no dia agendado ?
- ✓ Já foi feita a definição de todos os participantes da equipe de auditoria e dos envolvidos com itens auditados?
- ✓ A agenda de todos os participantes já foi reservada?
- ✓ Será necessária a participação de um membro do setor de TI?
- ✓ Será necessária a participação de um membro do setor de Jurídico?
- ✓ Será necessária a participação de um membro do setor de RH?
- ✓ Será necessária a participação do DPO ?
- ✓ Quais evidências serão solicitadas para cada item a ser auditado?
- ✓ Como os resultados apresentado pelas evidências serão registrados no relatório final?

- ✓ O cronograma da auditoria já foi elaborado?
- ✓ Existe algum problema específico que precisa ser monitorado durante a auditoria ?

3 – Conduzir o trabalho de auditoria

A equipe de auditoria deve conduzi-la de acordo com os planos e metodologias acordados durante a fase de planejamento. Durante este processo, entreviste os colaboradores selecionados, solicite as evidências e registre tudo no relatório da auditoria.

4 – Relatar os resultados

Compile toda a documentação relacionada a auditoria no modelo do relatório final a ser entregue aos responsáveis da empresa. O relatório deve conter todas as não conformidades e sugestões definidas para cada item auditado com uma explicação clara dos riscos que a empresa corre se a correção não for executada rapidamente.

5 - Tomar as ações necessárias para correção dos desvios encontrados.

O relatório final deve conter uma sessão específica para os planos de ação necessários para correção dos itens não conformes. Esses planos devem ter um responsável e uma data limite para execução negociada com todos os envolvidos e a diretoria.

5 – Fontes de informações para análise dos itens a serem auditados

Uma das grande dificuldades do processo de auditoria é definir quais itens serão avaliados e quais evidências serão utilizadas para validar a conformidade com os requisitos da LGPD. Para facilitar o planejamento do processo de auditoria sem algumas dicas importantes.

5.1 Auditoria de processos – A auditoria de processos deve ter como fonte de validação o inventário de dados elaborado durante o diagnóstico para a LGPD, as suas bases legais e os controles definidos. No plano de gestão de riscos criado no documento final do projeto de adequação existem vários controles definidos para cada processo mapeado. Uma grande fonte para as evidencias é validar se cada controle definido foi implementado e se ainda está sendo seguido após o projeto de adequação. **A Figura 1** mostra um exemplo da relação entre os processos, seus riscos e os controles propostos.

Nome do processo	Risco	Probabilidade	Impacto	Criticidade	Estratégia	Controle
GFI 04 - Pagar NF ou fatura de pessoa jurídica.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de documentos em via física	1	1	1	Mitigar	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Recebimento de documentos por meio digital [Organizacional]
CEP GT E UPS 01 - Gerenciar documentos enviados ao RH	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel	2	2	4	Mitigar	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]

Figura 1 - Plano de Gestão de Riscos.

Além do plano de gestão de gestão de riscos, outra fonte importante para a auditoria dos processos é o plano de ações gerado na fase de diagnóstico.

5.2 Auditoria de segurança da informação – A auditoria de segurança da informação deve ter como fonte de validação algumas normas e frameworks internacionalmente conhecidos. Alguns exemplos são:

- **Norma ABNT NBR ISO 27001:2013** – Tecnologia da Informação – Técnicas de Segurança.
- **Norma ABNT NBR ISO 27002:2013** – Tecnologia da Informação – Técnicas de Segurança;
- **Norma ABNT NBR ISO 27005:2011** – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação;
- **Norma ABNT NBR ISO 27701:2019** – Técnicas de Segurança – Extensão da ABNT ISO/IEC 27001;
- **Norma ABNT NBR ISO 29134:2017** – Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade – Diretrizes;
- **Norma ABNT NBR ISO 29151:2017** – Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais

- **CIS Controls®** - Os controles CIS são um conjunto de práticas recomendadas de segurança cibernética e ações defensivas que ajudam a evitar os principais ataques da atualidade. Os Controles CIS fornecem orientação específica e um caminho claro para que as organizações atinjam os objetivos e metas descritos por várias estruturas legais, regulamentares e políticas. São um conjunto de 20 controles tecnológicos e de processos, que ajudam a estruturar os fundamentos para seu programa de segurança de informações e a base para toda a sua estratégia de segurança. para mais detalhes acesse: https://www.cisecurity.org/controls.
- **NIST** - O framework de segurança cibernética NIST, também chamado em inglês de NIST Cyber Security Framework, fornece uma estrutura, com base nos padrões, diretrizes e práticas existentes para organizações do setor privado nos Estados Unidos, a fim de gerenciar e reduzir melhor o risco de segurança cibernética. Além de ajudar as organizações a prevenir, detectar e

responder a ameaças cibernéticas e ataques cibernéticos, ele foi projetado para melhorar as comunicações de segurança cibernética e gerenciamento de riscos entre as partes interessadas internas e externas. Para mais detalhes acesse: https://www.nist.gov/cyberframework.

- **MITRE ATT & CK®** - É uma base de conhecimento globalmente acessível de táticas e técnicas adversárias com base em observações do mundo real. A base de conhecimento da ATT & CK é usada como base para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de segurança cibernética. Para mais informações acesse: https://attack.mitre.org/.

Além dos frameworks sugeridos, outra fonte importante para a auditoria dos processos é o plano de ações gerado na fase de diagnóstico.

Auditoria jurídica – Como a ANPD está trabalhando continuamente no detalhamento do conteúdo da LGPD, é de se esperar que novas exigências sejam publicadas frequentemente. Cada novo requisito definido pela lei precisa ser implementado e inserido nos ciclos de auditoria de conformidade da LGPD. Todas as alterações da LGPD podem ser acompanhadas diretamente no site da ANPD: https://www.gov.br/anpd/pt-br.

Além do plano do acompanhamento das modificações da LGPD, outra fonte importante para a auditoria dos processos é o plano de ações gerado na fase de diagnóstico.

5 – PROCESSO DE AUDITORIA DO SGPD

O processo de auditoria do SGPD pode ser visto na **Figura 2**.

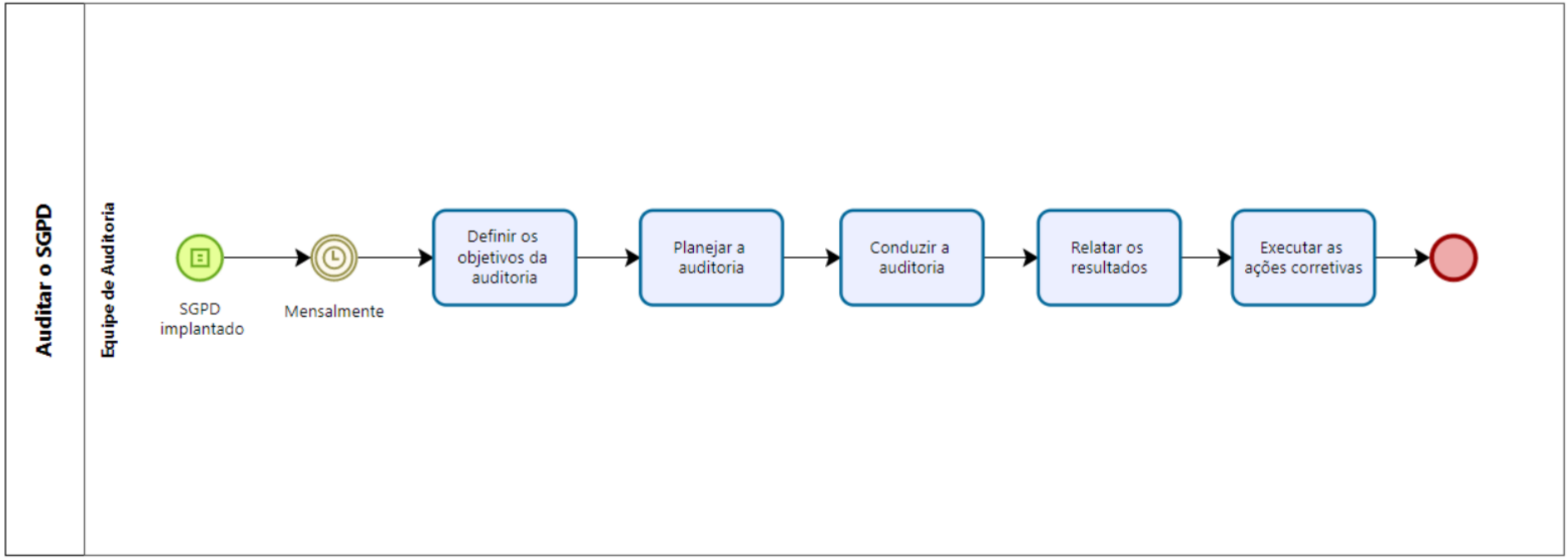

Figura 2- Processo de auditoria do SGPD.

8 CONCLUSÃO

O processo de auditoria do SGPD é essencial para a manutenção do funcionamento do programa de privacidade criado para a empresa.

É importante observar que atividades de auditorias só são possíveis se a organização estiver preparada. Para serem auditadas, as organizações devem criar mecanismos que registrem eventos relevantes e diversos que acontecem no dia a dia de cada setor da empresa.

Fica aqui a ressalva de que controle excessivo pode prejudicar o dia a dia das organizações tornando as atividades reféns desse mesmo controle que pretende qualificar o resultado dessas tarefas. Existe a percepção que uma boa parte do tempo útil dos agentes organizacionais é dedicada a preparar registros que se adequem ao Controle. Mas isso tem um alto custo e pode prejudicar a produtividade e motivação dos colaboradores.

Para termos uma auditoria eficiente, é preciso priorizar os processos que tratam dados pessoais mais importantes da empresa, garantindo dessa forma a minimização dos riscos e aumenta do valor da empresa para seus clientes internos e externos.

9 REFERÊNCIAS

- Lei nº 13.709 – Lei Geral de Proteção de Dados;
- Norma ABNT NBR ISO 19011 - Diretrizes para auditorias de sistema de gestão da qualidade e/ou ambiental.
- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes;
- Norma ABNT NBR ISO 27001:2013 – Tecnologia da Informação – Técnicas de Segurança;
- Norma ABNT NBR ISO 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de Riscos de Segurança da Informação;
- Norma ABNT NBR ISO 27701:2019 – Técnicas de Segurança – Extensão da ABNT ISSO/IEC 27001;
- Norma ABNT NBR ISO 27002:2013 – Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação;
- Norma ABNT NBR ISO 29134:2017 – Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade – Diretrizes;
- Norma ABNT NBR ISO 29151:2017 – Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais
- Guias Operacionais da LGPD do Governo Brasileiro;