Olá, aluno(a)!
Seja bem-vindo(a) à aula interativa!

Você entrará na reunião com a câmera e o microfone desligados.

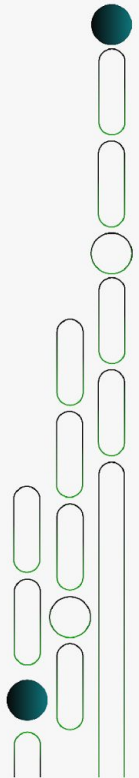
Sua presença será computada através da enquete.
Fique atento(a) e não deixe de respondê-la!

XPe
Aprenda com quem faz

> Serviços de Armazenamento, Banco de Dados e Analytics

Segunda Aula Interativa

Prof. Marcelo Maffra



Proteção de dados

- Prevenção de perda de dados.
  - Introdução;
  - Plano de proteção de perda de dados;
- Soluções de segurança para proteger as suas informações sensíveis.
- AWS Well-Architected Framework – Pilar de Segurança.

Proteção de dados

Introdução

- Os dados de uma empresa são extremamente importantes, logo, a perda de dados é uma preocupação constante para as equipes de TI e para os executivos. A perda de dados pode se dar por uma variedade de causas, desde falhas de hardware até o vazamento de dados feitos de dentro da empresa por um funcionário com intenções maliciosas ou hackers.

Proteção de dados

- As consequências de perda de dados também podem variar bastante. Os processos cruciais do negócio podem ser facilmente interrompidos e ter um dos seus documentos críticos acabando nas mãos dos seus competidores pode ter efeitos devastadores. A empresa também pode sofrer com multas dos compliances e a perda de confiança dos clientes. Todos esses fatores podem afetar negativamente a receita, até o ponto de colocar a empresa fora dos negócios.

Proteção de dados

- Para minimizar esses riscos, toda empresa deve ter um plano de prevenção de perda de dados (DLP – Data Lost Prevention) que assegura os dados críticos.

Proteção de dados

Plano de prevenção de perda de dados

- Uma das muitas soluções para a prevenção de perdas de dados.
- A prevenção de perda de dados efetiva requer uma aproximação mais ampla. É importante ter ciência de que apenas um software não é suficiente para um bom programa de prevenção de perda de dados.
- Os dados que você está tentando proteger são muito importantes e o potencial prejuízo das perdas seriam muito severas. Vejamos algumas práticas recomendadas para a criação de um programa verdadeiramente efetivo de prevenção de perda de dados.

Proteção de dados

Plano de prevenção de perda de dados

- **Aprovação de orçamento da alta gestão e/ou dos executivos da organização**: primeiramente, garanta a aprovação dos heads de todos os departamentos e divisões que podem ser impactadas. O suporte deles será necessário para o sucesso do programa.

Proteção de dados

Plano de prevenção de perda de dados

- **Identifique e classifique seus dados críticos**: fazer a distinção dos seus dados críticos e não críticos é provavelmente o passo mais importante na criação de programa de prevenção de perda de dados. A seguir, estão alguns dos tipos de dados que você possa ter que identificar.

Proteção de dados

Plano de prevenção de perda de dados

- Propriedade intelectual, documentos legais, documentos de planos estratégicos, dados de vendas, informação dos clientes, informação pessoal, dados de Marketing e previsões, documentos de operações, registros financeiros, dados de recursos humanos, dados governamentais, senhas e outros dados de TI, dados sujeitos a quaisquer regulações de compliance.

Proteção de dados

Plano de prevenção de perda de dados

- **Identifique as ameaças e os riscos**: monitore a atividade através dos dados críticos, incluindo quem os acessa e o que eles faz com eles. Identifique quaisquer ameaças à segurança de cada parte dos dados. Quais vulnerabilidades estarão presente durante o ciclo de vida dos dados? Quem é o responsável pela segurança de dados? O responsável tem as ferramentas necessárias para protegê-los? Documente o que pode acontecer em caso de perda de dados. Tenha certeza de considerar tanto o impacto direto do negócio e as penalidades dos compliances.

Proteção de dados

Plano de prevenção de perda de dados

- **Defina os seus objetivos**: especifique os objetivos que você espera atingir no programa de prevenção de perda de dados, como:
  - Identificar os riscos e encontrar uma forma de endereçá-los;
  - Garantir a segurança dos dados, em uso e dos arquivados;
  - Manter os dados disponíveis para uso sem aumentar o risco de exposição;
  - Padronizar procedimentos para a segurança, privacidade e compliance.

Proteção de dados

Plano de prevenção de perda de dados

- **Crie procedimentos passo-a-passo**: estabeleça procedimentos e políticas para armazenar e manusear dados críticos, assim como detalhar planos de resposta para o vazamento de dados e outros incidentes de segurança. Veja algumas das melhores práticas para um manuseio seguro dos dados críticos e sensíveis.

Proteção de dados

Plano de prevenção de perda de dados

- **Pessoas**
  - Não deixar os dados sensíveis isolados
  - Não permitir a cópia de dados sensíveis para dispositivos removíveis
  - Dê acesso apenas para leitura de informações sensíveis
  - Incorpore cláusulas de proteção de dados nos contratos

Proteção de dados

Plano de prevenção de perda de dados

- **Gerenciamento**
  - Implemente um ciclo de vida do gerenciamento de dados para organizá-los e gerenciar seu uso e armazenamento;
  - Atualize os perfis de riscos de dados regularmente para se manter atualizado de possíveis novas ameaças;
  - Identifique locais com potencial para vazamento de informação sensível;

Proteção de dados

Plano de prevenção de perda de dados

- **Gerenciamento**
  - Padronize os endpoints para que a implementação seja mais gerenciável;
  - Documente os incidentes de DLP (Data Lost Prevention);
  - Faça uma auditoria periódica na empresa para os compliances.

Proteção de dados

Plano de prevenção de perda de dados

- **Implementação (1/2)**
  - Faça a implementação da DLP em ondas (primeiro as áreas com maior risco, ou implementar as políticas em fases etc.);
  - Divida as tomadas de decisões e a implementações da solução em fases. Comece com uma base pequena para que você consiga cuidar dos falsos positivos, ajude a identificar os dados sensíveis e críticos e faça ajustes na política de DLP.

Proteção de dados

Plano de prevenção de perda de dados

- **Implementação (2/2)**
  - Teste a implementação em uma unidade pequena antes de implementá-la em todo o ambiente;
  - Garanta a segurança dos documentos (como criptografar os dados antes de transportá-los e armazená-los na nuvem);
  - Repita o processo de descobrimento e de ajustes para proteger a informação e estabelecer controles que possam ser entendidos por todas as partes interessadas e usuários do sistema.

Proteção de dados

Plano de prevenção de perda de dados

- **Controles restritivos da TI**
  - Não permitir dispositivos não autorizados na rede;
  - Bloqueie as conexões wireless;
  - Bloqueie arquivos que contenham informação pessoal identificável;
  - Desabilite todos os burners de CD/DVD;

Proteção de dados

Plano de prevenção de perda de dados

- **Controles restritivos da TI**
  - Faça com que todos os dispositivos USB sejam apenas para leitura exceto dispositivos autorizados.
  - Faça o escaneamento de descobrimento da DLP em uma frequência desejada (ou sob demanda) para auditar e manter a sob controle o status da segurança.

Proteção de dados

Plano de prevenção de perda de dados

- **Seleção do produto**
  - Cheque os produtos de DLP e veja se eles suportam os formatos dos dados da empresa;
  - Escaneie os dados armazenados em busca de informações sensíveis e, se necessário, tome ações para remediar riscos;

Proteção de dados

Plano de prevenção de perda de dados

- **Seleção do produto**
  - Use a ferramenta de DLP para encontrar automaticamente dados sensíveis não criptografados, criptografar a informação e remover a informação ou remediá-la de acordo com as políticas da empresa;
  - Selecione um produto que tenha relatórios de todas as violações da política de DLP.

Proteção de dados

Plano de prevenção de perda de dados

- **Avalie os sistemas disponíveis atualmente**: Considere se os seus hardwares e softwares podem atingir os seus objetivos com a DLP. Lembre-se que a maioria dos sistemas de proteção de dados não podem classificar os dados de forma consistente e precisa. Se os seus sistemas atuais são insuficientes, considere outras soluções, mantendo tanto seus objetivos quanto suas análises de custo e risco em mente. Quais funcionalidades você precisa e o quanto elas valem a pena pra você?

Proteção de dados

Plano de prevenção de perda de dados

- **Eduque todo mundo**: É importante construir uma cultura com a organização sobre a importância de programa de DLP. Inclua informações sobre:
  - O que constitui dados críticos;
  - Como os dados críticos devem ser manuseados em certas situações, incluindo e-mail e uso da internet;
  - Quais leis a empresa precisa cumprir.

Proteção de dados

Plano de prevenção de perda de dados

- Adapte o treinamento às necessidades dos diferentes grupos de funcionários, e repita o treinamento regularmente. Tenha certeza de periodicamente testar os seus usuários e faça acompanhamento dos indivíduos que não seguirem com os procedimentos corretos.

Proteção de dados

Soluções de segurança para proteger as suas informações sensíveis.

- Vazamentos de dados são frequentemente noticiados e as empresas estão cientes de que, mesmo que tenham alcançado conformidade com PCI ou SOX, novos regulamentos como a LGPD e/ou GDPR (General Data Protection Regulation) demandam um controle mais rigoroso da segurança de dados. Para ajudar a aprimorar a sua postura em relação a segurança e ao compliance, vamos falar sobre algumas das principais soluções de segurança de dados para proteger os seus dados sensíveis e te ajudar a ser aprovado nas auditorias.

Proteção de dados

Soluções de segurança para proteger as suas informações sensíveis.

- Descobrimento e classificação de dados;
- Firewall;
- Backup e Recuperação;
- Antivírus;
- Sistemas de Prevenção e Detecção de intrusos (IDS/IPS);
- Gerenciamento e correlação de eventos de segurança (SIEM - Security Information and Event Management);

Proteção de dados

Soluções de segurança para proteger as suas informações sensíveis.

- Prevenção de perda de dados (DLP);
- Controle de acesso;
- Soluções de segurança em cloud;
- Auditoria;
- Criptografia de dados;
- Segurança física.

Proteção de dados

AWS Well-Architected Framework – Pilar de Segurança

- O pilar de segurança descreve como aproveitar as tecnologias de nuvem para proteger dados, sistemas e ativos de uma maneira que possa melhorar sua postura de segurança.
- O documento referenciado no link abaixo fornece orientações detalhadas sobre as melhores práticas para a arquitetura de sistemas confiáveis na AWS.
- https://docs.aws.amazon.com/pt_br/wellarchitected/latest/security-pillar/welcome.html

Conclusão

- Quanto melhor seu programa de prevenção de perda de dados é, mais seguros seus dados estarão. Com isso, você estará melhor preparado para as auditorias de compliance e para prevenção de perda de dados. Este é um dos principais benefícios de um programa de DLP forte.