Normativa para Auditorias Periódicas e Avaliação de Conformidade.

1. Frequência e Escopo das Auditorias

- **Auditorias Semestrais**: Realizar auditorias semestrais para avaliar a conformidade com a LGPD e políticas internas de proteção de dados. Essa auditoria deve incluir uma análise detalhada dos fatores de risco internos e externos, como ambientais, tecnológicos, sociais e econômicos, que podem impactar a proteção de dados e a segurança da informação.
- **Auditorias Adicionais**: Além das auditorias semestrais, realizar auditorias adicionais sempre que houver mudanças substanciais nos processos de tratamento de dados ou quando novos riscos surgirem, como eventos críticos que ultrapassam o apetite ao risco da organização.
- **Escopo**: O escopo das auditorias deve abranger todos os processos de coleta, armazenamento, compartilhamento e descarte de dados pessoais, além de uma análise dos portfólios de riscos corporativos, com foco nos planos de resposta e contingência implementados para mitigar riscos identificados. A auditoria deve também avaliar a conformidade com os pilares de confidencialidade, integridade, disponibilidade e autenticidade.

2. Diretrizes e Critérios de Auditoria

- **Avaliação de Políticas e Procedimentos:** As auditorias devem avaliar as políticas internas e procedimentos de proteção de dados para assegurar que estejam em conformidade com a LGPD. Isso inclui a análise de práticas documentadas de mitigação de riscos e a verificação da transparência dos processos perante os titulares de dados.
- **Diretrizes:** Estabelecer diretrizes claras para a condução de auditorias periódicas que incluam a **análise documental**, **entrevistas com colaboradores-chave**, e a **verificação dos sistemas de controle interno** para assegurar que as práticas de tratamento de dados estejam em conformidade com a LGPD e outras regulamentações aplicáveis.
- **Monitoramento Contínuo**: Deve haver uma **avaliação contínua de conformidade** com a LGPD e outras regulamentações aplicáveis, utilizando ferramentas de monitoramento para acompanhar o impacto dos tratamentos de dados e o progresso dos planos de ação corretivos.

3. Etapas e Documentação de Auditoria

- **Documentação:** Documentar o ciclo de vida dos dados, incluindo a coleta, o armazenamento, a utilização e a exclusão de dados pessoais.
- **Testes:** Realizar testes de vulnerabilidade e riscos e implementar melhorias para proteger os dados contra vazamentos.
- **RIPD:** Formalizar um Relatório de Impacto à Proteção de Dados Pessoais, avaliando as implicações do tratamento de dados e sugerindo ações corretivas.

4. Principais Ferramentas e Procedimentos de Auditoria

- **Mapeamento:** Mapeamento de dados e análise de risco, identificando onde os dados estão armazenados e quem os acessa.
- **Relatórios e métricas de conformidade**: Verificar periodicamente o cumprimento das políticas de dados.
- **Treinamento:** Promover conscientização para funcionários públicos, assegurando que estejam cientes das obrigações da LGPD.

5. Critérios para Avaliação de Conformidade

- **Princípio da Minimização**: Verificar se os dados coletados estão estritamente alinhados ao princípio da minimização, avaliando se o escopo da coleta é compatível com as finalidades declaradas e se a política de retenção de dados está sendo seguida corretamente.
- **Bases Legais**: Além de garantir que as bases legais para o tratamento de dados estão adequadas, a auditoria deve verificar se os planos de resposta e contingência aos riscos estão devidamente implementados, principalmente para riscos críticos de conformidade.
- **Direitos dos Titulares**: A auditoria deve assegurar que os direitos dos titulares, como acesso, correção, eliminação e portabilidade dos dados, estão devidamente implementados e que os titulares são informados de maneira clara sobre o tratamento de seus dados.
- **Revisão das Políticas de Privacidade**: Revisar periodicamente as **políticas de privacidade**, práticas de **consentimento**, **mecanismos de transparência** e **segurança da informação** para garantir que estejam em conformidade com as exigências regulatórias. Essa revisão deve incluir uma avaliação detalhada das práticas de consentimento e da necessidade de proporcionalidade no tratamento dos dados.
- **Áreas Críticas**: Identificar e priorizar a auditoria em **áreas críticas**, como setores que lidam com dados sensíveis ou realizam operações de tratamento de alto risco, garantindo que esses setores tenham controles adequados e conformidade com a legislação vigente.

6. Obrigações Gerais de Conformidade

- **Transparência:** Transparência com os titulares dos dados, esclarecendo o uso, a finalidade e os processos de tratamento de dados pessoais.
- **Segurança da informação**: Adotar medidas técnicas e administrativas para proteger os dados.
- **Controles:** Controle de acesso e restrições, especialmente em dados sensíveis.

7. Responsabilidades e Registros

- **Designação de Proprietários dos Riscos**: Cada risco identificado deve ter um proprietário do risco designado, responsável pelo monitoramento contínuo e pela implementação das medidas corretivas. Esses proprietários devem reportar regularmente qualquer mudança na probabilidade, impacto e severidade dos riscos sob sua responsabilidade.
- **Registros Detalhados**: Manter um histórico completo dos riscos identificados, das ações corretivas realizadas e dos resultados das auditorias. Esses registros devem incluir a matriz de severidade dos riscos, que considera tanto a probabilidade quanto o impacto dos riscos, e os planos de resposta e contingência que foram adotados.
- **Relatórios Periódicos**: As auditorias devem gerar **relatórios periódicos** contendo uma **descrição das atividades auditadas**, os **resultados da auditoria**, **recomendações** para ajustes e melhorias, e um **plano de ação** para mitigar riscos identificados e corrigir as não conformidades encontradas.

8. Plano de Ação Corretiva

- **Desenvolvimento de Planos Corretivos**: Após cada auditoria, um plano de ação corretiva deve ser desenvolvido para mitigar os riscos identificados. Esses planos devem incluir ações específicas para tratar riscos residuais e inerentes, garantindo que o impacto e a probabilidade de ocorrência sejam reduzidos.
- **Auditorias de Acompanhamento**: Implementar auditorias de acompanhamento para verificar a eficácia das ações corretivas e dos planos de resposta. Essas auditorias devem garantir que os planos estão sendo executados conforme o planejado e que os riscos estão sendo mitigados de forma eficaz.
- **Medidas de Mitigação de Riscos**: As ações corretivas devem ser acompanhadas de medidas de mitigação dos riscos identificados, especialmente aqueles que afetam os direitos dos titulares e podem resultar em danos físicos, materiais ou morais.

9. Metodologia de Avaliação de Riscos

- **Avaliação de Riscos**: Adotar uma metodologia de avaliação de riscos baseada em uma matriz de probabilidade e impacto, categorizando os riscos em níveis de baixa, moderada, alta e extrema severidade. Essa avaliação deve considerar tanto fatores internos quanto externos que possam impactar a organização.
- **Categorização de Riscos**: Os riscos identificados devem ser categorizados em diferentes níveis de severidade, e qualquer risco que ultrapasse o apetite ao risco da organização deve ser tratado com prioridade máxima. A categorização deve abranger riscos estratégicos, operacionais, de conformidade, tecnológicos e ambientais.
- **Avaliação Contínua e Proporcionalidade**: Deve-se realizar uma **avaliação contínua do impacto** das operações de tratamento de dados, especialmente aquelas que apresentam maiores riscos. Essa avaliação deve assegurar que o tratamento de dados é **proporcional** à necessidade e que não há excessos na coleta e armazenamento de informações pessoais.
- **Identificação de Riscos e Impacto**: Além disso, é necessário realizar a **identificação dos riscos** associados ao tratamento de dados e a **avaliação da probabilidade e impacto** desses riscos, assegurando que os controles apropriados estejam em vigor para mitigar os efeitos adversos.

10. Matriz de Riscos e Monitoramento Contínuo

- **Matriz de Riscos**: Utilizar uma matriz de riscos que combine a probabilidade e o impacto de cada risco identificado, permitindo uma visão clara de quais riscos demandam atenção imediata e quais podem ser monitorados com menos urgência.
- **Monitoramento Contínuo**: O monitoramento dos riscos deve ser realizado de maneira contínua, com relatórios trimestrais sobre o andamento das ações corretivas, a efetividade dos planos de resposta e o desempenho dos controles implementados. O acompanhamento deve ser feito de acordo com a matriz de severidade e priorização de riscos.
- **Ferramentas de Monitoramento**: A conformidade com a LGPD deve ser monitorada continuamente utilizando **ferramentas tecnológicas**, que permitam uma análise em tempo real do tratamento de dados e dos riscos associados.