Adiantado dia 11/11/2025

Semana 32 - Aula 01

Tópico Principal da Aula: Auditoria e Monitoramento de Conformidade com a LGPD: Introdução e Mapeamento de Dados

Subtítulo/Tema Específico: Implementação da Auditoria e Monitoramento (Etapas Essenciais)

Código da aula: [SIS]ANO1C2B4S32A1

Objetivos da Aula:

- Compreender a auditoria e o monitoramento de conformidade com a LGPD.
- Implementar o mapeamento dos dados pessoais na organização.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Introdução ao tema (Slide 06) - Implementar a auditoria e monitoramento de conformidade com a LGPD

- **Definição:** A implementação da **auditoria** e do **monitoramento de conformidade** com a Lei Geral de Proteção de Dados (**LGPD**) é uma etapa crucial para garantir que a organização mantenha-se em aderência às regulamentações de proteção de dados pessoais. É o ciclo de vida que sucede a adequação inicial, focando na sustentação.
- **Aprofundamento/Complemento:** A LGPD exige medidas contínuas de segurança e *compliance*. A auditoria é um exame periódico que valida o status de conformidade em um momento específico, enquanto o monitoramento é um processo contínuo e proativo, focado na detecção em tempo real de eventos suspeitos.
- **Exemplo Prático:** A empresa precisa de uma auditoria externa anual para o relatório de transparência (auditoria). Em paralelo, mantém ferramentas de **SIEM** (Security Information and Event Management) ligadas 24 horas por dia para identificar acessos indevidos aos bancos de dados (monitoramento).
    - Link de vídeo 1: Mapeamento de Dados para LGPD

Referência do Slide: Slide 07 - Mapeamento de Dados

- **Definição:** O **Mapeamento de Dados (Data Mapping)** é o processo de identificação e documentação de todos os dados pessoais que a organização coleta, armazena e processa.
- **Aprofundamento/Complemento:** Esta atividade é a fundação do programa de governança em privacidade. Ela envolve responder a perguntas-chave como: **Quais**

dados (RG, nome, e-mail)? **Onde** estão (servidor, nuvem, papel)? **Com que Finalidade** (marketing, recrutamento)? **Qual a Base Legal** para o tratamento? E **Quem** tem acesso?

- **Exemplo Prático:** Uma equipe de TI mapeia o sistema de *backup* e descobre que ele está retendo dados de clientes inativos há 10 anos. O mapeamento revela uma violação do princípio da **limitação da retenção**, permitindo a criação de uma política de descarte imediato.
    - Link de vídeo 1: Como fazer o MAPEAMENTO DE DADOS de acordo com a LGPD?

Referência do Slide: Slide 09 - Avaliação de riscos

- **Definição:** A **Avaliação de Riscos de Privacidade** identifica e analisa potenciais vulnerabilidades e ameaças à segurança e integridade dos dados, permitindo que a empresa priorize as ações de mitigação.
- **Aprofundamento/Complemento:** O processo não foca apenas em riscos de segurança (vazamento), mas também em riscos de *compliance* (uso indevido de base legal). Classifica-se o risco pela matriz de impacto (financeiro, reputacional, legal) versus probabilidade (frequência).
- **Exemplo Prático:** Risco: O sistema legado de atendimento ao cliente não possui autenticação de dois fatores. A avaliação classifica este risco como **Alto Impacto** e **Média Probabilidade**, levando à recomendação imediata de implementação de MFA para todos os usuários.

Referência do Slide: Slide 11 - Implementação de controles de segurança

- **Definição:** Implementação de medidas técnicas e administrativas para proteger os dados pessoais contra uso indevido, acesso não autorizado e violações de segurança.
- **Aprofundamento/Complemento:** No contexto técnico, os controles incluem a **Criptografia** (em repouso e em trânsito), o **Controle de Acesso Baseado em Função (RBAC)** e o uso de **Firewalls** e sistemas de **Monitoramento de Rede**.
- **Exemplo Prático:** O departamento de desenvolvimento só tem permissão para acessar dados anonimizados para testes (RBAC). Se um desenvolvedor tentar acessar dados pessoais de produção, o controle de acesso nega a solicitação e o sistema de monitoramento registra a tentativa de violação.

(Demais Tópicos da Aula 1: Treinamento, Auditorias Regulares, Monitoramento Contínuo, Registro de Atividades e Resposta a Incidentes, são abordados em detalhes nas aulas seguintes e resumem a necessidade de uma gestão contínua dos temas.)

Roteiro: Semana 32 - Aula 02

Semana 32 - Aula 02

Tópico Principal da Aula: Auditoria e Monitoramento de Conformidade com a LGPD: Processo de Auditoria sobre o Mapeamento de Dados

Subtítulo/Tema Específico: Implementação da Auditoria sobre o Mapeamento de Dados Pessoais

Código da aula: [SIS]ANO1C2B4S32A2

Objetivos da Aula:

- Implementar a auditoria sobre o mapeamento de dados pessoais.
- Compreender as etapas de um processo de auditoria de dados.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slides 06 a 10 - Passos da Auditoria sobre o Mapeamento de Dados

- **Definição:** A **Auditoria sobre o Mapeamento de Dados Pessoais** é uma avaliação detalhada do documento de *Data Mapping* para assegurar sua precisão, completude e conformidade legal com a LGPD.
- **Aprofundamento/Complemento:** O processo é metodológico e essencial para a melhoria contínua (*Plan-Do-Check-Act*), focando em validar as informações registradas com a realidade operacional.
    - **Passo 1: Planejamento:** Define o escopo, cronograma e a equipe de auditores.
    - **Passo 2: Revisão da Documentação:** Analisa se políticas, termos de consentimento e procedimentos de segurança estão completos, precisos e atualizados.
    - **Passo 3: Entrevistas:** Conversas com os operadores e controladores (equipes de RH, Vendas, TI) para entender como o processo de tratamento de dados realmente ocorre.
    - **Passo 4: Teste de Amostragem:** Seleciona-se aleatoriamente uma fonte de dados para comparar a informação documentada no mapeamento com os dados reais armazenados e processados (validação técnica).
    - **Passo 5: Avaliação da Conformidade Legal:** Confirma se o tratamento de dados (bases legais, finalidades) está em total aderência à LGPD.
- **Exemplo Prático:** Durante o **Teste de Amostragem**, a auditoria revisa o banco de dados de clientes e encontra uma coluna de "anotações pessoais" sem finalidade legal. No **Relatório de Auditoria** (Passo 7), é registrada uma **Lacuna** (Passo 6), recomendando a eliminação imediata da coluna, pois o dado não tem base legal para existir.
    - Link de vídeo 1: LGPD - Auditoria de Dados

Roteiro: Semana 32 - Aula 03

Semana 32 - Aula 03

Tópico Principal da Aula: Auditoria e Monitoramento de Conformidade com a LGPD: Programa de Monitoramento Contínuo

Subtítulo/Tema Específico: Implementação de um Programa de Monitoramento Contínuo

Código da aula: [SIS]ANO1C2B4S32A3

Objetivos da Aula:

- Implementar um programa de monitoramento contínuo para detecção de ameaças.
- Conhecer as ferramentas e procedimentos para monitoramento de segurança.

Recursos Adicionais (Sugestão, pode ser adaptado):

- Caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slides 07 a 11 - Etapas do Programa de Monitoramento Contínuo

- **Definição:** O **Programa de Monitoramento Contínuo** é um sistema de vigilância ativa essencial para garantir a segurança dos dados e identificar possíveis ameaças de forma **antecipada**.
- **Aprofundamento/Complemento:** O monitoramento é a espinha dorsal da segurança moderna.
    - **Seleção de Ferramentas:** Envolve a escolha de tecnologias como **SIEM** (Security Information and Event Management), que centraliza e analisa logs de segurança; e ferramentas de **Análise Comportamental** para identificar padrões atípicos de uso por parte de usuários ou sistemas.
    - **Configuração e Implementação:** Envolve a definição de **políticas de alerta** – o que é um evento "normal" e o que é uma anomalia que deve disparar um alarme.
    - **Monitoramento e Análise:** Acompanhamento constante dos logs, tráfego de rede e atividades dos usuários em busca de desvios.
    - **Resposta a Incidentes:** O monitoramento deve estar diretamente ligado a um **Plano de Resposta a Incidentes (PRI)**, permitindo que a equipe de segurança aja rapidamente para conter a ameaça detectada.
    - **Avaliação e Ajuste:** O programa deve ser regularmente revisado para se adaptar a novas ameaças e garantir a eficácia.
- **Exemplo Prático:** O SIEM (Ferramenta) detecta 500 tentativas de login de um funcionário fora do horário de trabalho (Comportamento Anômalo) vindas de um país diferente. O sistema dispara um **alerta crítico**, e a equipe de Resposta a Incidentes bloqueia imediatamente a conta do usuário antes que qualquer dado seja comprometido.
    - Link de vídeo 1: Implementação da LGPD - Aula 1

- Link de vídeo 2: Webinar - Como Preencher o Mapeamento de Dados da LGPD