GUIAS PARA GERENCIAMENTO DE RISCO RELACIONADO AO USO DE TECNOLOGIA DA INFORMAÇÃO

ISO 27001/2

A ISO 27001 é a norma internacional que trata da gestão de segurança da informação em uma organização. Ela fornece um conjunto de diretrizes e melhores práticas para ajudar as organizações a proteger suas informações e minimizar os riscos relacionados à segurança da informação.

A ISO 27002, por sua vez, é uma norma complementar que oferece um conjunto detalhado de controles de segurança da informação que podem ser implementados para atender aos requisitos da ISO 27001.

- No contexto do gerenciamento de riscos, a ISO 27001/2 oferece uma abordagem estruturada para identificar, avaliar, tratar e monitorar os riscos de segurança da informação:

  - **Identificação de Ativos:** A primeira etapa é identificar todos os ativos de informação críticos da organização, incluindo dados, sistemas, redes, hardware e software.

  - **Avaliação de Riscos:** Uma vez que os ativos críticos são identificados, a organização precisa realizar uma avaliação de riscos para identificar as ameaças que podem afetar esses ativos e as vulnerabilidades que podem ser exploradas pelas ameaças.

- **Análise de Riscos:** Após a identificação de ameaças e vulnerabilidades, a organização deve analisar o impacto potencial desses riscos e a probabilidade de ocorrência. Isso ajuda a classificar os riscos em termos de sua gravidade.

- **Tratamento de Riscos:** Com base na análise de riscos, a organização pode decidir como tratar os riscos. As opções incluem aceitar o risco, mitigar o risco (por meio de controles de segurança), transferir o risco (por exemplo, por meio de seguros) ou evitar o risco (por exemplo, interrompendo uma atividade de alto risco).

- **Implementação de Controles:** A ISO 27001/2 fornece uma lista de controles de segurança que podem ser implementados para reduzir os riscos de segurança da informação. Isso inclui medidas técnicas, organizacionais e humanas.

- **Monitoramento e Revisão:** Após a implementação dos controles, a organização deve monitorar continuamente a eficácia desses controles e revisar periodicamente a avaliação de riscos para garantir que as medidas permaneçam adequadas.

- **Comunicação e Conscientização:** A norma enfatiza a importância de comunicar as políticas de segurança e conscientizar os funcionários e partes interessadas sobre as práticas de segurança da informação.

- **Documentação:** A ISO 27001/2 também enfatiza a necessidade de documentar todo o processo de gerenciamento de riscos, incluindo políticas, procedimentos e registros relacionados à segurança da informação.

- Essa abordagem baseada em riscos é fundamental para a implementação bem-sucedida da ISO 27001/2, pois ajuda as organizações a tomar decisões informadas sobre como proteger suas informações de acordo com sua importância e os riscos associados. A norma fornece um quadro sólido para garantir a segurança da informação e é amplamente reconhecida em todo o mundo.

- A norma ISO/IEC 27005 é uma norma específica para a gestão de riscos de segurança da informação. É de grande utilidade para aqueles que buscam uma compreensão aprofundada da avaliação e mitigação de riscos no contexto da segurança da informação.
  - Se o seu interesse é atuar como consultor nessa área ou se pretende lidar com a segurança da informação e a gestão de riscos de forma regular, a norma ISO/IEC 27005 se torna uma valiosa fonte de conhecimento e orientação.

ISO 27005

- A ISO/IEC 27005 é uma norma internacional que se concentra na gestão de riscos de segurança da informação. Ela fornece diretrizes e melhores práticas para organizações que desejam avaliar, tratar e gerenciar os riscos relacionados à segurança da informação de forma eficaz. A seguir os postos-chave a serem destacados sobre a norma ISO 27005:

  - **Objetivo Principal:** o principal objetivo da ISO 27005 é auxiliar as organizações a implementar um processo estruturado e sistemático para a gestão de riscos de segurança da informação, que envolve identificar, avaliar e tratar os riscos que podem afetar a confidencialidade, integridade e disponibilidade das informações.

- **Estrutura de Abordagem:** adota uma abordagem baseada em riscos, que é fundamental para a gestão eficaz da segurança da informação. Fornece uma estrutura detalhada para esse processo, que inclui a identificação de ativos, ameaças, vulnerabilidades e impactos, bem como a avaliação e tratamento dos riscos.

- **Personalização:** Uma das características mais flexíveis da ISO 27005 é que ela pode ser adaptada às necessidades específicas de cada organização. Isso significa que as organizações podem personalizar o processo de gestão de riscos de acordo com o tamanho, complexidade e setor em que operam.

- **Relação com a ISO 27001:** a norma ISO 27005 é intimamente relacionada à ISO 27001, que trata da gestão de segurança da informação.
  - **ISO 27001:** estabelece os requisitos gerais para a implementação de um Sistema de Gestão de Segurança da Informação (SGSI).
  - **ISO 27005:** fornece diretrizes detalhadas para o gerenciamento de riscos dentro desse sistema.

- **Processo de Gestão de Riscos:** descreve o ciclo contínuo de gestão de riscos, que inclui a identificação, avaliação, tratamento, aceitação e monitoramento dos riscos.
  - Envolve a definição de critérios de avaliação de riscos, a seleção de medidas de tratamento de riscos apropriadas e a revisão regular do processo.

- **Benefícios:** a implementação da ISO 27005 traz vários benefícios para as organizações:
  - Capacidade de tomar decisões informadas sobre a segurança da informação
  - Melhorar a resiliência contra ameaças e vulnerabilidades, garantir a conformidade com regulamentações e normas, e aumentar a confiança de partes interessadas.

- **Aplicação Universal:** a ISO 27005 é aplicável a organizações de todos os setores e tamanhos. Ela é valiosa tanto para grandes corporações quanto para pequenas empresas que buscam proteger suas informações.

ISO 31000

- A ISO 31000 é uma norma internacional que aborda a gestão de riscos de forma abrangente. Ela fornece um conjunto de princípios, estruturas e diretrizes que podem ser aplicados por organizações de todos os tipos e tamanhos para estabelecer um processo eficaz de gerenciamento de riscos. A seguir os postos-chave a serem destacados sobre a ISO 31000:

- **Abordagem Holística (Integrada):** adota uma abordagem holística para a gestão de riscos, que pode ser aplicada a uma ampla gama de riscos, incluindo riscos estratégicos, operacionais, financeiros, de conformidade e outros.
  - **Ela não se limita à segurança da informação, sendo aplicável a qualquer tipo de risco.**

- **Princípios Fundamentais:** uma série de princípios fundamentais que orientam o processo de gerenciamento de riscos que incluem:
  - Integração da gestão de riscos nas atividades organizacionais.
  - Personalização do processo de acordo com as necessidades da organização.
  - Consideração de fatores humanos e culturais.
  - Comunicação e consulta com partes interessadas.
  - Avaliação contínua e a melhoria do processo.

- **Estrutura do Processo:** a ISO 31000 descreve uma estrutura de processo de gestão de riscos que inclui:
  - Identificação, avaliação, tratamento, monitoramento e revisão de riscos.
  - Processo é iterativo e contínuo, o que significa que as organizações devem revisar e ajustar suas estratégias de gerenciamento de riscos ao longo do tempo.

- **Compatibilidade com Outros Sistemas de Gestão:** A norma é projetada para ser compatível com outros sistemas de gestão, como a **ISO 9001 (gestão da qualidade)** e a **ISO 14001 (gestão ambiental)**. Isso permite que as organizações integrem a gestão de riscos em suas práticas de gestão existentes.

- **Adaptabilidade:** a ISO 31000 é flexível e adaptável às necessidades específicas de cada organização. Ela não prescreve um conjunto específico de ferramentas ou técnicas, permitindo que as organizações escolham as abordagens mais adequadas para gerenciar seus riscos.

- **Benefícios:** a implementação da ISO 31000 oferece vários benefícios, como uma melhor tomada de decisões, uma compreensão mais clara dos riscos enfrentados, uma maior resiliência organizacional, uma melhoria na capacidade de inovar e uma maior confiança das partes interessadas.

- **Aplicação Universal:** A norma é aplicável a organizações de todos os setores e tamanhos, desde pequenas empresas até grandes corporações e entidades governamentais.

ISO 38500

- Um novo padrão de governança em tecnologia da informação (TI) com o objetivo principal de auxiliar as organizações por meio de um conjunto de princípios para avaliar, gerenciar e monitorar o uso de TI. Esses princípios estão alinhados com modelos e melhores práticas, como o CobiT 4.1.

- A estrutura da norma é composta por três partes principais:
  1. Escopo, aplicação e objetivos.
  2. Estrutura para uma governança corporativa de TI adequada.
  3. Guia para a governança corporativa de TI.

- A norma aborda a utilização eficaz de TI para atingir os objetivos de negócios da organização, bem como o retorno sobre os investimentos em TI, incluindo onde são alocados, como são gastos e onde ocorrem os investimentos. A aplicação dessa norma é destinada a organizações de todos os tipos, sejam elas públicas ou privadas, independentemente de seu porte (pequeno, médio ou grande).

- Ela se baseia em seis princípios fundamentais que orientam a governança de TI. Esses princípios são:

- **Responsabilidade:** a governança de TI deve ser liderada e supervisionada pelos órgãos de governança da organização, como o conselho de administração. A responsabilidade pela tomada de decisões relacionadas à TI deve ser claramente definida, garantindo que os riscos e oportunidades sejam devidamente considerados.

- **Estratégia:** a governança de TI deve estar alinhada com a estratégia da organização. Isso significa que as decisões relacionadas à TI devem contribuir para a realização dos objetivos de negócios e refletir a visão de longo prazo da organização.

- **Aquisição:** a aquisição de recursos de TI deve ser planejada e gerenciada de forma a otimizar o valor para a organização. Isso envolve a escolha criteriosa de fornecedores, a gestão de contratos e a avaliação contínua do desempenho e custo dos ativos de TI.

- **Desempenho:** A governança de TI deve assegurar que os recursos de TI sejam usados efetivamente para alcançar os resultados desejados. O desempenho e os riscos associados à TI devem ser monitorados regularmente para garantir que a organização esteja atingindo seus objetivos.

- **Conformidade:** as práticas de governança de TI devem garantir que a organização cumpra todas as leis, regulamentações e normas aplicáveis relacionadas à TI. Isso envolve a implementação de políticas e procedimentos para garantir a conformidade.

- **Mensuração:** a governança de TI deve incluir métricas e indicadores que permitam a medição do desempenho, o monitoramento de riscos e a avaliação do valor gerado pela TI. A mensuração é fundamental para a tomada de decisões informadas e a melhoria contínua.

Cobit 4.1 x ISO 38500

- **Similaridades**
  - São direcionados a organizações de todos os tamanhos e setores.
  - Enfatizam a importância da governança de TI para o sucesso do negócio.
  - Fornecem uma estrutura para a avaliação e melhoria da governança de TI.

- **Diferenças**
  - O COBIT 4.1 é mais abrangente e detalhado do que a ISO 38500.
  - A ISO 38500 é mais concisa e menos detalhada do que o COBIT 4.1.
  - O COBIT 4.1 oferece programas de certificação, a ISO 38500 não.

- **Qual framework escolher?**
  - Depende das necessidades específicas da organização.
    - Organizações que precisam de um framework abrangente e detalhado para a governança de TI devem considerar o COBIT 4.1.
    - Organizações que precisam de um framework mais conciso e menos detalhado podem considerar a ISO 38500.

- **Exemplos de uso**
  - O COBIT 4.1 e a ISO 38500 são amplamente utilizados por organizações de todos os tamanhos e setores. Alguns exemplos de uso incluem:
    - Avaliação da maturidade da governança de TI.
    - Desenvolvimento de estratégias de governança de TI.
    - Implantação de frameworks de governança de TI.
    - Auditoria de governança de TI.

NIST Série 800

- O NIST (Instituto Nacional de Padrões e Tecnologia) é uma instituição dos Estados Unidos cujo principal propósito é promover o progresso econômico e o bem-estar público do país, oferecendo liderança técnica por meio da criação de padrões e medições de infraestrutura.

- O Instituto de Tecnologia da Informação (ITL), uma parte integral do NIST, concentra-se na pesquisa, desenvolvimento de testes, métodos de ensaio, implementação prática e análise técnica para fomentar o avanço e a utilização produtiva da tecnologia da informação.
  - Suas responsabilidades incluem a formulação de técnicas, diretrizes administrativas e normas de gestão, tudo isso voltado para a segurança, eficiência econômica e proteção da privacidade das informações.

- A série 800 (NIST-800) abrange uma coleção de relatórios que oferecem orientações e delineiam os esforços necessários para assegurar a segurança da informação em diversas áreas, como organizações públicas, indústrias, instituições acadêmicas, e muito mais.

- Os documentos SP 800-30, SP 800-53 e SP 800-60 são alguns dos mais relevantes dentro da série SP 800, e cada um tem um foco específico.

- O"SP" nas normas NIST refere-se a "Special Publication" em inglês, que em português pode ser traduzido como "Publicação Especial".

NIST SP 800-30:
"Guide for Conducting Risk Assessments"

- O NIST SP 800-30 fornece orientações detalhadas para a realização de avaliações de risco de segurança da informação.
- Descreve o processo de identificação de ativos críticos, ameaças, vulnerabilidades e impactos, bem como a avaliação de riscos.
- Auxilia as organizações a entender e gerenciar os riscos de segurança da informação e é essencial para a tomada de decisões informadas sobre a implementação de medidas de segurança.

NIST SP 800-53: "Security and Privacy Controls for Federal Information Systems and Organizations"

- O NIST SP 800-53 é um guia que estabelece um conjunto abrangente de controles de segurança e privacidade que devem ser implementados em sistemas de informação federais dos EUA, bem como em organizações que lidam com informações sensíveis.

- Abrange uma ampla gama de tópicos, incluindo autenticação, controle de acesso, criptografia, monitoramento, resiliência cibernética e conformidade.

- Esses controles ajudam a proteger informações críticas e garantir a integridade, confidencialidade e disponibilidade dos sistemas.

NIST SP 800-60: "Guide for Mapping Types of Information and Information Systems to Security Categories"

- O NIST SP 800-60 é um guia que ajuda as organizações a mapear tipos de informações e sistemas de informação em categorias de segurança.
- Útil para classificar os níveis de proteção necessários com base na sensibilidade das informações e no contexto operacional.
- Fornece um modelo de como as informações devem ser classificadas em categorias, ajudando as organizações a determinar as medidas de segurança apropriadas a serem aplicadas a cada categoria.