LIVE AUDITORIA DE SISTEMAS

O que é Auditoria de Sistemas?

Porque Auditoria de Sistema

Definição é a como uma rápida avaliação da eficiência da segurança e da conformidade que dos sistemas que a empresa utiliza, destaque para proteção dos dados.

**Motivos para usar: Quais os objetivos de uma Auditoria de Sistemas?**

Conferencia

Fiscalização analise, mas o

Principal motivo é a segurança da informação.

Integridade dos dados

Mitigação de risco.

Monitorar as atividades.

Proteger os ativos.

Garantir a segurança.

Integridade dos dados.

Oferecer aos clientes confiança que os seus dados estão protegidos.

Evitar incidentes, vazamentos de dados.

Mitigação de riscos.

Manter selos de qualidade.

Verificação se o sistema esta dentro das normas tanto da legislação vigente quanto interna.

Esses objetivos contribuem para a melhora do sistema, da empresa que o desenvolve para o cliente:

**Tipo de Auditorias de Sistemas e de Segurança**

**Auditoria de Conformidade**

Avaliar e garantir a segurança do sistema, protegendo contra ameaças e assegurando a integridade e a confidencialidade e disponibilidade dos dados. Politica internas e externas

**Auditoria de Sistemas Operacionais**

Avalia a segurança e desempenhos dos sistemas utilizados na organização.

**Auditoria de Banco de Dados**

Avalia integridade do BD, eficiência e acesso dentro do Banco

**Auditoria de Redes**

Segurança, eficiência da comunicação da infraestrutura com o hardware, da parte do servidor, a parte de cabeamento, no caso de server local

**Auditoria de Aplicações**

Segurança do software adquirido pelas empresas.

**Auditoria de Gestão de Identidade e Acesso**

Avalia a identidade, autenticação, controle de acesso.

**Auditoria de Incidentes de Segurança**

Investigar e analisar o incidente de segurança, verificar as causas e os impactos colocando as medidas corretivas.

**Auditoria de Privacidade de Dados**

Basicamente LGPD, visa a conformidade das lei e a proteção dos dados, garantido a proteção dos dados

**Auditoria de Segurança Física.**

Avaliam locais de acesso a empresa, ao servidor, é avaliação física da empresa.

**Auditoria de Logs e Monitoramento.**

Avalia os log do sistema.

**Auditoria de Politicas de Backup e Recuperação**

**Auditoria de Vulnerabilidade.**

**Normas de auditoria de sistemas**

São diretrizes e padrões estabelecidos para orientar profissionais na condução de auditorias, garantindo a consistência, qualidade e eficácia desse processo.

Norma é regra.

ISO: **International Organization for Standardization**

Normas, regras que precisam ser compridas para pegar um o selo de acordo com uma normal internacional.

**ISO COMUM:**

ISSO/IEC 27001 – Segurança da Informação

ISSO/IEC 27002 – Código de Prática para Controles de Segurança da Informação;

COBIT (Control Objetives for Information and Related Technologies);

ITIL (Information Technology Infrastructure Library);

ISSO/IEC 20000 – Gestão de Serviçõs de TI;

ISSO/IEC 38500 – Governança de TI;~

**Introdução à metodologia de Auditoria de Sistemas da Informação**

* **Planejamento**

**Escopo/ Objetivos:**

* + Recursos necessário(Carro, pessoas)
  + Identificar o sistema que será auditado
  + Estabelecer metas e critérios de avalição
  + Designar Equipe
* **Coleta de informações**

**Objetivo:** Obter informações como o sistema funciona, o processo, como ele funciona.

* + Revisar documentação existente
  + Verificar as politicas de segurança
  + Procedimentos operacionais que o software passa ou precisa passar
  + Entrevista com os usuários
  + Analisar infraestrutura da empresa
  + Analisar infraestrutura de TI
* **Avaliação de risco**

**Objetivos:** Identificar os risco, uma questão de segurança ou associados aos sistemas que serão auditados

* + Analise de vulnerabilidade, fazendo teste de carga de estresse, teste de vazão.
  + Identificar ame-as potenciais
  + Eficácia e controle existentes
* **Desenvolvimento do plano de Auditoria**

**Criar plano detalhado de como será a Auditoria.**

* + Definir os procedimentos de teste e amostragem
  + Definir critérios de aceitação dos testes
  + Programar as atividades da Auditoria
* **Execução de Auditoria**
  + **Inicio da Auditoria**
  + Realizar os testes que foram planejados na fase anterior e na de avaliação de risco.
  + Avaliar registros de Logs
  + Avaliar Conformidade.
* **Análise de resultados**
  + **Interpretar os resultados dos testes e avaliações**
  + Comprovar se aquilo que foi documentado esta sendo aplicado.
* **Relatório e Comunicação**
  + **Relatório detalhado**
  + **Comunicar os achados**
  + **Recomendar ações que precisam ser feitas**
* **Acompanhamento e Monitoramento.**
  + Verificar o que a empresa diz fazer

**As ferramentas mais conhecidas na Auditoria de Sistemas:**

* ACL
  + Faz o mesmo que o PENTANA porém mais caro.
* IDEA (Interactive Data Extration & Analysis)
* AUDIMATION
* GALILEO
  + Gestão de Risco
  + Documentação e emissão de relatório
  + Controle interno
  + Rápido para detectar falhas
* PENTANA
  + Software de planejamento estratégico
  + Muito Utilizado
  + Monitoramente
  + Controle de Hora
  + Registro de check list
  + Analise de desempenho
  + Plano de Ação
  + Util na área de governaça
  + Controle de risco
  + Legal para adequação de leis
  + Gráficos
  + Relatórios sensíveis ao contexto de tempo real
  + Acesso simultâneo do pessoal da auditoria
  + Importação dos dados da empresa (não são todos os softwares que fazem isso)
  + Dados extraídos em tempo real e em vários formatos

Auditor Auxiliar = Entra como Junior

Auditor principal = Equivalente ao Senior