Auditoria da Informação

Gestão de Sistemas e Redes

Pedro Amaral
30008241@students.ual.pt

Eduardo Araújo
30008290@students.ual.pt

João Lucas
30008215@students.ual.pt

Este trabalho de pesquisa aborda o tema "Auditoria da Informação" em ambientes de computação em nuvem, com ênfase na certificação ISO 27001. O problema identificado reside na necessidade crítica de garantir a Segurança da Informação num contexto de evolução tecnológica acelerada, especialmente em ambientes onde a confidencialidade, integridade e disponibilidade dos dados são essenciais...

Palavras-chave: Auditoria da Informação; ISO 27001; Confidencialidade; Integridade; Disponibilidade; Computação em Nuvem; Segurança da Informação;

I. Dedicatória

Dedicamos este trabalho a todos os Professores e colegas que nos ajudaram a chegar até este momento, tendo nós adquirido todo o conhecimento necessário para ultrapassarmos as várias dificuldades ao longo desta licenciatura.

II. Resumo

Este trabalho de investigação aborda a temática da Auditoria da Informação em ambientes de computação em nuvem, com ênfase na certificação ISO 27001. O problema identificado reside na necessidade crítica de garantir a **Segurança da Informação** num contexto de evolução tecnológica acelerada, especialmente em ambientes de nuvem, onde a [7] confidencialidade, integridade e disponibilidade dos dados são essenciais. A pertinência desta pesquisa é evidenciada pelo crescente uso de serviços em nuvem e pela importância de garantir a **Segurança da Informação** nesse cenário.

III. Lista de Abreviaturas

- **ISO -** International Organization for Standardization
- **IEC -** International Electrotechnical Commission
- **PCI DSS** - Payment Card Industry Data Security Standard
- **GDPR** - General Data Protection Regulation
- **SGSI** - Sistema de Gestão de Segurança da Informação
- **NIST** - National Institute of Standards and Technology
- **RGPD** - Regulamento Geral de Proteção de Dados

IV. Auditoria da Informação

A auditoria da informação é um processo que visa avaliar a estrutura dos sistemas internos de uma organização. O objetivo primordial é assegurar a [7] integridade, confidencialidade, disponibilidade e autenticidade dos dados, garantindo que as práticas e políticas estabelecidas estejam alinhadas com os objetivos estratégicos da organização. Esta área abrange uma análise minuciosa dos sistemas de informação, infraestrutura tecnológica, políticas de segurança, procedimentos operacionais e práticas de gestão de dados. A auditoria da informação é vital para identificar riscos potenciais relacionados com segurança da informação, reduzindo assim a probabilidade de ocorrência de problemas, como acessos não autorizados, perda de dados ou interrupções nos serviços. Além disso, a auditoria da informação frequentemente procura estar de acordo com os padrões e normas reconhecidos internacionalmente de modo a garantir que as práticas de auditoria estejam em conformidade com aquilo que de mais atualizado se pratica. Em resumo, a auditoria da informação desempenha um papel crucial na salvaguarda da integridade e segurança da informação, contribuindo para a tomada de decisões informadas e para a manutenção adequada dos ativos de uma organização.

V. Standards definidos para a auditoria da informação

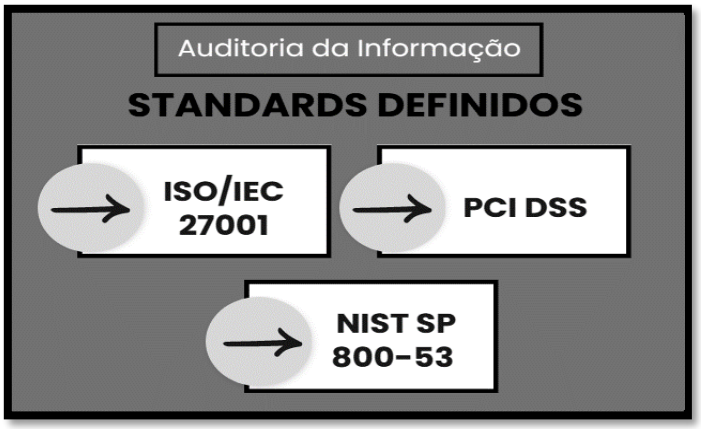
A **ISO/IEC 27001 - Sistema de Gestão de Segurança da Informação** é uma norma internacional que define os requisitos para um SGSI. Esta fornece orientações e práticas recomendadas para a auditoria de Sistemas de Informação, incluindo análise e monitorização de dados.

O **PCI DSS (Payment Card Industry Data Security Standard)** é um conjunto de requisitos de Segurança para organizações que lidam com informações de cartões de

pagamento. Desenvolvido pelo **Conselho de Padrões de Segurança da Indústria de Cartões de Pagamento.**

O **NIST SP 800-53 - Security and Privacy Controls for Federal Information Systems and Organizations** foi publicado pelo National Institute of Standards and Technology (NIST) dos EUA e fornece controlos de Segurança e Privacidade para sistemas de informação.

Estes são apenas alguns exemplos de standards que podem ser usados como referência em auditorias da informação. A escolha do standard depende da indústria, regulamentações aplicáveis e das necessidades específicas de cada organização.



[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes

VI. Processos da Auditoria de Informação

A auditoria da informação é um processo abrangente que compreende várias etapas essenciais para garantir a eficácia no processo de auditar. Desse modo, consideramos abaixo as etapas principais do processo de "**Auditoria da Informação**". O "Planeamento" é a primeira destas etapas de maior importância. Nesta fase, os auditores trabalham em estreita colaboração para definir os objetivos da auditoria, critérios de avaliação e recursos necessários. O plano de auditoria também inclui a identificação de áreas críticas a serem auditadas, avaliação de riscos associados e a definição de métodos e ferramentas a ser utilizadas durante a execução da auditoria. De acordo com a plano estabelecido, a etapa de **"Execução"** visa implementar as atividades já planeadas. Desse modo, os auditores procuram evidências que confirmem os padrões estabelecidos, identificando possíveis vulnerabilidades ou lacunas nos sistemas de segurança. Após a conclusão da fase de análise do sistema, deverão ser feitas as apresentações dos resultados. Estes serão compilados e apresentados em formato de relatório. Este documento deve conter as falhas encontradas e riscos identificados. A clareza e a precisão do relatório são fundamentais, permitindo que sejam tomadas medidas corretivas eficazes. A eficiência deste processo depende da integridade, competência e independência dos auditores, bem como da colaboração estreita com as partes interessadas.

VII. Avaliação de Riscos e Seleção de Áreas Críticas para Auditoria da Informação

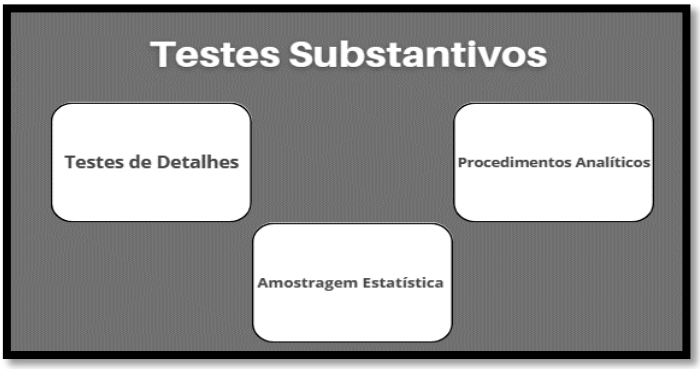
Sobre este capítulo, é essencial referirmos que a avaliação de riscos e a seleção de áreas críticas para auditoria da informação contribuem para um processo mais direcionado. A seleção é baseada na exposição ao risco, na importância estratégica e na criticidade em relação aos objetivos da organização. As áreas críticas deverão ser definidas de acordo com a "Sensibilidade dos dados", "Importância operacional", "Conformidade regulatória" e "Histórico de incidentes**". A avaliação de riscos e a seleção de áreas críticas são elementos fundamentais** para o sucesso da auditoria da informação. Ao adotar uma abordagem criteriosa e estratégica, as organizações podem fortalecer proactivamente as suas defesas contra ameaças à **Segurança da Informação** e garantir a [7] integridade e confidencialidade dos dados críticos.

[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (2)

VIII. Testes Substantivos e Testes de Conformidade

[8] Existem dois tipos principais de testes usados em auditoria, sendo estes os testes substantivos e os testes de conformidade. **Os testes substantivos** visam obter evidências diretas sobre a validade e a precisão dos processos, incluindo estes:

- **Testes de Detalhes**: Análise detalhada de transações de dados que permitem verificar a precisão e integridade dos mesmos;
- **Procedimentos Analíticos**: Análise de variações de dados para verificar anomalias;
- **Amostragem Estatística**: Seleção aleatória de amostras que permitem avaliar a representatividade dos dados.



[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (3)

Os **testes de conformidade** focam na avaliação de políticas, procedimentos e regulamentos estabelecidos, incluindo:

- **Revisões Documentais**: Análise de documentos para verificar a conformidade com políticas internas e externas;
- **Entrevistas e Inquirições**: Diálogo com pessoal-chave para confirmar o entendimento e a aplicação de políticas;
- **Observação**: Verificação visual das práticas operacionais para garantir que estejam em conformidade.

[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (4)

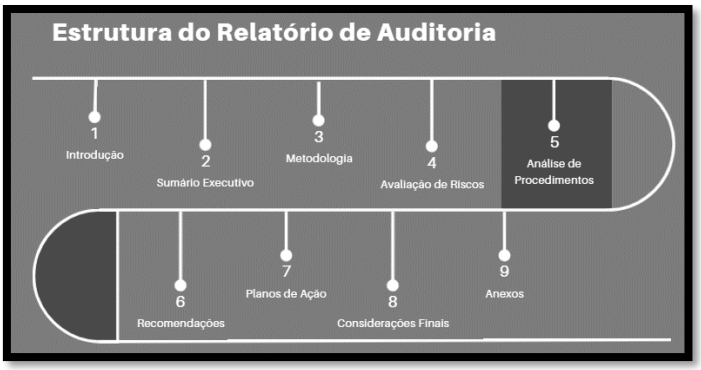
Considerando o **oitavo capítulo deste trabalho** "Testes Substantivos e Testes de Conformidade" em relação à ISO 27001, podemos considerar analisar o seguinte exemplo:

- **Teste Substantivo**: Análise da implementação de controlos de segurança exigidos pela norma;
- **Teste de Conformidade**: Verificação da documentação para garantir que a organização atenda aos requisitos específicos da ISO/IEC 27001.

IX. Estrutura do Relatório de Auditoria

A estrutura de um relatório é fundamental para garantir que as descobertas são compreendidas de maneira clara e que as recomendações sejam implementadas de maneira eficaz. Um tipo de estrutura que pode ser utilizada é o seguinte:

- **Introdução;**
- **Sumário Executivo;**
- **Metodologia;**
- **Avaliação de Riscos;**
- **Análise de Procedimentos;**
- **Recomendações;**
- **Planos de Ação;**
- **Considerações Finais;**
- **Anexos.**



[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (5)

O relatório deverá ser escrito em linguagem simples e prática, evitando termos desnecessários para garantir a compreensão por parte **do público-alvo.** Deverá ser feita a descrição do impacto potencial das falhas na segurança do sistema. Para comprovarmos os problemas encontrados, deverão ser apresentados registos, relatórios e dados específicos. Poderão ser apresentadas soluções, dependendo do serviço prestado. Poderá ser ainda feita a recomendação relativamente à revisão periódica de implementações de melhoria contínua.
Em resumo, a estrutura e o seu conteúdo devem ser cuidadosamente planeados para fornecerem uma visão abrangente dos resultados da auditoria, promovendo continuamente a **Segurança da Informação** na organização.

X. Princípios Éticos e Questões Legais associadas à Auditoria da Informação

A auditoria da informação, ao procurar garantir a segurança e a integridade dos dados, inevitavelmente depara-se com questões éticas e legais que exigem uma abordagem cuidadosa e ponderada. A **"Privacidade"** é uma preocupação no que se refere a auditoria da informação, especialmente em cenários nos quais as organizações lidam com uma quantidade crescente de informações pessoais. A recolha, análise e o processamento dos dados devem estar em conformidade com as regulamentações específicas, como **o Regulamento Geral de Proteção de Dados (RGPD)**. Os auditores precisam de se assegurar que a organização auditada irá proceder de forma adequada em relação à autorização legal dos dados para efeitos de auditoria. Desse modo, devem ser assinados todos os documentos legais necessários destinados ao efeito. Os auditores têm a responsabilidade ética e legal de proteger as informações mais sensíveis, durante o processo de auditoria. Isto inclui a implementação de medidas de segurança estruturadas de modo que apenas o pessoal creditado possa aceder aos resultados da auditoria. Os procedimentos adotados estabelecidos entre a organização auditada e os auditores

devem conter os acordos de **"Confidencialidade"**. Conforme referido anteriormente, os auditores devem aderir a padrões éticos rigorosos, incluindo imparcialidade, integridade e independência. Transparência na comunicação de resultados é também essencial para manter a confiança das partes interessadas. Os auditores deverão ainda permanecer sempre atualizados sobre as mudanças na legislação e nas regulamentações.

XI. TENDÊNCIAS EMERGENTES NA AUDITORIA DA INFORMAÇÃO

O setor da **Segurança da Informação** está em constante evolução à medida que se torna necessário abordar os desafios contemporâneos. Neste contexto, apresentamos três tendências que se destacam:

- A "**Auditoria da Segurança Cibernética**" foi desenvolvida como resposta à crescente ameaça de ataques cibernéticos, com forte potencial de causarem danos às organizações. Esta área encontra-se associada à identificação de vulnerabilidades, conforme referido noutros capítulos. Esta auditoria envolve a análise das políticas de segurança de uma determinada organização, análise do sistema de deteção de intrusões e de testes de penetração. Além disso, a auditoria de segurança cibernética normalmente está alinhada com padrões de segurança reconhecidos, de modo a fornecerem diretrizes sólidas e práticas.

- A "**Auditoria de Dados**" é uma resposta à crescente importância dos dados nas empresas e instituições. Neste tipo de auditoria, os auditores concentram-se na avaliação do conteúdo dos dados, bem como na qualidade dos mesmos. A auditoria dos dados deverá estar alinhada com as regulamentações de forma a serem estabelecidos padrões para a proteção da privacidade.

- À medida que vamos evoluindo tecnologicamente, vamos tornando a "Inteligência Artificial" como parte integrante do nosso trabalho. De modo que a "**Auditoria de Inteligência Artificial**" é considerada uma tendência emergente. Os auditores de IA avaliam os algoritmos, modelos e sistemas de IA para garantir a conformidade dos mesmos. A auditoria de IA também aborda questões éticas como a transparência dos algoritmos. Os auditores devem também conseguir entender como funcionam os métodos e ferramentas específicos de análise deste tipo de algoritmos.

Conforme abordado neste capítulo, as tendências emergentes apresentam novos desafios, com a especialização técnica e uma compreensão mais aprofundada dos diferentes tipos de auditoria. No entanto, também oferecem oportunidades para fortalecer a **Segurança da Informação** e melhorar a qualidade das auditorias.

XII. ISO 27001

[5] A ISO 27001, formalmente conhecida como ISO/IEC 27001, é uma norma internacional que estabelece requisitos e diretrizes para a gestão da **Segurança da Informação** em empresas e instituições. Procura garantir a segurança, [7] confidencialidade, integridade e disponibilidade da informação, bem como a boa gestão de riscos da mesma.
Esta certificação é mundialmente reconhecida como padrão na área da **Segurança da Informação**, sendo aplicável a organizações de todos os tamanhos e setores. **A ISO 27001** tem como principal foco a implementação de medidas de segurança, definição de políticas, realização de avaliações de risco, implementação de controlos de segurança e monitorização contínua de sistemas.
É amplamente utilizada como "selo de conformidade", demostrando o compromisso que uma determinada organização tem com a **Segurança da Informação**, bem como forma de melhorar a confiança depositada pelos clientes.
Considerando o oitavo capítulo deste trabalho **"Testes Substantivos e Testes de Conformidade"** em relação à ISO 27001, consideramos importante analisar o seguinte exemplo:

- **Teste Substantivo**: Análise da implementação de controlos de segurança exigidos pela norma;
- **Teste de Conformidade**: Verificação da documentação para garantir que a organização atenda aos requisitos específicos da ISO/IEC 27001.

XIII. SÉRIE 27000

A norma 27001 pertence à família da **Segurança da Informação** e está relacionada com os padrões ISO, sendo esta agrupada à **Série 27000**. Nesta Série, estão contidas normas como:

- **[6] ISO 27000 –** Vocabulário de **Gestão de Segurança da Informação**;
- **[6] ISO 27002 –** Contem um guia de boas práticas para controlo de **Segurança da Informação.** Não contem certificação acreditada;
- **[6] ISO 27003 –** Sistema de Gestão de Segurança da Informação – Orientação;
- **[6] ISO 27004 -** Gestão de Segurança da Informação – Monitorização, mediação, análise e avaliação;

- **[6] ISO 27005 -** Gestão de riscos na Segurança da Informação;
- **[6] ISO 27006 –** Requisitos para os organismos que fornecem auditoria e certificação de sistemas de **Gestão de Segurança da Informação.**

[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (6)

XIV. OUTRAS CERTIFICAÇÕES ISO

A **"International Organization for Standardization"** desenvolve e publica várias normas internacionais para garantir a qualidade e eficiência de diversos setores. Além da **ISO 27001**, que trata especificamente da segurança da informação, existem outras normas específicas relacionadas com a área da Tecnologia da Informação, sendo estas:

- **ISO 9001 – Gestão de Qualidade:**
  - Esta norma foca-se na gestão da qualidade e define os critérios para um sistema mais eficiente. É aplicável a organizações de todos os tipos, independentemente do seu tamanho e estrutura.

- **ISO 20000 – Gestão de Serviços de Tecnologia da Informação (TI):**
  - Define os requisitos para um sistema de gestão de serviços de tecnologias da informação, procurando a entrega eficiente e eficaz de serviços e promovendo a satisfação do cliente.

- **ISO 22301 – Continuidade de Negócios:**
  - Responsável pela gestão da continuidade negócios, estabelece requisitos para planos de continuidade, visando garantir a resiliência e a capacidade de resposta a interrupções.

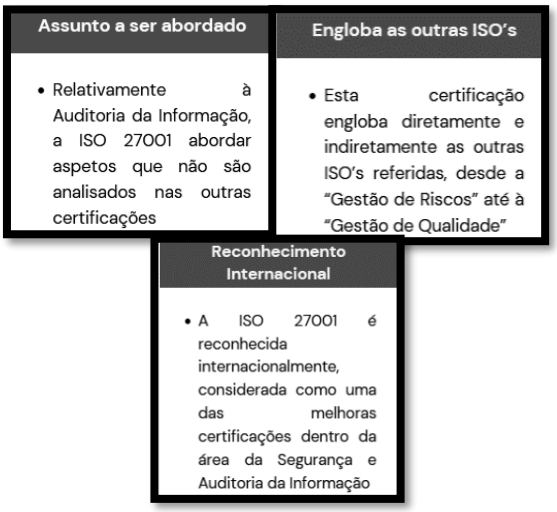
- **ISO 31000 – Gestão de Riscos:**
  - Fornece princípios e diretrizes para a gestão de riscos em organizações. Não é certificável, mas oferece um guia sobre como identificar, avaliar e resolver riscos de maneira sistemática.

[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (7)

XV. Justificativa - ISO 27001

Enquanto a ISO 27001 se concentra na segurança da informação, as outras normas aplicam-se a assuntos como a qualidade de serviços, gestão de serviços e gestão de riscos. A escolha de uma das certificações em relação às outras depende dos objetivos pretendidos por determinada entidade, podendo esta obter até várias certificações ISO, se esse for o objetivo pretendido. Apesar disso, algumas das vantagens da escolha da ISO 27001 na abordagem deste trabalho são as seguintes:

- O assunto a ser tratado influenciou diretamente nessa escolha, considerando que a ISO 27001 aborda aspetos que não são analisados noutras certificações ISO;
- A ISO 27001 é **a única norma da série 27000 com requisitos de certificação e passível de certificação acreditada;**
- O reconhecimento internacional desta norma foi importante para a nossa escolha, considerando que a ISO 27001 é uma das certificações de maior destaque em relação à Segurança da Informação.



[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (8)

XVI. Caso de Estudo – Entidade Governamental (Devoteam Cyber Trust)

Iremos utilizar como caso de estudo uma Entidade Governamental com a disponibilização do caso de estudo pela "Devoteam Cyber Trust", uma vez que foi esta empresa que implementou a Certificação ISO 27001 na Entidade Governamental, foi elaborado um relatório de implementação.

XVII. Caso de Estudo – Desafio

O desafio consistia no desenvolvimento de procedimentos de segurança, considerando que o cliente tinha uma exigência regulatório para a adoção e implementação de um sistema de gestão de segurança da informação. Desse modo, considerando que a Entidade Governamental não tinha recursos e conhecimento suficiente para realizar essa implementação, **ficou a "Devoteam Cyber Trust" encarregada por planear e implementar esse conjunto de procedimentos.** Esta empresa é de **origem portuguesa.**

XVIII. Caso de Estudo – SOLUÇÃO

Foi prestado um serviço com um projeto bem definido, com a intervenção de uma equipa de consultoria, que realizou todo um conjunto de processos de implementação e apoio na certificação obtida pela Entidade Governamental. Este Projeto contou com um conjunto de 5 etapas, sendo estas aplicadas em muitos outros projetos do mesmo tipo, através dos quais o cliente é apoiado em todas as atividades. Sobre estas fases, não foi divulgado o tempo exato de duração de cada uma, por uma questão de proteção de dados, sendo estas as seguintes:


devoteam
Cyber Trust

ISO 27001

Case Study

Adopting and certification by ISO 27001

The Client

National Government Entity.

The Challenge

Within the scope of functions development, the client had a regulatory requirement for the adoption and implementation of an information security management system (SGSI ISO 27001), with its certification by an accredited entity.
The Client did not have sufficient knowledge or resources to carry out the implementation.

The Solution

We provided a service composed by a project, with the intervention of its consulting team that carried out the process of implementation and support in the certification obtained by the client.
During this project, which lasted 9 months, we applied our 5-step Roadmap proven in numerous projects, through which supports the client in all activities, namely in the structuring of processes and documentation, in the implementation of these processes, definition and action of risk management analysis, operation, among other critical activities.
All activities carried out were supported by IntegrityGRC platform, which has a proven effectiveness of more than 40% at the time of its implementation, taking into account the functionalities provided by the platform that fully support all key activities in the implementation of a given standard or regulation, from the documentary components to ensuring its connection with the operational component.

The Impact

The Client was able to increase its maturity and information security management practice very sharply through the adoption of ISO 27001, and was able to meet its ISO 27001 certification objective in the established time, through our implementation service.

Related Services

- ISO 27001 Implementation
- IntegrityGRC

Making your tech journey more secure.

For more information, please visit www.integrity.pt

[2] Caso de Estudo - Entidade Governamental (Devoteam Cyber Trust)

1. [2] Preparação: Estabeleceu-se a estrutura apropriada para as necessidades de negócio e dotou a organização com as competências necessárias. O período de preparação demorou cerca de 1 a 2 meses e foi subdividida em 3 subfases:

a. [3] Escopo: Caracteriza as funcionalidades, processos de negócio e ativos a serem protegidos;

b. [3] Treino específico para a ISO 27001: Fornece à equipa cliente, todo o conhecimento necessário sobre Sistemas de Informação em relação à Certificação ISO 27001;

c. [3] Treino geral sobre Segurança da Informação: Fornece à equipa cliente, todo o conhecimento de Segurança, associado ao momento presente.

[4] Caso de Estudo 01

[4] Caso de Estudo 01.1

2. [2] Diagnóstico: Identificou todas as falhas do sistema, desde os processos, aos controlos aplicáveis, riscos e controlos de mitigação. Esta fase torna-se fundamental para definir quais são as lacunas a alocar recursos para uma implementação eficiente. Esta fase demorou cerca de 1 a 3 meses e foi dividida da seguinte maneira:

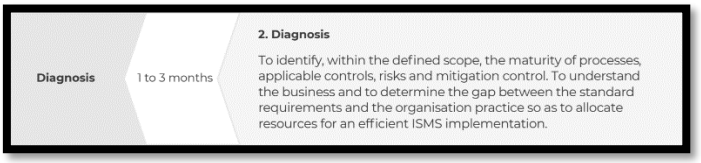
a. [3] Diagnóstico específico: Útil para se entender a dinâmica de negócio de determinada empresa, bem como para se encontrarem falhas;

b. [3] Preparação dos resultados: São apresentados os resultados analisados na subfase de diagnóstico;

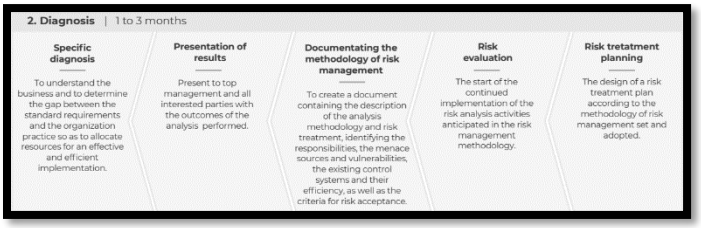
c. [3] Documentação da metodologia de risco: Cria-se um documento contendo a descrição da análise metodológica, identificando-se responsabilidades e vulnerabilidades, bem como os critérios para aceitação de riscos;

d. [3] Avaliação de riscos: Contínua implementação de atividades de análise de riscos previstos;

e. [3] Esboço do risco planeado: É feito o desenho de um determinado risco planeado de acordo com os processos de análise de riscos.



[4] Caso de Estudo 02



[4] Caso de Estudo 02.1

3. [2] Procurou-se implementar e mitigar as falhas existentes em relação ao sistema a ser abordado. Esta fase demorou cerca de 1 a 4 meses e está dividida em 4 subfases:

a. [3] Definição das políticas de segurança: Esta subfase serve para se documentar os objetivos da Segurança da Informação, bem como os compromissos da "gestão de liderança", com redução de riscos associados e políticas de incumprimento;

b. [3] Documentação de processos de SI: Deverão ser documentados os processos de SI, de forma a serem atribuídas responsabilidades;

c. [3] Declaração de Aplicabilidade (**SoA**): Criação de um registo contendo todas as informações sobre o controlo aplicável aos sistemas, com eventuais restrições e devidas justificativas;

d. [3] Documentação Aprovada: Aprovação do sistema de SI e do plano de tratamento e risco, pelo líder de projetos.

[4] Caso de Estudo 03

[4] Caso de Estudo 03.1

4. [2] Execução: Executou-se os processos de forma bem definida, destacando-se o cumprimento de objetivos, identificando oportunidades de melhoria e de não conformidade do sistema de SI. O sistema de SI deverá ser revisto pelo líder de projetos. Esta fase demorou cerca de 3 e 6 meses e está subdividida da seguinte maneira:

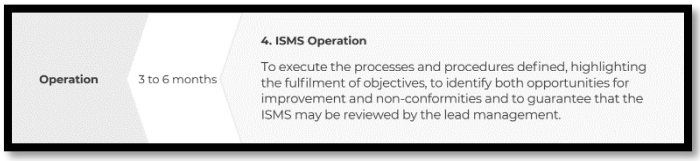
a. [3] Treino e Ações de Sensibilização: Deverão ser feitos treinos de forma inopinada, bem como ações de sensibilização para toda a organização, para as boas práticas de SI;

b. [3] Processo de Avaliação contínua: É importante serem implementadas tarefas que permitam avaliar, de forma direta ou indireta, o sistema de SI, de forma que esta possa constantemente ser melhorado;

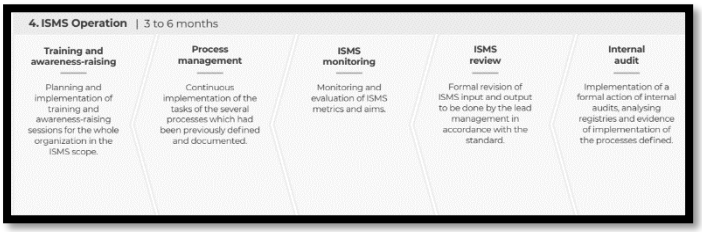
c. [3] Monitoramento de Métricas e Objetivos: O monitoramento de métricas e objetivos é essencial para uma boa gestão dos SI;

d. [3] Revisão formal do Sistema: Deverá ser feita uma revisão forma do sistema de SI, pelo líder de projetos, de forma a analisar falhas;

e. [3] Auditoria Interna: Implementação de uma auditoria interna de forma a ser analisados dados e registos de processos definidos.



[4] Caso de Estudo 04



[4] Caso de Estudo 04.1

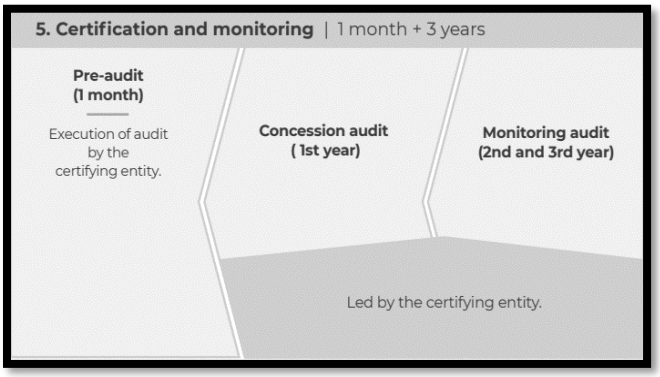
5. [2] Certificação ISO 27001 e Monitoramento: O processo de certificação demorou entre 1 mês e 3 anos, de acordo com as análises da empresa certificadora, considerando aspetos como a avaliação de desempenho do sistema de SI, processos de melhoria contínua, entre outros… Esta fase está dividida nas seguintes fases:

a. [3] Pré-Auditoria: Demora cerca de 1 mês;

b. [3] Análise da Auditoria: É feita toda a análise de procedimentos relacionados com a SI;

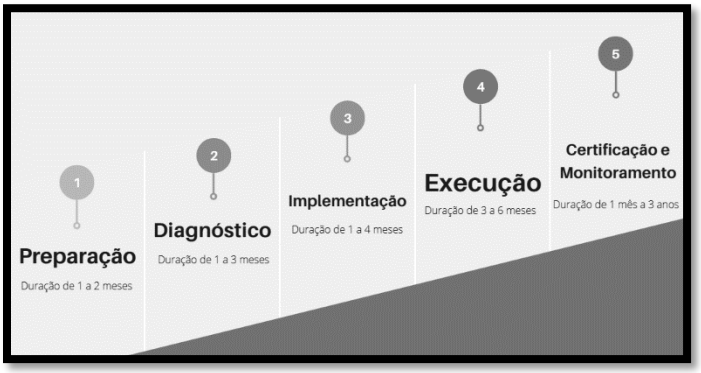
c. [3] Auditoria de Monitoramento: É feito um controlo posterior à entrega da certificação, de forma a verificar-se se a empresa avaliada deve continuar a receber a certificação.

[4] Caso de Estudo 05



[4] Caso de Estudo 05.1

De seguida, apresentamos o **"Processo de Implementação e Certificação ISO 27001"** por fases e o **relatório geral de implementação elaborado pela Devoteam Cyber Trust:**



[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (9)

[3] 5 Etapas para a Certificação ISO 27001 - Caso de Estudo

[3] Além de todo o processo explicado de forma detalhada nestas 5 etapas, é sempre necessário considerando que na procura da certificação ISO 27001, são avaliados conceitos como:

- **Controlo interno de Sistemas;**
- **Operacionalidade de procedimentos;**
- **Revisões pelo líder de Projetos;**
- **Tratamento de Riscos;**
- **Testes ao Sistemas e Ações de Formação;**
- **Evolução e Performance.**

Todas as atividades realizadas foram apoiadas pela plataforma **"IntegrityGRC",** que possui comprovada eficácia na implementação de funcionalidades-chave, bem como no cuidado a ter com a ligação do sistema a componentes mais operacionais.

XIX. Caso de Estudo – IMPACTO

Com a certificação atribuído à Entidade Governamental, esta conseguiu ganhar maturidade em relação às suas políticas de segurança. A Certificação serviu ainda para aumentar a credibilidade da empresa perante clientes, em relação à **Segurança da Informação**. **O processo de implementação das 5 etapas demorou cerca de 9 meses. A manutenção da certificação demorou até 3 anos.**

XX. Conclusões sobre Auditoria da Informação

Este trabalho de investigação abrangeu conceitos relacionados com Auditoria da Informação, com ênfase na **certificação ISO 27001**. O problema central identificado foi a necessidade crítica de garantir a **Segurança da Informação** num contexto de rápida evolução tecnológica, onde a [7] confidencialidade, integridade e disponibilidade dos dados em sistemas é essencial. Os objetivos do estudo incluíram a compreensão das etapas do processo de Auditoria da Informação, desde o planeamento até ao acompanhamento, com importância especial **na avaliação de riscos e na seleção de áreas críticas** a serem auditadas, sendo estas áreas fundamentais para direcionar os esforços de forma eficiente, priorizando os pontos mais sensíveis dos sistemas em relação a ambientes complexos. Abordámos ainda métodos e técnicas de teste, incluindo testes substantivos e de conformidade. Questões éticas e legais, como a privacidade, foram referidas, sublinhando a importância de uma abordagem ética na execução de procedimentos. O estudo também antecipou tendências emergentes, como **auditoria de segurança cibernética, auditoria de dados e auditoria de inteligência artificial,** destacando a necessidade de adaptação contínua às mudanças do setor tecnológico.

XXI. Resistência em relação a procedimentos de Segurança

Numa organização, a implementação de medidas e procedimentos de **Segurança da Informação** é essencial para proteger dados sensíveis e garantir a Integridade do sistema. No entanto, muitas vezes, deparamo-nos com a resistência dos colaboradores em adotar estas práticas, o que pode apresentar desafios significativos. Aqui apresentamos alguns dos principais motivos para esta resistência:

- **Falta de Consciencialização:** A falta de compreensão acerca da importância da **Segurança da Informação** pode resultar em resistência. Colaboradores que não percebem as potenciais ameaças e os riscos associados podem subestimar a necessidade de seguir procedimentos específicos e rigorosos;

- **Inconveniência:** Algumas medidas de segurança podem ser percebidas como inconvenientes pelos colaboradores. **Senhas complexas, autenticação de dois fatores e outros protocolos de segurança podem ser vistos como obstáculos ao trabalho diário;**

- **Cultura Organizacional:** Uma cultura organizacional que não enfatiza a importância da **Segurança da Informação** pode contribuir para a resistência. Se a liderança não promove ativamente práticas seguras, os colaboradores podem não considerar a **Segurança da Informação** como uma prioridade;

- **Falta de Formação Adequada:** A ausência de formação adequada sobre as práticas de segurança pode levar a mal-entendidos ou desconhecimento dos procedimentos corretos. A formação regular e eficaz é crucial para garantir que todos compreendam e implementem as medidas de segurança necessárias;

- **Desconfiança nas Políticas Organizacionais:** Se os colaboradores não confiarem nas políticas de segurança implementadas pela organização, podem resistir à sua adoção. A transparência e a comunicação são essenciais para construir confiança;

- **Experiências Passadas Negativas:** Se os colaboradores passaram por experiências passadas negativas, como medidas excessivamente restritivas ou sistemas de segurança que interferiram no desempenho das suas tarefas, podem estar menos propensos a adotar novas práticas.

[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes (10)

XXII. Desafios do Futuro

À medida que a tecnologia e os ambientes de computação em nuvem continuam a evoluir, surgem novas oportunidades e desafios na área de Auditoria da Informação. Com a ascensão de tecnologias "de futuro", como a Inteligência Artificial, Blockchain e Internet das Coisas (loT), desafios futuros podem surgir com a integração dessas tecnologias nos processos de auditoria. Será bastante interessante verificar e investigar os impactos destas novas tecnologias na Segurança da Informação. Poderá ser analisada a forma como as futuras ferramentas de proteção de dados irão ser implementadas nestas novas tecnologias. O cálculo da previsão de possíveis vulnerabilidades de segurança com base em padrões históricos poderá ser uma das áreas de estudo a ser aprofundado. Investigar a eficácia de boas práticas na utilização das novas tecnologias também poderá ser um bom tema a ser abordado. Estas sugestões representam apenas algumas possibilidades para **futuros trabalhos de investigação na área da Auditoria e Segurança da Informação…**

XXIII. Referências

[1] Slide de Apresentação Canva - Gestão de Sistemas e Redes – Trabalho sobre Auditoria da Informação

[2] Caso de Estudo - Entidade Governamental (Devoteam Cyber Trust) - www.integrity.pt/pdf/case_study2_adoption_and_certification_by_iso27001_standard.pdf

[3] 5 Etapas para a Certificação ISO 27001/Caso de Estudo – www.integrity.pt/pdf/roadmap_en.pdf

[4] Imagens "Casos de Estudo" 01, 01.1, 02, 02.1, 03, 03.1, 04, 04.1 ,05 e 05.1 - www.integrity.pt/pdf/roadmap_en.pdf

[5] Explicação do capítulo "XII" com base no site da ISO - www.iso.org/standard/27001

[6] Definição e explicação de outras ISO da Série 27000 foram retiradas do Site - pt.wikipedia.org/wiki/ISO_27001

[7] Pilares Princípais da Segurança da Informação - www.aenorportugal.com/certificacion/tecnologias-da-informacao/iso-27001-seguranca-da-informacao

[8] A explicação básica dos Testes Substantivos e de Conformidade foram inicialmente aprendidos através do site - ojpeao.blogs.sapo.mz/3838.html