GESTÃO DE PROJETOS E GOVERNANÇA DE TI
TRABALHO 2º BIMESTRE

MATHEUS HENRIQUE BUTKOSKI
GUSTAVO PERUZZO

ISO 27000

A ISO 27000 não é uma norma em si, mas sim um **conjunto de normas**. Dessa maneira, cada membro desse conjunto recebe uma denominação única e objetivos específicos. Existem mais de 40 normas, que foram desenvolvidas com base em procedimentos para a implementação nas empresas, havendo algumas também dedicadas exclusivamente a determinados segmentos de mercado.

Implementar a ISO 27000 em uma empresa é uma iniciativa que oferece um excelente retorno sobre o investimento, **ela influencia tanto na construção de uma boa imagem para a marca quanto na organização interna da empresa**.

Tratando de organizações que se relacionam com proteção de dados, privacidade e governança de tecnologia da informação, isso se mostra em maior intensidade. Enfim, a ISO 27000 pode oferecer metodologias que permitem tratar a segurança da informação de uma maneira mais **eficiente**.

Do ponto de vista da LGPD (Lei Geral de Proteção de Dados) , a ISO 27000 significa um diferencial a mais, pois praticamente toda empresa lida com algum nível de informação confidencial e no ponto de vista dos clientes, agrada a ideia de haver um cuidado voltado exclusivamente à segurança das informações fornecidas.

ISO/IEC 27001

A ISO/IEC 27001 foi publicada em outubro de 2005 pelo International Organization for Standardization e pelo International Electrotechnical Commission.O nome completo dessa norma para sistema de gestão da segurança da informação é ISO/IEC 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos.

O objetivo da norma é criar um modelo padronizado para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar os sistemas e processos de segurança da informação de uma empresa. É a única norma da família 27000 que é passível de certificação acreditada, todas as seguintes são apenas guias de boas práticas.

A auditoria é feita por uma terceira parte, garantindo a credibilidade, a independência e a transparência da certificação, se concedida.É fundamental que a empresa auditora obedeça à ISO/IEC 27006. Normalmente, a auditoria para conseguir a certificação ISO/IEC 27001 acontece em dois estágios:

Primeiro estágio: análise preliminar e informal, onde verifica-se a existência de documentos-chave para a gestão, como as políticas de segurança da informação e de gerenciamento de risco.

Segundo estágio: nesta etapa, é feita uma análise profunda e detalhada pela auditoria, que inclui a existência e a eficácia de aplicação dos controles ISMS (Information Security Management System).

Depois da primeira emissão do certificado certificado ISO/IEC 27001, a renovação é feita por meio de revisões periódicas e de novas declarações da empresa de que os padrões ISMS continuam em plena e eficaz operação.

Nenhuma organização é obrigada a ter a certificação ISO/IEC 27001, porém essa pode ser uma exigência dos clientes e parceiros de negócio antes de fecharem contrato com a empresa. Dessa forma, adotar os padrões da norma é uma decisão estratégica, que deve ser tomada de acordo com as necessidades, tamanho e área de atuação do negócio, assim como seguindo as exigências dos clientes e o padrão do mercado.

A comprovação de que a gestão de segurança da informação da empresa obedece aos mais altos padrões do setor é uma garantia de que essa parte do negócio está no caminho certo. Com o entendimento de que as informações e dados mais sensíveis estão devidamente protegidos, é possível operar com mais confiança, buscando continuamente a inovação e o crescimento do setor e da organização como um todo.

ISO/IEC 27002

A ISO/IEC 27002 é um regulamento que conta com uma série de práticas que, quando aplicadas corretamente, ajudam na implementação de um SGSI (Sistema de Gestão de Segurança da Informação).

Ela serve como um guia prático que ajuda no desenvolvimento e implantação de métodos e controles da segurança da informação dentro de uma empresa. Sendo assim, o intuito se torna o **de assegurar que os negócios terão prosseguimento ao mesmo tempo em que os riscos são minimizados e o retorno sobre investimento, bem como oportunidades da organização, são maximizados.**

Para isso, a norma técnica considera os ambientes de risco existentes no negócio, de modo a selecionar, implementar e gerenciar os controles adequados.

Quando fala-se sobre a importância de um guia de segurança, é necessário ter em mente os possíveis prejuízos decorrentes da ausência de proteção adequada. O tempo de inatividade de sistemas e o vazamento de dados, por exemplo, representam perda de produtividade e dinheiro, além de danos à reputação da marca e riscos à própria sobrevivência das empresas.

Para evitar esses possíveis imprevistos, os gestores não podem manter uma postura passiva, esperando a ocorrência de problemas desastrosos para agir e proteger seu negócio.

Principais vantagens da ISO/IEC 27002:

- Redução de custos decorrentes da prevenção dos incidentes de segurança;
- Controle correto dos ativos e dados sensíveis/críticos do negócio;
- Melhoria da conscientização acerca da segurança da informação no ambiente empresarial;
- Fornecimento de uma abordagem para implementar as políticas de controle;
- Detecção de riscos e possibilidade de corrigir pontos fracos;
  Maior diferencial competitivo no mercado e, em consequência, maior atração de clientes;
- Melhor estruturação de processos e mecanismos, além do seu correto gerenciamento.

ISO/IEC 27002 E LGPD:

A implementação da ISO/IEC 27002 também é fundamental para a adequação às regras de compliance e legislações vigentes, a exemplo da LGPD (Lei Geral de Proteção de Dados). De maneira geral, ambas possuem objetivos em comum: **mitigar o risco de violações de dados e fortalecer a segurança da informação**.

A LGPD exige a aplicação de medidas técnicas e organizacionais para garantir um nível adequado de proteção de dados. Para cumprir esse objetivo, a ISO/IEC 27002 fornece medidas eficazes para reduzir riscos e garantir a proteção necessária a dados confidenciais.

ISO/IEC 27003

A ISO/IEC 27003, é um guia para a implementação ou criação de um SGSI (Sistema de Gestão de Segurança da Informação) que mostra todo o processo de aprovação e execução do SGSI na organização, indo desde a escolha do escopo até a etapa de aprovação pela alta direção e partes interessadas. Além disso, possui um modelo de estrutura das políticas que serão desenvolvidas no processo de implantação.

De acordo com a norma, estas são as 5 fases do planejamento de um projeto de SGSI.

- Obter aprovação da direção/alta administração para iniciar o projeto de SGSI
- Definir o escopo, os limites e a política do SGSI;
- Conduzir a análise dos requisitos de segurança da informação;
- Conduzir a análise/avaliação de riscos e planejar o tratamento dos riscos;
- Definir o SGSI.

ISO/IEC 27004

A segurança da informação é fundamental para o sucesso de qualquer organização, uma falha de segurança errada e a reputação de uma empresa consolidada pode ser arruinada.

Os ciberataques estão entre as ameaças mais significativas que uma empresa pode enfrentar e a segurança dos dados pessoais e da informação comercialmente sensível é essencial. Mas como saber se o Sistema de Gestão de Segurança da Informação (SGSI) de uma empresa está entre os conformes da ISO/IEC 27001?.

A ISO/IEC 27004 fornece **diretrizes para o desenvolvimento e uso de métricas e medições** a fim de avaliar a eficácia de um SGSI implementado e dos controles ou grupos de controles, conforme especificado na ISO/IEC 27001. Ela mostra como criar um programa de medição de segurança da informação, como escolher, o que calcular, e como operar os processos de medição apropriados.

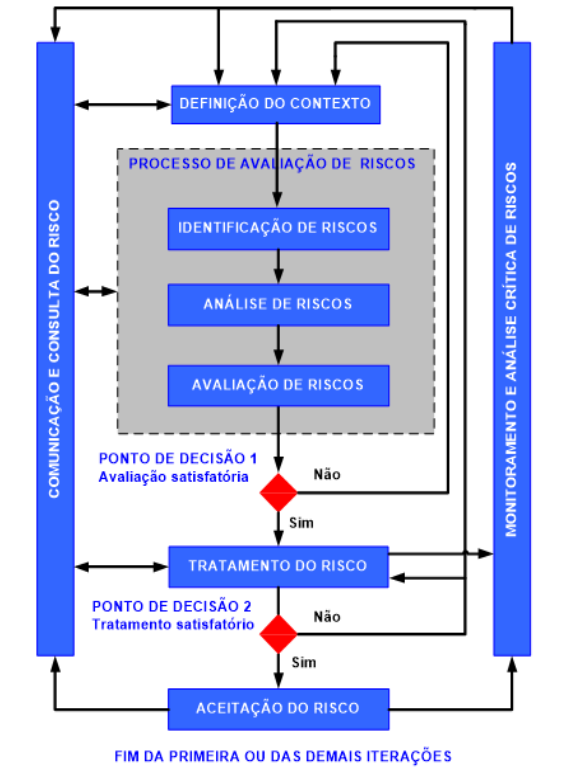
As métricas de segurança podem fornecer uma visão da eficiência do SGSI e, como tal, assumir um papel central. Um engenheiro ou empreiteiro responsável pela análise de segurança e gestão, ou um executivo que pretende uma melhor informação para a tomada de decisões, as métricas de segurança tornam-se um meio crítico para comunicar o estado da postura de risco cibernético de uma organização.

Vantagens para as organizações que utilizam a ISO/IEC 27004 encontram-se as seguintes:

- Aumento da transparência
- Melhoria da eficiência da gestão da informação e dos processos do SGSI
- Prova de conformidade com as especificações da ISO/IEC 27001, bem como com as regras, legislação e regulamentos pertinentes

ISO/IEC 27005

A ISO/IEC 27005 define o processo de gestão de risco como atividades coordenadas para dirigir e controlar o risco de uma organização. Neste contexto, o processo de gestão de riscos é definido por **oito atividades**, como observado na figura abaixo.



DEFINIÇÃO DE CONTEXTO:

Definir o escopo e limites que serão levados em consideração na gestão de riscos. Deverão ser descritos os processos que fazem parte do escopo, garantindo a identificação dos ativos relevantes para a gestão dos riscos. Além disso, a definição do contexto inclui determinar os critérios gerais de aceitação dos riscos para a organização e as responsabilidades para a gestão de riscos. A atividade de avaliação de riscos é subdividida em outras três atividades: Identificação de riscos, análise de riscos e avaliação de riscos

O ponto de decisão 1, presente na figura, tem a função de verificar se a avaliação dos riscos foi adequada conforme os critérios estabelecidos pela organização. Caso não seja satisfatória, a atividade pode ser reiniciada de forma que se possa revisar, aprofundar e detalhar ainda mais a avaliação, assegurando que os riscos possam ser avaliados corretamente.

TRATAMENTO DO RISCO:

Trata de implementar controles para reduzir/evitar os riscos. Dessa forma, outro ponto de decisão é explicitado, em que se o tratamento do risco não for satisfatório, ou seja, não resultar em um nível de risco residual adequado aos padrões, deve-se iniciar novamente a atividade ou o processo até que os riscos residuais sejam explicitamente aceitos pelos gestores da organização.

ACEITAÇÃO DO RISCO:

Registra-se formalmente a aprovação dos planos de tratamento do risco e os riscos residuais resultantes, juntamente com a responsabilidade pela decisão.

COMUNICAÇÃO DO RISCO:

Desenvolve-se planos de comunicação dos riscos para assegurar que todos tenham consciência sobre os riscos e controles a serem adotados.

MONITORAMENTO E ANÁLISE CRÍTICA DOS RISCOS

Nesta etapa deve ocorrer o monitoramento contínuo dos riscos e seus fatores a fim de identificar eventuais mudanças no contexto. Dessa forma, certificando que o processo de gestão de riscos de segurança da informação e as atividades relacionadas permaneçam apropriados nas circunstâncias presentes.

É importante lembrar que a norma ISO/IEC 27005 não inclui uma metodologia específica para a gestão de riscos de segurança da informação, cabendo a cada organização definir a melhor abordagem conforme o contexto na qual está inserida.

TI Verde

É um movimento global na área de TI para diminuir os efeitos do consumo de tecnologia nas cadeias produtivas e ecossistemas. O conceito envolve um conjunto de práticas ecológicas, como por exemplo, o armazenamento em nuvem, melhora no consumo de energia, a modernização de equipamentos para aumentar a vida útil e uma política eficiente de descarte.

Em um contexto amplo, é um movimento de conscientização sobre a gravidade da situação climática e reestruturação de cadeias produtivas, desde a extração da matéria-prima até o descarte de materiais.

As práticas de TI Verde podem ser divididas em três níveis:

TI Verde de incrementação tática:

Não modifica a infra-estrutura de TI nem as políticas internas, apenas incorpora medidas de contenção de gastos elétricos excessivos, como por exemplo, o uso de monitoramento automático de energia disponível nos equipamentos, o desligamento dos mesmos nos momentos de não-uso, a utilização de lâmpadas fluorescentes e etc.

TI Verde Estratégico:

Exige a convocação de uma auditoria sobre a infra-estrutura de TI e seu uso relacionado ao meio-ambiente, desenvolvendo e implementando novos meios viáveis de produção de bens ou serviços de forma ecológica, como por exemplo, a criação de uma nova infra-estrutura na rede elétrica visando à sua maior eficiência e sistemas computacionais de menor consumo elétrico.

Deep IT:

Mais amplo que os dois primeiros, incorpora o projeto e implementação estrutural de um parque tecnológico visando a maximização do desempenho com o mínimo gasto elétrico, isto inclui projetos de sistemas de refrigeração, iluminação e disposição de equipamentos no local com base nas duas primeiras estruturas anteriores.

Environmental, Social and Governance (ESG)

É um conjunto de padrões e boas práticas que visa definir se uma empresa é socialmente consciente, sustentável e corretamente gerenciada. Trata-se de uma forma de medir o desempenho de sustentabilidade de uma organização. Busca-se mensurar se a empresa é realmente uma opção viável de investimentos sustentáveis, capazes de gerar impactos positivos financeiros, sociais e ambientais.

Ambiental

O critério ambiental inclui exigências nesse campo, como:

- A gestão de resíduos.
- A política de desmatamento (caso aplicável).
- O uso de fontes de energia renováveis pela empresa.
- O posicionamento da empresa em relação a questões de mudanças climáticas.

Social

Entre os pontos analisados, incluem-se:

- taxa de turnover.
- plano de previdência para os funcionários.
- envolvimento dos funcionários com a gestão da empresa.
- benefícios e vantagens oferecidos aos funcionários, além do salário.
- salário justo em relação aos praticados dentro da empresa e também em relação ao mercado.

Governança

Nesse caso, busca entender se a gestão executiva e o conselho administrativo atendem aos interesses das várias partes interessadas da empresa.

Algumas questões avaliadas:

- Transparência financeira e contábil.
- Relatórios financeiros completos e honestos.
- Remuneração dos acionistas.

O setor de TI tem um peso grande em relação ao ESG, apresentando boas resoluções através do acesso a informações, abriu caminho para questões financeiras e de saúde em locais que não tinham acesso anteriormente.

Algumas medidas que podem ser implementadas pelo setor de TI:

- Passar os servidores para a alternativa virtual, diminuindo a pegada de carbono.
- A utilização de aplicativos com maior capacidade, de maneira que, ao usar um software com maior rapidez, evitando ter que usar sua capacidade máxima que implica em um gasto maior de energia.
- Uso de drones para encontrar focos de incêndio.
- O uso da inteligência artificial para reconhecer rostos e adquirir dados.
- Melhorias dos sistemas de segurança com o objetivo de acionar alarmes para impedir acidentes.
- A implementação e concordância com as leis, através da LGPD.

Cidades inteligentes

São espaços urbanos caracterizados pela utilização generalizada de Tecnologias da Informação e da Comunicação (TIC 's), com o **objetivo de melhorar a eficiência político-econômica e amparar o desenvolvimento humano e social**, promovendo assim, a qualidade de vida de seus cidadãos.

Uma cidade é considerada inteligente quando há impulsionadores de crescimento econômico sustentável, elevada qualidade de vida e gestão consciente dos recursos naturais, por meio de uma governança participativa e democrática. Além disso, outros aspectos que devem ser levados em conta na classificação de cidades como inteligentes, como a mobilidade urbana, o compromisso com os assuntos ambientais e com as questões sociais.

Objetivos e características de uma cidade inteligente:

- Garantir acesso à cultura e oferecer educação de qualidade.
- Promover o desenvolvimento econômico com planos para a indústria, inovação e iniciativas empreendedoras
- Utilização de tecnologias inovadoras, como inteligência artificial (AI), sensores avançados e redes de dados de alta velocidade.
- Utilização de redes sociais e fóruns digitais como facilitadores da comunicação entre os habitantes e o poder público.
- Utilização de diversas tecnologias aplicadas às Cidades Inteligentes.

Segundo o Cities in Motion Index, as **5 cidades mais inteligentes do mundo são**:

Londres: Ocupa o 1° lugar por conta da sua performance em quase todos os quesitos analisados. Ocupou também o 1° lugar em capital humano, isso porque a cidade investe em um alto número de escolas de negócios e universidades de qualidade.

Nova York: Ocupa o 2° lugar devido sua liderança em economia, devido ao seu capital humano, tecnologia, planejamento urbano, alcance internacional e mobilidade

urbana. É o centro econômico mais importante do mundo e abriga cerca de 7.000 empresas de alta tecnologia

Amsterdã: É uma importante potência europeia, com investimentos em tecnologia financeira, eficiência energética e cultura. Como 90% da cidade utiliza bicicletas como meio de transporte, foi implantado um serviço automatizado de compartilhamento de bicicletas.

Paris: É uma cidade caracterizada por ser aberta à inovação e por oferecer a rede de dados aberta aos moradores. Para promover um transporte limpo através do uso de bicicletas e carros elétricos, isso influencia também na aplicação da IoT para otimizar o fluxo de pessoas e veículos.

Reykjavik: É a cidade mais populosa da Islândia, onde 99% de sua produção de eletricidade e mais de 80% da produção de total de energia vêm da energia hidrelétrica e geotérmica, o que torna seus edifícios e construções naturalmente “verdes”. Além disso, apresentou um documento com políticas climáticas objetivando se tornar uma cidade com emissão zero de carbono.

REFERÊNCIAS

https://ostec.blog/geral/iso-27000-vantagens-certificacao-seguranca/

https://blog.idwall.co/iso-27001/

https://www.certifiquei.com.br/iso-27002/

https://www.microserviceit.com.br/iso-27002/

https://www.mjvinnovation.com/pt-br/blog/o-que-e-ti-verde-e-por-que-devemos-investir-nisso

https://www.totvs.com/blog/business-perfomance/esg/

https://www.dinamio.com.br/blog/2022/08/04/esg-o-que-e-e-como-a-ti-pode-ajudar-a-implementar/#:~:text=O%20papel%20da%20TI,que%20n%C3%A3o%20teriam%20acesso%20anteriormente.

https://www.eosconsultores.com.br/cidades-inteligentes/

https://fgvprojetos.fgv.br/noticias/cidades-mais-inteligentes-do-mundo#:~:text=Segundo%20o%20estudo%2C%20T%C3%B3quio%2C%20Londres,transporte%2C%20capital%20humano%20e%20governan%C3%A7a.

https://www.isms.online/iso-27004/

https://www.aedb.br/seget/arquivos/artigos12/57616827.pdf