

Corrigir: Questionário - Avaliação de Mapeamento

Entrevistado

2

Caroline Monteiro de França

29:17

Tempo para
concluir

Informações Gerais

1. Nome do processo

Pontua / 0 pontos

Auditoria Interna

2. Descrição do processo

Pontua / 0 pontos

Anualmente, a AI elabora o plano de auditoria interna da Excelsior com as áreas e processos que serão auditados. Adicionalmente ao plano de auditoria, também surgem demandas da alta administração, para se analisar um processo específico. Ou seja, as auditorias podem ser programadas ou requeridas extraordinariamente pela presidência. Além disso, podem haver auditorias para analisar a conformidade dos processos às Circulares da SUSEP. A AI estuda as áreas a serem auditadas e monta o planejamento de testes e solicitação de documentações a ser enviada para as áreas (solicitação vai com cópia ao gestor da área). Existe a análise dos contextos interno e externo para garantir conformidade dos processos e verificar se estão sendo executados da melhor forma possível, com posterior produção de relatório conclusivo. Na análise do contexto interno, analisam-se os documentos solicitados à área que está sendo auditada. Os documentos podem ter natureza diversa, sendo que os mais comuns são: dossier de sinistro, vistoria, comprovante de pagamento, processos judiciais, documentos da subscrição (proposta, cotação, apólice, endosso, documentos da empresa ou pessoais), notas fiscais. A auditoria interna possui, portanto, um amplo acesso a uma gama inestimável de dados, porém com uma finalidade estritamente restrita. A partir dos dados analisados, é produzido um relatório, o qual é compartilhado com o gestor da área e com a presidência. No relatório produzido, não existem dados pessoais. Em relação a áreas que são executadas por terceiros, existe a auditoria, mas só se analisam documentos que a Excelsior já possui.

3. Responsável pelo processo

Pontua / 0 pontos

José Alves

4. Departamento ou setor

Pontua / 0 pontos

Auditoria Interna

Informação do tratamento de dados

5. Finalidade do tratamento

Pontua / 0 pontos

Realizar os testes de auditoria em atendimento à RES. CNSP n.º 416/2021

6. Este tratamento de Dados Pessoais é realizado com base no consentimento do titular?

Pontua / 0 pontos

 Não

7. São tratados dados pessoais sensíveis?

Pontua / 0 pontos

 Sim Não

8. São tratados dados de idosos?

Pontua / 0 pontos

 Sim Não

9. São tratados dados de crianças e adolescentes?

Pontua / 0 pontos

 Sim Não

10. Quais são os dados pessoais tratados?

Pontua / 0 pontos

Funcionários: Podem ser recebidas quaisquer informações. Segurado: Todos os dados da apólice/sinistro necessário para o atendimento da demanda. Fornecedores: Podem ser recebida quaisquer informações.

11. Como ocorre a coleta dos dados? Qual a origem dos dados?

Pontua / 0 pontos

Os dados pessoais utilizados no processo de auditoria interna tem origens diversas, mas são dados que a empresa já possuía para a finalidade do processo que está sendo auditado. Via: E-mail/Teams.

12. Qual o volume de dados afetados?

Pontua / 0 pontos

 1mil - 10mil

13. Quais são os países que usam o processo?

Pontua / 0 pontos

 Brasil

14. Qual o volume de dados afetados?

Pontua / 0 pontos

 1mil-10mil

15. Onde ocorre o armazenamento dos dados?

Pontua / 0 pontos

 Sharepoint, Teams, E-mail, Canva.

Informação de Compartilhamento Interno

16. Há compartilhamento interno? (Destino)

Pontua / 0 pontos

- Sim
 Não

17. Com quais setores os dados são compartilhados?

Pontua / 0 pontos

O relatório pode ser compartilhado com presidência e responsável da área que está sendo auditada.

18. Finalidade do compartilhamento

Pontua / 0 pontos

Para mostrar o resultado da auditoria.

Informações de Compartilhamento Externo

19. Há compartilhamento Externo?

Pontua / 0 pontos

- Sim
 Não

20. Partes que acessam/usam os dados externamente (Fornecedores)

Pontua / 0 pontos

Microsoft e Canva.

21. Método de compartilhamento Externo

Pontua / 0 pontos

Armazenamento nos sistemas.

22. Finalidade do Compartilhamento (externamente)

Pontua / 0 pontos

Para elaborar os testes de auditoria

23. Existem Entidades Governamentais relacionados a esta Atividade de Tratamento?

Pontua / 0 pontos

Sim. SUSEP

24. Há transferência internacional de dados pessoais?

Pontua / 0 pontos

- Sim
 Não

25. Finalidade de tratamento para transferência internacional

Pontua / 0 pontos

N/A

Ativos relacionados

26. Quais são os ativos/sistemas relacionados ao processo?

Pontua / 0 pontos

E-mail, Excel, Teams, Canva.

Segurança dos dados

27. Você tem conhecimento se existe tomada de decisão automatizada

Pontua / 0 pontos

neste processo? *Uma decisão automatizada é caracterizada como um ato decisório realizado por meio de mapeamento de perfis, mediante qualquer forma de tratamento automatizado de dados pessoais, para avaliar aspectos pessoais relativos a uma pessoa.

 Sim Não

Retenção e Descarte

28. Quais os documentos tratados/elaborados nessa atividade?

Pontua / 0 pontos

1. Documentos diversos solicitados pela AI à área que está sendo auditada; 2. Relatórios conclusivos produzidos pela AI (sem dados pessoais).

29. Existe prazo legal ou regulatório de retenção?

Pontua / 0 pontos

 Sim Não

30. Informar prazo de retenção

Pontua / 0 pontos

5 anos - prazo da SUSEP

31. Formas de descarte

Pontua / 0 pontos

A ser definida.

Atividades de tratamento relacionadas

32. Cite atividades de tratamento relacionadas

Pontua / 0 pontos

N/A

Riscos

33. Detalhe os riscos encontrado na atividade de tratamento.

Pontua / 0 pontos

A ser definido.

Equipe de Privacidade

34. Qual a base legal usada para tratamento dos Dados Pessoais Comuns?

Pontua / 0 pontos

- Consentimento;
- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres;
- Realização de estudos por órgão de pesquisa;
- Execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;
- Exercício regular de direitos em processo judicial, administrativo ou arbitral;
- Proteção da vida ou da incolumidade física do titular ou de terceiro;
- Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Atender aos interesses legítimos do controlador ou de terceiro
- Proteção do crédito

35. Qual a base legal usada para tratamento dos Dados Pessoais Sensíveis?

Pontua / 0 pontos

- Cumprimento de obrigação legal ou regulatória pelo controlador;
- Realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
- Exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral
- Proteção da vida ou da incolumidade física do titular ou de terceiro;
- Tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;
- Garantia da prevenção à fraude e à segurança do titular

36. Medidas de Segurança preeexistentes

Pontua / 0 pontos

Restrições de acesso. Senhas de acesso. Autenticação multifator.