Semana 23 - Aula 1

Tópico Principal da Aula: Auditoria e certificação da ISO 27001

Subtítulo/Tema Específico: Introdução à Auditoria ISO 27001

Código da aula: [SIS]ANO1C2B3S23A1

Objetivos da Aula:

- Compreender os processos de auditoria para a ISO 27001.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio.
- Identificar e analisar problemas.
- Agir com curiosidade na resolução de problemas técnicos.
- Desenvolver relacionamento (trabalho em equipe).

Recursos Adicionais (Sugestão, pode ser adaptado):

- Recurso audiovisual para exibição de vídeos e imagens;
- Lápis e caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 07 - Ataques de ransomware estão aumentando

- **Definição:** O ransomware é um tipo de software malicioso que criptografa os arquivos de um sistema, tornando-os inacessíveis, e exige um pagamento, geralmente em criptomoeda, para restaurar o acesso aos dados. Os ataques de ransomware têm crescido em frequência e sofisticação, visando tanto indivíduos quanto grandes organizações.
- **Aprofundamento/Complemento (se necessário):** As motivações comuns por trás dos ataques de ransomware são principalmente financeiras, buscando o lucro através do resgate. Outras motivações podem incluir o roubo de dados para venda ou extorsão, e em alguns casos, motivações políticas ou ideológicas. A crescente interconexão de dispositivos na Internet das Coisas (IoT) aumenta a superfície de ataque, tornando mais dispositivos vulneráveis a serem explorados como pontos de entrada para redes maiores e mais valiosas. O pagamento de resgates, infelizmente, pode incentivar mais ataques, pois demonstra que a tática é lucrativa para os cibercriminosos.
- **Exemplo Prático:** Um grupo de estudantes universitários compartilha um computador sem software de segurança atualizado e sem backup de arquivos. Um dia, o computador é infectado com ransomware, e todos os seus arquivos são criptografados. Os hackers exigem um resgate que os estudantes não podem pagar, resultando na perda de seus trabalhos acadêmicos e dados pessoais. Este exemplo ilustra a importância de backups e softwares de segurança.

Referência do Slide: Slide 09 - Auditoria da ISO 27001

- **Definição:** Uma auditoria da ISO 27001 é uma avaliação independente e sistemática dos processos, controles e práticas de segurança da informação de uma organização. Ela é conduzida por auditores qualificados e credenciados com o objetivo principal de verificar a conformidade com os requisitos da norma e a eficácia dos controles de segurança da informação.
- **Aprofundamento/Complemento (se necessário):** Existem dois tipos principais de auditoria: interna e externa. A auditoria interna é realizada pela própria organização para autoavaliar sua conformidade antes de uma auditoria externa. A auditoria externa é conduzida por uma empresa de certificação independente e credenciada, sendo a responsável por conceder a certificação ISO 27001. A certificação é um reconhecimento formal de que a organização demonstrou conformidade com a norma.
- **Exemplo Prático:** Uma empresa de serviços financeiros, a XYZ, decide buscar a certificação ISO 27001 devido à crescente preocupação com a segurança da informação. Antes da auditoria externa, a XYZ realiza uma auditoria interna para identificar lacunas em seus controles de segurança, como políticas de acesso inconsistentes e falta de monitoramento proativo de ameaças. Essa auditoria interna permite que a empresa resolva essas questões antes da avaliação por um organismo de certificação independente.

Semana 23 - Aula 2

Tópico Principal da Aula: Auditoria e certificação da ISO 27001

Subtítulo/Tema Específico: Processo de Certificação ISO 27001

Código da aula: [SIS]ANO1C2B3S23A2

Objetivos da Aula:

- Compreender os processos de auditoria para a ISO 27001.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio.
- Identificar e analisar problemas.
- Agir com curiosidade na resolução de problemas técnicos.
- Desenvolver relacionamento (trabalho em equipe).

Recursos Adicionais (Sugestão, pode ser adaptado):

- Recurso audiovisual para exibição de vídeos e imagens;
- Lápis e caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 09 - Certificação ISO 27001

- **Definição:** O objetivo da certificação ISO 27001 é fornecer confiança às partes interessadas de que a organização implementou controles eficazes de segurança

da informação para proteger seus ativos e dados. Embora a certificação não impeça ataques cibernéticos, ela ajuda a organização a ter processos e controles robustos para responder e se recuperar de incidentes.

- **Aprofundamento/Complemento (se necessário):** O processo de certificação envolve várias etapas. Primeiramente, a organização se prepara, documentando processos e controles de segurança da informação conforme a ISO 27001. Em seguida, uma auditoria de certificação externa, conduzida por uma empresa credenciada, avalia a conformidade. Esta auditoria se divide em duas fases: a pré-avaliação (Fase 1), que revisa a documentação e identifica lacunas, e a auditoria principal (Fase 2), que é uma avaliação detalhada da conformidade. Após a avaliação e decisão do organismo de certificação, a organização deve manter seus controles e passar por auditorias de monitoramento periódicas para sustentar a certificação.
- **Exemplo Prático:** A subsidiária brasileira da Aker Solutions, mesmo certificada ISO 27001, sofreu um ataque cibernético. No entanto, a certificação ajudou a empresa a gerenciar a crise de forma mais eficaz, pois ela já possuía processos estabelecidos para resposta a incidentes, comunicação com autoridades e recuperação de dados. Isso demonstra que a ISO 27001 foca na resiliência e na capacidade de resposta, não apenas na prevenção.

Semana 23 - Aula 3

Tópico Principal da Aula: Auditoria e certificação da ISO 27001

Subtítulo/Tema Específico: Relação entre ISO 27001 e COBIT 2019

Código da aula: [SIS]ANO1C2B3S23A3

Objetivos da Aula:

- Compreender a relação entre a certificação ISO 27001 e o COBIT 2019.
- Conhecer técnicas de computação e gerenciar dados para soluções em nuvem, parametrizar aplicações e dimensionar de acordo com as necessidades do negócio.
- Identificar e analisar problemas.
- Agir com curiosidade na resolução de problemas técnicos.
- Desenvolver relacionamento (trabalho em equipe).

Recursos Adicionais (Sugestão, pode ser adaptado):

- Recurso audiovisual para exibição de vídeos e imagens;
- Lápis e caderno para anotações;
- Acesso ao laboratório de informática e/ou internet.

Exposição do Conteúdo:

Referência do Slide: Slide 09 - Conceitos-chave do COBIT 2019

- **Definição:** **O COBIT 2019 (Control Objectives for Information and Related Technologies) é um framework de governança e gestão de TI que fornece um**

conjunto abrangente de princípios, práticas e ferramentas para as organizações gerenciarem seus sistemas de informação e tecnologia de forma eficaz. Ele visa alinhar os objetivos de TI com os objetivos de negócios, gerenciar riscos e garantir a conformidade.

- **Aprofundamento/Complemento (se necessário):** Tanto o COBIT 2019 quanto a ISO 27001 buscam promover a eficácia, eficiência, confidencialidade, integridade, disponibilidade e conformidade dos sistemas de informação, focando no alcance dos objetivos de negócio através de práticas de segurança da informação. A ISO 27001 oferece requisitos específicos para um Sistema de Gestão de Segurança da Informação (SGSI), enquanto o COBIT 2019 apresenta um escopo mais amplo de governança de TI. Ambos os frameworks enfatizam a gestão de riscos e podem ser integrados para uma abordagem mais holística. É possível mapear os requisitos da ISO 27001 para os processos e objetivos do COBIT 2019, permitindo sua implementação simultânea.
- **Exemplo Prático:** A Caixa Econômica Federal implementou com sucesso tanto a ISO 27001 quanto o COBIT 2019. Essa integração permitiu ao banco fortalecer sua segurança da informação, aumentar a confiabilidade de sua TI e melhorar a governança organizacional. Ao combinar os frameworks, a Caixa conseguiu uma abordagem mais robusta para proteger seus dados e garantir a continuidade dos negócios.