CBD 0289 - Administração de Recursos e Produtos de Informação

Compliance e Auditoria em Segurança da Informação

Prof. Dr. Pedro Luiz Côrtes – ECA USP
www.pedrocortes.com.br

CBD 0289 - Administração de Recursos e Produtos de Informação

Compliance e Auditoria em Segurança da Informação

Compliance, em segurança da informação, refere-se ao **cumprimento de leis**, **regulamentos**, **diretrizes** e **padrões** estabelecidos por **entidades governamentais**, ou **setores específicos** da indústria ou mesmo **normas internas** da organização.

Essas regras podem abordar a **privacidade dos dados**, **proteção de informações** sensíveis, **gerenciamento de riscos**, segurança cibernética e outras questões relacionadas à proteção de dados.

O objetivo do compliance é garantir que uma organização esteja em conformidade com essas exigências legais e regulatórias, bem como com suas próprias políticas internas de segurança.

Prof. Dr. Pedro Luiz Côrtes – ECA USP
www.pedrocortes.com.br

Compliance e Auditoria em Segurança da Informação

Auditoria em segurança da informação é o processo de **avaliação sistemática e independente** das **políticas**, **controles**, **práticas** e **procedimentos de segurança** de uma organização.

A auditoria é conduzida por **auditores internos ou externos** que possuem **conhecimento especializado** em segurança da informação.

O **objetivo** da auditoria é identificar e **avaliar os riscos de segurança**, analisar a **eficácia dos controles** existentes, **detectar** possíveis **vulnerabilidades** e garantir a **conformidade com os requisitos regulatórios e políticas internas**.

Prof. Dr. Pedro Luiz Côrtes – ECA USP
www.pedrocortes.com.br

Compliance e Auditoria em Segurança da Informação

Processo de Compliance em Segurança da Informação

1. **Avaliação de requisitos legais e regulatórios**: identificar os requisitos legais e regulatórios, incluindo leis de privacidade de dados, regulamentos específicos do setor e diretrizes da própria organização. **Em resumo, quais regras devemos seguir.**

2. **Análise de lacunas**: análise para identificar as lacunas e falhas existentes entre as práticas de segurança atuais da organização e os requisitos de conformidade identificados. **Em resumo, o que devemos fazer mas não estamos fazendo.**

3. **Desenvolvimento de políticas e controles**: Com a análise de lacunas, são desenvolvidas políticas de segurança e controles adequados para atender aos requisitos de conformidade. **Em resumo, o que devemos fazer para nos adequarmos às normas e leis que não estamos seguindo.**

Prof. Dr. Pedro Luiz Côrtes – ECA USP
www.pedrocortes.com.br

Compliance e Auditoria em Segurança da Informação

Processo de Compliance em Segurança da Informação

4. **Implementação e execução:** Políticas e os controles desenvolvidos são implementados em toda a organização. **Em resumo, como executaremos o item nº 3?**

5. **Monitoramento e auditoria:** estabelecer um processo contínuo de monitoramento e auditoria para avaliar a eficácia dos controles de segurança implementados. **Em resumo, como garantir que o item nº 3 está sendo executado?**

6. **Melhoria contínua:** Considerando os resultados da auditoria e do monitoramento, são identificadas áreas que necessitam de melhorias. Ações corretivas são implementadas para fortalecer ainda mais a segurança da informação da organização. Essa etapa é um processo contínuo. **Em resumo, se estamos fazendo tudo certo, é possível fazermos ainda melhor?**

Prof. Dr. Pedro Luiz Côrtes – ECA USP
www.pedrocortes.com.br

Compliance e Auditoria em Segurança da Informação

Processo de Auditoria em Segurança da Informação

1. **Planejamento da auditoria:** definir os objetivos, escopo e abrangência da auditoria. Quais os requisitos legais e normas devem ser atendidos? Quais as áreas serão averiguadas? Quais os sistemas serão analisados?

2. **Coleta de informações:** levantar as informações relevantes sobre os sistemas, políticas, processos e controles de segurança da organização que serão auditados.

3. **Avaliação de riscos:** identificação das ameaças e vulnerabilidades relevantes aos sistemas e processos de segurança da organização. O que pode falhar? Quais as vulnerabilidades?

4. **Testes e procedimentos de auditoria:** execução de testes e procedimentos planejados. Isso pode incluir testes de invasão de vulnerabilidades.

Prof. Dr. Pedro Luiz Côrtes – ECA USP
www.pedrocortes.com.br

Compliance e Auditoria em Segurança da Informação

Processo de Auditoria em Segurança da Informação

5. **Análise de resultados:** verificação dos resultados dos testes efetuados x requisitos legais e normas da organização.

6. **Elaboração de relatório de auditoria:** documento em que as normas e os requisitos legais são documentados.

7. **Acompanhamento e implementação de ações corretivas:** após a conclusão do relatório de auditoria, a organização deve implementar as ações corretivas necessárias para resolver as não conformidades identificadas.

Prof. Dr. Pedro Luiz Côrtes – ECA USP
www.pedrocortes.com.br