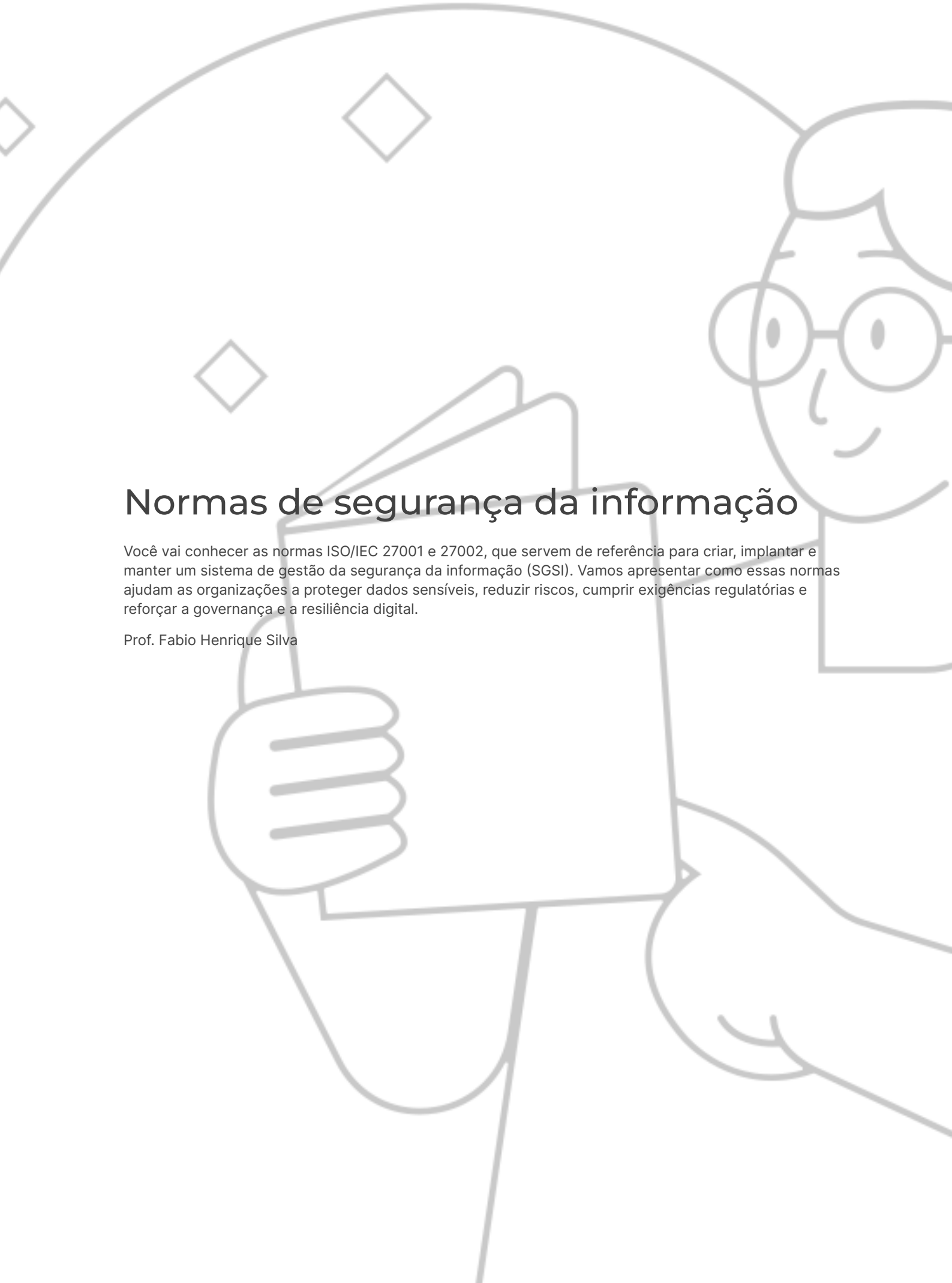


Normas de segurança da informação

Você vai conhecer as normas ISO/IEC 27001 e 27002, que servem de referência para criar, implantar e manter um sistema de gestão da segurança da informação (SGSI). Vamos apresentar como essas normas ajudam as organizações a proteger dados sensíveis, reduzir riscos, cumprir exigências regulatórias e reforçar a governança e a resiliência digital.

Prof. Fabio Henrique Silva

Objetivos

- Reconhecer as finalidades e os benefícios da adoção das normas ISO/IEC 27001 e 27002.
- Identificar as aplicações das normas ISO/IEC 27001 e ISO/IEC 27002.
- Analisar o conceito e as técnicas de auditoria de segurança

Introdução

Neste vídeo, veremos os conceitos que serão explorados ao longo do conteúdo: normas ISO/IEC 27001 e 27002, enfatizando a aplicação conjunta de ambas na implementação e manutenção de um sistema de gestão da segurança da informação.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Normas ISO e segurança da informação

A segurança da informação tornou-se um pilar estratégico para as organizações. Conhecer as normas que tratam do tema é passo decisivo para implantar um sistema de gestão da segurança da informação (SGSI) eficiente.

Neste vídeo, abordaremos as ISO/IEC 27001 e ISO/IEC 27002, assim como a correlação entre elas e um sistema de gestão da segurança da informação (SGSI).

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A ISO - International Organization for Standardization (Organização Internacional de Padronização) é uma entidade fundada em 1947, sediada na Suíça e que congrega organismos de normalização nacionais. Sua principal atividade é elaborar padrões para especificações e métodos de trabalho nas mais diversas áreas da sociedade.

Entre as diversas normas elaboradas pela ISO, destaca-se a ISO/IEC 27001, que trata especificamente da gestão da segurança da informação. Essa norma, reconhecida internacionalmente, estabelece diretrizes fundamentais para que organizações desenvolvam sistemas eficazes na proteção de dados e na mitigação de riscos relacionados à informação.

Segundo a ABNT NBR ISO/IEC 27001:2022 (Tecnologia da informação – Sistemas de gestão de segurança da informação – Requisitos), a norma foi elaborada para definir os requisitos necessários à criação, implementação, manutenção e melhoria contínua de um sistema de gestão da segurança da informação (SGSI). A versão atual destaca especialmente o contexto organizacional, o alinhamento com os objetivos estratégicos da empresa e o papel ativo da alta liderança na condução da segurança da informação.

> Cabe à alta direção não só decidir pela adoção de um sistema de gestão da segurança da informação (SGSI), mas também mostrar envolvimento real com sua eficácia, garantindo que a segurança da informação faça parte dos processos da empresa e esteja alinhada aos seus objetivos estratégicos.

A ISO/IEC 27001:2022 cita alguns fatores de influência para o estabelecimento e a implementação do SGSI, com um foco maior no contexto organizacional. Esses fatores incluem:

1. Necessidades.
2. Objetivos.
3. Requisitos de segurança.
4. Processos organizacionais.
5. Tamanho e estrutura da organização.
6. Considerações sobre as partes interessadas (stakeholders) e seu impacto nas decisões relacionadas à segurança da informação.

O SGSI preserva a tríade CID (confidencialidade, integridade e disponibilidade) da informação, aplicando um processo de gestão de riscos. Com isso, as partes interessadas (stakeholders) poderão ter maior confiança de que os riscos serão gerenciados de forma adequada, considerando não apenas os controles técnicos, mas o contexto organizacional e o envolvimento ativo da alta direção.

Segundo a ABNT (2022), um SGSI deve estar integrado aos **processos da organização** e à sua estrutura de **administração global**, garantindo que a segurança da informação seja considerada desde a fase de planejamento de processos, sistemas e controles, sempre em sintonia com os objetivos estratégicos e o cenário da organização.

> A ISO/IEC 27001, em conjunto com a ISO/IEC 27002 (Controles de Segurança da Informação), é uma das principais referências para quem busca lidar com a segurança da informação de forma eficiente e eficaz. As duas normas destacam a importância do contexto organizacional, da atuação da liderança e da gestão integrada de riscos.

As normas técnicas nacionais são estabelecidas por um organismo nacional de normalização para aplicação em dado país. No Brasil, as Normas Brasileiras (NBRs) são elaboradas pela ABNT (Associação Brasileira de Normas Técnicas).

Atenção

A ABNT é reconhecida pelo Estado brasileiro como o Fórum Nacional de Normalização, e as NBRs são reconhecidas formalmente como as normas brasileiras. As nomenclaturas das normas ISO/IEC 27001 e 27002 são, respectivamente, ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002.

Ao longo do texto, podem ser consideradas tanto as normas brasileiras quanto as normas ISO, mas as NBRs são idênticas às normas ISO, sendo possível fazer referência a ambas sem prejuízo no contexto do conteúdo e no entendimento.

Certificados

Uma visão geral da situação dos certificados no mundo pode ser obtida através dos dados disponibilizados no The ISO Survey of Certifications.

Trata-se de uma pesquisa anual do número de certificados válidos para os padrões do sistema de gerenciamento ISO em todo o mundo. Os dados são fornecidos pelos organismos de certificação credenciados. Veja mais a seguir.

Certificado

É o documento emitido por um organismo de certificação.

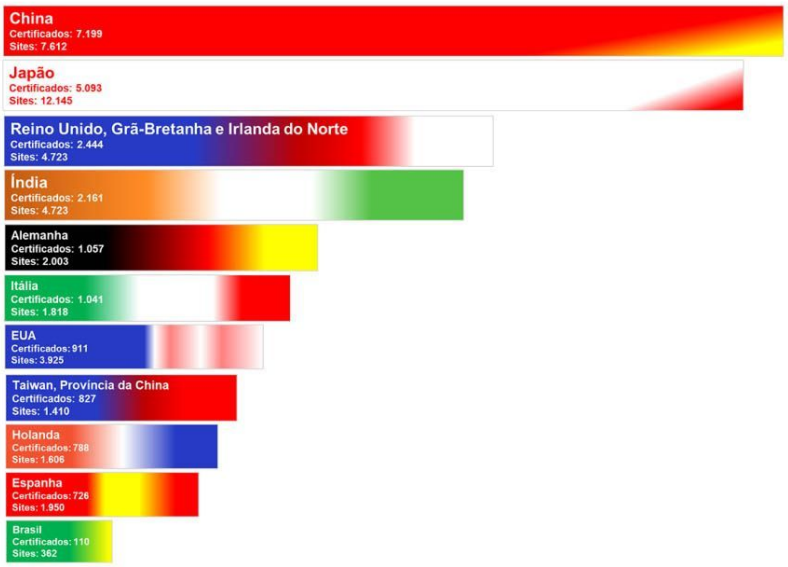
Site

É um local permanente em que uma organização realiza trabalho ou serviço.

O gráfico a seguir foi extraído da planilha disponível na página da ISO. Ele exibe um trecho do **número total de certificados válidos** e o **número total de sites para o padrão ISO/IEC 27001:2013**. Até o momento da redação desse texto, essa é a última versão oficial divulgada com esse nível de detalhamento.

Conteúdo interativo

Acesse a versão digital para ver mais detalhes da imagem abaixo.



Lista dos 10 países com maior número de certificados. O Brasil aparece na posição 39.

Tendências

O estudo das normas técnicas não se limita apenas ao aprendizado dessas normas aqui apresentadas.

Um caminho que pode ser seguido é analisar também outras normas de sistemas de gestão, tais como: qualidade, meio ambiente, conhecimento, ativos, educação etc.

Atividade 1

Em um cenário de aumento constante dos riscos cibernéticos, uma organização decide implementar um sistema de gestão da segurança da informação (SGSI) fundamentado nas normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022. Qual das alternativas representa um aspecto essencial para a eficácia de um SGSI, conforme orientam as normas ISO/IEC 27001 e ISO/IEC 27002?

A Priorizar a implementação de controles técnicos em setores específicos da organização, com foco em ações pontuais relacionadas à segurança da informação.

B Concentrar os esforços do SGSI em tarefas operacionais rotineiras, promovendo agilidade na adoção das medidas de segurança.

C Adotar medidas voltadas à proteção de instalações e equipamentos, considerando o ambiente físico como ponto central da estratégia de segurança.

D Estabelecer um setor dedicado à segurança da informação para coordenar as ações e decisões relacionadas ao tema dentro da organização.

E Definir requisitos e objetivos de segurança alinhados ao contexto organizacional, com envolvimento ativo da alta direção.

A alternativa E está correta.

Um SGSI eficaz, de acordo com as normas ISO/IEC 27001 e 27002, deve integrar os requisitos de segurança à estratégia e aos processos organizacionais, para que a alta direção esteja comprometida e envolvida na gestão dos riscos. Essa abordagem promove uma visão holística da segurança da informação, diferenciando-se das demais alternativas que propõem medidas isoladas ou reduzem elementos essenciais para a proteção e continuidade dos negócios.

Norma ISO/IEC 27001: SGSI – Requisitos

A norma internacional ISO/IEC 27001 define os requisitos para implantar e manter um sistema de gestão da segurança da informação (SGSI). Voltada à proteção dos ativos de informação, ela busca assegurar a confidencialidade, integridade e disponibilidade dos dados. A versão mais recente, de 2022, também reforça a importância de alinhar a segurança da informação aos objetivos estratégicos da organização. Com base nesse padrão, é possível entender as responsabilidades das empresas em relação à gestão e proteção das informações.

Neste vídeo, apresentaremos a ISO/IEC 27001. Essa norma detalha os requisitos para a implementação e manutenção de um sistema de gestão da segurança da informação (SGSI).

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Conforme a ABNT NBR ISO/IEC 27001:2022, o título da norma permanece o mesmo da versão anterior (2013): Sistemas de Gestão da Segurança da Informação – Requisitos. Porém, a sua abordagem foi aprimorada para refletir uma visão mais estratégica e integrada.

> A ISO/IEC 27001:2022 especifica os requisitos para estabelecer, implementar, manter e aprimorar continuamente um SGSI, enfatizando a integração da segurança da informação com a governança e os objetivos estratégicos da organização, dentro de um contexto que considera fatores internos e externos.

Além disso, a versão 2022 reforça a gestão de riscos e oportunidades, ampliando o escopo para que o tratamento dos riscos seja dinâmico e adaptável às mudanças do ambiente organizacional.

A característica principal, ou palavra-chave, continua sendo DEVE, indicando de forma clara as obrigações da organização. Por exemplo, na seção 4.3, a organização deve determinar os limites e a aplicabilidade do SGSI para definir o escopo, considerando o contexto e as necessidades específicas de forma abrangente e contínua.

Observe, a seguir, sobre o que a Norma ISO/IEC 27001 é e não é.

A Norma ISO/IEC 27001 é:

- Uma metodologia estruturada reconhecida internacionalmente dedicada à segurança da informação.
- Um processo definido para validar, implementar, manter e gerenciar a segurança da informação.
- Um grupo detalhado de controles compreendidos das melhores práticas de segurança da informação.
- Desenvolvido para apoiar organizações na proteção de informações, considerando o contexto e as partes interessadas.

A Norma ISO/IEC 27001 não é:

- Um padrão técnico.
- Um produto ou tecnologia dirigida.
- Uma metodologia de avaliação do equipamento.
- Mas pode exigir a utilização de níveis de garantia dos equipamento.

A versão mais recente da norma, válida até o momento da redação deste texto, é a ISO/IEC 27001:2022, que substitui a edição anterior de 2013.

A versão 2013 trouxe como uma das novidades o alinhamento com a estrutura de alto nível (HLS), também conhecida como Anexo L, que padroniza definições e estruturas de diferentes sistemas de gestão ISO.

> O Anexo L é uma seção da ISO/IEC Directives, Part 1, Consolidated ISO Supplement, que padroniza definições e estruturas de diferentes sistemas de gestão ISO. Com isso, a norma está alinhada com outros padrões de sistemas de gestão, como ISO 9001, ISO 14000, ISO 20000, ISO 22000, ISO 22301.

Na versão 2022 da ISO/IEC 27001, a norma continua seguindo o alinhamento com o Anexo L, mas com ênfase no **contexto organizacional**, **partes interessadas** e maior foco na **gestão de riscos e desempenho do SGSI**.

Atenção

A estrutura de alto nível não pode ser modificada; por sua vez, podem ser acrescentadas subcláusulas e textos específicos para cada disciplina abordada.

Veja a tabela a seguir:

Cláusula 1	Escopo
Cláusula 2	Referência normativa
Cláusula 3	Termos e definições
Cláusula 4	Contexto da organização
Cláusula 5	Liderança
Cláusula 6	Planejamento
Cláusula 7	Suporte
Cláusula 8	Operação
Cláusula 9	Avaliação de Desempenho
Cláusula 10	Melhoria

Tabela 1: Estrutura geral de uma norma de gestão que segue as diretrizes do Anexo L.
Fabio Henrique Silva

O ISO/IEC *Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO*, documento do qual o Anexo L faz parte, pode ser lido na página da ISO.

Para você que está começando a se familiarizar com a ISO/IEC 27001:2022, uma boa maneira de ter uma visão geral dos conteúdos é analisando a estrutura e o sumário das normas. A estrutura da versão 2022 dessa ISO pode ser conferida na nova organização, que segue um formato mais focado na governança e no ciclo de vida do SGSI, com maior ênfase na análise de riscos e na integração estratégica com os objetivos organizacionais.

Algumas razões para adotar a norma incluem:

- Melhoria contínua na gestão da segurança da informação, alinhada com os objetivos estratégicos.
- Diferenciação competitiva no mercado, com credibilidade internacional.
- Satisfação das necessidades e expectativas dos clientes e partes interessadas.
- Padrão globalmente aceito para a proteção de informações.
- Maior clareza nas responsabilidades da equipe de segurança da informação.
- Envolvimento de toda a organização, incluindo áreas além de TI, com foco na governança e nos controles organizacionais.
- Conformidade com legislações, regulamentações e requisitos contratuais.

A Norma ISO/IEC 27001 é passível de certificação acreditada. Alguns **benefícios da certificação ISO/IEC 27001** incluem:

- Responsabilidade reduzida devido às políticas e aos procedimentos não implementados ou reforçados.
- Oportunidade de identificar e eliminar fraquezas.
- A gerência participa da Segurança da Informação.
- Revisão independente do seu SGSI.
- Fornece segurança a todas as partes interessadas.
- Melhor consciência da segurança.
- Une recursos com outros sistemas de gerenciamento.
- Mecanismo para medir o sucesso do sistema.

O ISO/IEC *Directives, Part 1, Consolidated ISO Supplement – Procedures specific to ISO*, documento do qual o Anexo L faz parte, pode ser lido na página da ISO.

Atividade 2

No contexto da implementação de um SGSI, a ISO/IEC 27001:2022 apresenta aprimoramentos em relação à versão de 2013, embora mantenha o mesmo título. Qual das alternativas melhor descreve essas principais inovações da ISO/IEC 27001:2022?

A A ISO/IEC 27001:2022 enfatiza a integração da segurança da informação com a governança, o desempenho do SGSI e a gestão dinâmica de riscos em um contexto organizacional.

B A ISO/IEC 27001:2022 propõe uma abordagem com foco operacional na implementação de controles, priorizando práticas previamente consolidadas pela organização.

C Na ISO/IEC 27001:2022, a gestão de riscos é tratada por meio de métodos que privilegiam a análise de cenários recorrentes, com foco em procedimentos já mapeados.

D A ISO/IEC 27001:2022 amplia a flexibilidade na definição da estrutura de gestão, permitindo ajustes metodológicos conforme as particularidades de cada organização.

E A ISO/IEC 27001:2022 detalha mecanismos técnicos para proteção da informação, propondo diretrizes alinhadas ao ambiente tecnológico da organização.

A alternativa A está correta.

Embora o título da norma permaneça inalterado, a versão 2022 introduz melhorias significativas na abordagem do SGSI. Essas melhorias incluem a integração dos controles de segurança com os objetivos estratégicos, a ênfase na governança e no desempenho, bem como uma abordagem mais dinâmica e

adaptável para a gestão de riscos, considerando tanto fatores internos quanto externos. As demais alternativas apresentam informações que não condizem com as inovações reais da norma.

Norma ISO/IEC 27002: controles de segurança da informação

A ISO/IEC 27002, diferentemente da ISO/IEC 27001, não é uma norma de requisitos, mas uma especificação de controles de segurança da informação. Sua versão 2022 trouxe uma nova organização para os controles de segurança da informação, facilitando aplicação e alinhamento com as necessidades das organizações. Além disso, a norma introduziu atributos que permitem classificar os controles de maneira mais eficiente, proporcionando maior flexibilidade na sua implementação. A seguir, são apresentados um resumo dessa nova estrutura, os principais atributos dos controles e a forma como a norma os organiza para apoiar a gestão da segurança da informação.

Neste vídeo, abordaremos a ISO/IEC 27002, com ênfase na organização dos controles de segurança em quatro categorias: organizacionais, de pessoas, físicos e tecnológicos.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

A norma **ABNT NBR ISO/IEC 27002:2022** (Segurança da Informação, Segurança Cibernética e Proteção à Privacidade — Controles de Segurança da Informação), apresenta as melhores práticas para a gestão da segurança da informação, mantendo o foco no que convém.

> A versão 2022 organiza os controles de forma revisada, substituindo a estrutura de 14 seções por quatro grupos temáticos.

Nesta nova estrutura, a norma recomenda 93 controles básicos:

- Organizacionais (37 controles)
- De pessoas (8 controles)
- Físicos (14 controles)
- Tecnológicos (34 controles)

Em cada grupo temático são apresentados:

- Os objetivos dos controles, definindo o que se espera alcançar.
- Os controles correspondentes que podem ser aplicados para atingir esses objetivos.

Na versão atual da norma, 27002:2022, foram adicionados alguns controles para casos específicos referentes à segurança da informação, são eles:

- Inteligência de ameaças (compreensão da lógica das ameaças).
- Segurança da informação para uso de serviços em nuvem.
- Prontidão da TIC para continuidade de negócios.
- Monitoramento de segurança física.
- Gerenciamento de configurações.
- Exclusão de informações.
- Mascaramento de dados.
- Prevenção de vazamento de dados.
- Atividades de monitoramento.
- Filtragem da web.
- Codificação segura.

As descrições dos controles foram revisadas para acompanhar a reorganização e a nova estrutura dos grupos temáticos. Cada controle apresenta:

Declaração

Orienta o controle para atingir seu objetivo, alinhada à mitigação dos riscos por meio de processos, políticas, dispositivos ou prática.

Segundo a ISO/IEC 27000 (2018), o controle é uma medida que pode modificar o risco, seja ele através de um processo, política, dispositivo, prática ou outras ações que modifiquem a ameaça e/ou a vulnerabilidade e, consequentemente, o risco.

Diretrizes para implementação

Fornece orientações detalhadas para a aplicação prática do controle, auxiliando na obtenção dos objetivos de segurança.

As diretrizes podem não ser totalmente adequadas ou suficientes em todas as situações e podem, portanto, não atender completamente aos requisitos de controle específicos de uma organização.

Informações adicionais

Apresenta mais dados que podem ser considerados, como questões legais e referências normativas. Se não existem informações adicionais, esta parte não é mostrada no controle.

Para tornar a categorização e a organização mais intuitivas, os controles passaram a contar com novos atributos que facilitam sua localização dentro da norma. Vejamos quais são eles!

Tipo de controle
Preventivo, detectivo e corretivo.

Propriedades da segurança da informação
Confidencialidade, integridade e disponibilidade.

Conceitos de segurança cibernética
Identificar, proteger, detectar, responder e recuperar.

Capacidades operacionais
Governança, gestão de ativos, segurança física, continuidade, entre outras.

Domínios de segurança
Governança e ecossistema, proteção, defesa e resiliência.

A nova estruturação dos atributos dos controles permite que cada organização identifique com mais facilidade aqueles que melhor atendem a suas necessidades e seus objetivos, tornando sua aplicação mais eficiente.

Em síntese, a atualização da ISO/IEC 27002:2022 reflete uma abordagem mais estruturada e flexível, permitindo que as organizações adaptem seus controles de segurança da informação de maneira mais eficaz às suas necessidades e ao cenário tecnológico em constante evolução.

Atividade 3

A ISO/IEC 27002:2022 fornece diretrizes para a implementação de controles da segurança da informação, focando a implementação de controles. A versão de 2022 trouxe mudanças significativas, como a reorganização dos controles e a adição de novos atributos. Com base nas informações apresentadas sobre a norma, indique as principais mudanças introduzidas pela versão 2022 da ISO/IEC 27002.

A A versão 2022 da ISO/IEC 27002 manteve a estrutura anterior de 14 seções, mas adicionou novos controles para a segurança em nuvem e inteligência de ameaças.

B A norma agora organiza os controles em quatro grupos temáticos, com a adição de novos controles relacionados à segurança da informação para uso em nuvem e ao monitoramento de segurança física.

C A versão 2022 passou a incluir a segurança cibernética como um dos principais objetivos dos controles, mas manteve a estrutura de 14 seções para garantir maior flexibilidade.

D A ISO/IEC 27002:2022 recomenda 93 controles com a introdução de atributos como governança, continuidade e proteção, mas manteve a classificação de controles em apenas dois tipos: preventivos e corretivos.

E A ISO/IEC 27002:2022 optou por eliminar os controles sobre segurança física, priorizando controles tecnológicos e de nuvem.

A alternativa B está correta.

A ISO/IEC 27002:2022 promoveu uma reformulação significativa na estrutura dos controles, adotando uma organização mais moderna e categorizada, que facilita a aplicação prática nas organizações. Essa reformulação contribui para uma visão mais estratégica da segurança da informação, especialmente ao incluir temas atuais como computação em nuvem e vigilância física. As demais alternativas erram ao manter elementos da estrutura antiga da norma ou ao introduzir conceitos que não condizem com a versão 2022, como a exclusão da segurança física ou a classificação simplificada de controles.

Estudo de caso: análise de riscos e execução de controles de segurança

A gestão da segurança da informação tem como objetivo proteger os ativos mais valiosos da organização. Normas como a ISO/IEC 27001:2022 e a ISO/IEC 27002:2022 oferecem uma base confiável para implantar um sistema de gestão da segurança da informação (SGSI), facilitando a identificação de riscos, a aplicação de controles e a adoção de boas práticas reconhecidas no mercado. A seguir, veremos como analisar os requisitos do negócio, identificar riscos e definir as medidas adequadas para reduzir ameaças e proteger dados e recursos da empresa.

Neste vídeo, veremos o contexto de uma situação envolvendo uma empresa fictícia, através da qual demonstraremos a aplicação das normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022. Acompanhe!

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Neste estudo de caso, analisaremos a abordagem da organização fictícia Tech & Safe, uma empresa de médio porte com foco em soluções de segurança de TI, que recentemente passou por uma avaliação de riscos para proteger suas informações sensíveis. A partir dessa análise, foram identificados riscos críticos relacionados a acesso indevido, vazamento de dados e ausência de monitoramento adequado, entre outros. O objetivo é mostrar como a Tech & Safe lidou com esses desafios e os passos que deu para implementar controles de segurança conforme as normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Situação-problema

Em um monitoramento de rotina no setor financeiro da Tech & Safe, com base nos requisitos para gestão da segurança da informação estabelecidos na ISO/IEC 27001:2022, o sistema de segurança da empresa detectou diversas tentativas de log-on fora do horário habitual. Nessas tentativas, notou-se que foi utilizado o mesmo conjunto de credenciais. Com o desenrolar da inspeção dos requisitos de segurança na documentação da Tech & Safe, foram revelados os seguintes problemas:

Compartilhamento de credenciais

As credenciais estavam sendo compartilhadas entre departamentos, permitindo que usuários de funções distintas acessassem áreas restritas de forma indevida.

Falta de segregação de funções

A inexistência de controles de acesso individualizados facilitou o acesso não autorizado a dados sensíveis.

Ausência de monitoramento eficaz

O sistema de logs não estava configurado para registrar e alertar de forma adequada, o que culminou em atrasos na detecção de comportamentos anômalos.

Relação entre requisitos de negócios, riscos e medidas de segurança

Para contextualizar o problema, é importante relacionar os requisitos de negócios com os riscos identificados e as necessidades de segurança. Vamos lá!

Requisitos de negócios

- Garantir a confidencialidade dos dados
- Preservar a integridade das informações
- Assegurar a continuidade dos serviços

Riscos identificados

- Acesso indevido
- Compartilhamento de credenciais
- Ausência de monitoramento eficaz

Medidas de segurança

- Controle de acesso individualizado e segregado
- Políticas rigorosas de senhas e adoção de autenticação multifator (MFA)
- Logs centralizados, alertas automáticos e monitoramento contínuo

Avaliação dos riscos

Com base no cenário identificado, o próximo passo seria avaliar os riscos detectados e classificá-los nestes termos:

1

Impacto
A gravidade que determinado risco poderia causar à empresa.

Categorias: Muito alto, Alto, Médio ou Baixo.

2 Probabilidade
Avaliação da probabilidade de ocorrência do risco.

Categorias: Muito alta, Alta, Média ou Baixa.

3
Classificação
A quantificação do risco em termos de seu impacto e de sua gravidade.

Categorias: Crítico, Alto, Médio ou Baixo.

A classificação do risco como Crítico seria a junção de um impacto Muito alto ou Alto e uma probabilidade Muito alta ou Alta*;* a classificação como Altose daria por um impacto Alto ou Médio e uma probabilidade Alta ou Média*;* o risco seria classificado como Médio quando o impacto fosse Médio e a probabilidade Média ou Baixa; por fim, a classificação do risco como Baixo ocorreria quando o impacto fosse Baixo e a sua probabilidade de ocorrência Baixa ou Muito Baixa. A tabela a seguir ilustra a relação entre impacto, probabilidade e a classificação dos riscos levantados no monitoramento do setor financeiro da Tech & Safe.

Risco	Impacto	Probabilidade	Classificação
Acesso indevido	Muito Alto	Alta	Crítico
Compartilhamento de credenciais	Alto	Alta	Alto
Ausência de monitoramento	Alto	Média a Alta	Alto

Tabela: Matriz de riscos.
Kleber de Aguiar (curador).

Após a identificação, avaliação e classificação dos riscos, é possível compreender claramente as áreas mais vulneráveis da organização e a prioridade de ações que precisam ser tomadas para mitigar esses riscos. Com a tabela de riscos estabelecida, a Tech & Safe agora tem uma visão detalhada sobre os potenciais impactos e probabilidades de ocorrência dos incidentes, permitindo a priorização de esforços de segurança de forma eficaz.

O próximo passo será determinar as medidas corretivas e preventivas que serão implementadas para minimizar os riscos mais críticos, assegurando a continuidade dos negócios e a proteção das informações sensíveis, conforme as exigências das normas ISO/IEC 27001:2022 e 27002:2022.

Atividade 1

Com base no estudo de caso da Tech & Safe, considere a necessidade de mitigar os riscos relacionados ao acesso indevido e ao compartilhamento de credenciais. Considerando os princípios da ISO/IEC 27001:2022 e da ISO/IEC 27002:2022, qual das opções a seguir representa uma ação estratégica mais adequada e sustentável para reduzir esses riscos em médio e longo prazo?

A Adotar autenticação multifator (MFA) nos setores com maior sensibilidade de dados.

B Criar um manual interno com boas práticas e confiar que os colaboradores seguirão as orientações.

C Implementar controles de acesso individualizados e políticas de segurança robustas, incluindo autenticação multifator, segregação de funções e monitoramento contínuo.

D Realizar treinamentos periódicos sobre segurança da informação, sem alterar os sistemas de controle de acesso.

E Permitir o uso compartilhado de credenciais entre equipes confiáveis, desde que haja registro de acesso em logs.

A alternativa C está correta.

Controles de acesso individualizados e políticas de segurança bem definidas fazem parte de um conjunto de medidas alinhadas aos princípios das normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, que propõem uma abordagem contínua e estruturada para reduzir riscos à segurança da informação. A integração desses controles com a segregação de funções e o uso de autenticação multifator (MFA) busca assegurar a confidencialidade, integridade e disponibilidade das informações — a chamada tríade CID — especialmente frente às falhas observadas no caso da Tech & Safe.

Implementação do SGSI: requisitos e controles de segurança

Com os riscos identificados e classificados, o próximo passo é implementar medidas de segurança para mitigar ou eliminar esses riscos, em concordância com os requisitos de implementação e manutenção de um sistema de gestão de segurança da informação (SGSI) expressos na ISO/IEC 27001:2022 e com a implementação de controles de segurança da informação detalhadas na norma 27002:2022. Neste estudo, veremos omo essas medidas são integradas ao sistema de gestão de segurança da informação (SGSI), a partir de controles técnicos, administrativos e físicos, e como elas se refletem em políticas e procedimentos da organização.

Neste vídeo, vamos conferir a aplicação prática das normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022 na situação-problema da empresa fictícia Tech & Safe.

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Plano de tratamento de riscos

Para cada risco identificado, um controle específico foi implementado, com prazos e responsáveis definidos, como pode ser visto na tabela seguinte.

Risco	Controle implementado	Prazo	Responsável

Acesso indevido	Sistema de gerenciamento de identidades com perfis individualizados e segregação de funções	30 dias	Gestor de TI
Compartilhamento de credenciais	Política de senhas com requisitos de complexidade e expiração (90 dias) e implementação de autenticação multifator (MFA)	45 dias	Equipe de segurança
Ausência de monitoramento	Implementação de sistema de logs centralizados e alertas automáticos	30 dias	Administrador de sistemas

Tabela: Tratamento de riscos.
Kleber de Aguir.

Exemplo de política de segurança da informação

Após a aplicação das medidas de segurança, a política de segurança da informação (PSI) da Tech & Safe passou a seguir as melhores práticas das normas ISO/IEC 27001:2022 e ISO/IEC 27002:2022, com foco em reduzir os riscos identificados durante a avaliação de segurança.

A seguir, confira todos os controles, os que já existiam e os aplicados após o incidente, com suas respectivas referências normativas.

Gestão de incidentes de segurança

A PSI define claramente o processo para identificação, resposta e resolução de incidentes de segurança, como acesso não autorizado e vazamento de dados.

Referência: ISO/IEC 27001:2022, cláusula 6.1.2 (Ações para tratar riscos e oportunidades) e ISO/IEC 27002:2022, seção 16 (Gestão de incidentes de segurança da informação).

Controle de acesso e autenticação multifatorial (MFA)

A PSI implementa a autenticação multifatorial (MFA) para proteger os sistemas críticos contra acessos não autorizados, especialmente no caso de phishing ou vazamento de credenciais.

Referência: ISO/IEC 27001:2022, cláusula 9.1 (controle de acesso) e ISO/IEC 27002:2022, seção 9.4 (controles de acesso).

Classificação da informação

A política estabelece a classificação da informação (Confidencial, restrita, pública) para assegurar que dados sensíveis recebam proteção apropriada.

Referência: ISO/IEC 27001:2022, cláusula 8.2 (classificação da informação) e ISO/IEC 27002:2022, seção 8.2 (classificação e manuseio da informação).

Segurança física e ambiental

A PSI define controles de segurança física para proteger os ativos de TI contra roubo ou acesso não autorizado.

Referência: ISO/IEC 27001:2022, cláusula 11.1 (segurança física e ambiental) e ISO/IEC 27002:2022, seção 11.1 (controle físico e ambiental).

Monitoramento e auditoria

A PSI estabelece a necessidade de monitoramento contínuo e auditoria de logs para detectar atividades suspeitas e garantir a conformidade com a segurança da informação.

Referência: ISO/IEC 27001:2022, cláusula 9.4 (monitoramento e auditoria) e ISO/IEC 27002:2022, seção 12.4 (monitoramento e auditoria).

Plano de continuidade de negócios

A política estabelece procedimentos para a continuidade dos negócios, incluindo backup de dados e planos de recuperação em caso de incidente.

Referência: ISO/IEC 27001:2022, cláusula 17 (continuidade de negócios) e ISO/IEC 27002:2022, seção 17.1 (planejamento de continuidade).

A política de segurança é parte fundamental do sistema de gestão de segurança da informação (SGSI) e deve ser implementada e mantida conforme as melhores práticas de segurança estabelecidas pela ISO/IEC 27001:2022 e ISO/IEC 27002:2022. A organização deve garantir que todos os controles técnicos e administrativos estejam em vigor para proteger suas informações e manter a conformidade com as normas internacionais, criando um ambiente seguro e resiliente.

É importante destacar a aderência às normas de 2022, considerando as seguintes atualizações:

ISO/IEC 27001:2022

Implementação de controles de segurança, monitoramento contínuo, e a gestão de incidentes de segurança.

ISO/IEC 27002:2022:

Gestão de acesso, classificação da informação, controle físico, continuidade de negócios e conformidade

Para a eficácia e a relevância da política de segurança da informação, é essencial que ela seja revisada e atualizada periodicamente, conforme mudanças nas ameaças cibernéticas, nas necessidades da organização e nas evoluções das normas ISO/IEC.

Atividade 2

No contexto da implementação de medidas de segurança da informação, a integração de controles no sistema de gestão de segurança da informação (SGSI) é fundamental para a proteção das informações organizacionais. Para que a segurança da informação seja eficaz, são aplicados controles técnicos, administrativos e físicos de acordo com normas, como a ISO/IEC 27001:2022 e ISO/IEC 27002:2022.

Qual das alternativas descreve de forma adequada um aspecto importante da implementação de controles de segurança no SGSI?

A A política de segurança da informação (PSI) pode priorizar a gestão de incidentes como eixo central, considerando outros controles conforme as necessidades identificadas pela organização.

B A autenticação multifatorial (MFA) pode ser considerada uma medida complementar, especialmente quando já existem controles de senha que atendem a requisitos robustos de segurança.

C O monitoramento e a auditoria são ferramentas úteis para o controle de acessos e podem ser direcionadas a áreas específicas da segurança da informação conforme critérios internos.

D O plano de tratamento de riscos deve definir controles específicos para cada risco identificado, com prazos e responsáveis, garantindo que todos os riscos sejam mitigados.

E A segurança física e ambiental pode ser tratada de forma integrada aos controles técnicos, conforme o tipo de dado e infraestrutura utilizados pela organização.

A alternativa D está correta.

A gestão eficaz dos riscos em um SGSI exige um planejamento estruturado que permita à organização estabelecer ações concretas diante das vulnerabilidades identificadas. Atribuir responsabilidades, estabelecer prazos e direcionar recursos são elementos essenciais para que os controles de segurança tenham efetividade prática. Essa abordagem está em conformidade com os princípios da melhoria contínua e com a necessidade de demonstrar que os riscos estão sendo tratados de forma sistemática e mensurável, como previsto pelas normas da família ISO/IEC 27000.

Conceitos de auditoria

A auditoria é uma atividade essencial para verificar se um sistema de gestão da segurança da informação (SGSI) está funcionando corretamente. Ela ajuda a identificar se os processos estão sendo seguidos como planejado e se os riscos à segurança da informação estão sendo bem controlados. A seguir, vamos entender o que é auditoria, como ela funciona dentro das normas ISO/IEC 27001 e ISO/IEC 27002, e quais são suas etapas principais. Além disso, você verá como a auditoria contribui para melhorar continuamente a segurança da informação nas organizações.

Neste vídeo, apresentaremos os conceitos de auditoria, de acordo com as normas ISO/IEC 27001 e ISO/IEC 27002. Acompanhe!

Conteúdo interativo

Acesse a versão digital para assistir ao vídeo.

Certamente, você já percebeu a relevância das normas **ISO/IEC 27001** e **ISO/IEC 27002**, que objetivam o **estabelecimento**, a **implementação**, a **manutenção** e a **melhoria** de um **sistema de gestão da segurança da informação (SGSI)**, bem como a adoção de controles de segurança no processo de gestão desse sistema.

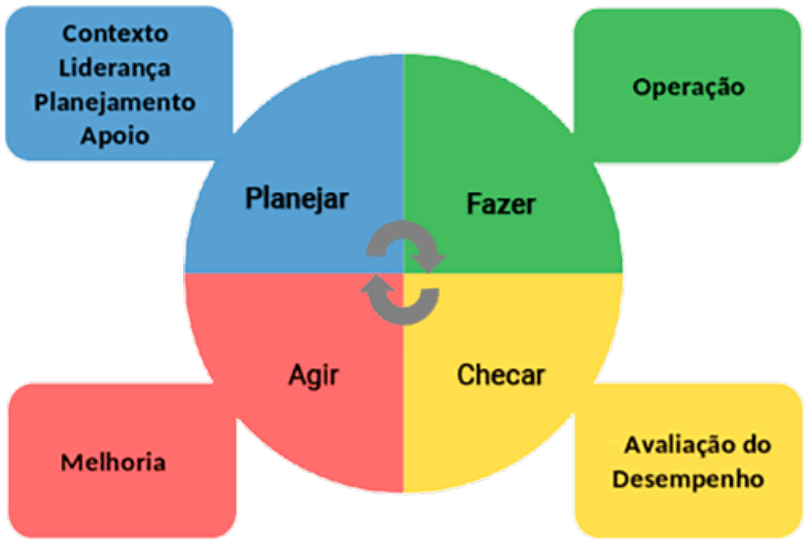
Atenção

A ISO/IEC 27001 é a norma que estabelece os diversos requisitos para gestão de um SGSI, desde sua concepção até sua manutenção e melhoria contínua, tendo como alvo identificar e tratar de forma adequada os riscos de segurança da informação.

Os diversos requisitos da ISO/IEC 27001 são estruturados nos moldes do ciclo PDCA (do inglês Plan – Planejar, Do – Fazer, Check – Checar e Act – Agir), conforme mostra o esquema a seguir.

Conteúdo interativo

Acesse a versão digital para ver mais detalhes da imagem abaixo.



Requisitos de SGSI da ISO 27001 e ciclo PDCA.

Como vimos, um dos requisitos da norma é **avaliação e desempenho**. E é aqui que entra a atividade de auditoria!

Veja como o Gabinete de Segurança Institucional da Presidência da República (GSI/PR) define o termo "auditoria":

> Processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos.
>
> —
>
> (Brasil, 2019)

Observe que essa definição aborda todos os requisitos da norma **ISO/IEC 27001** e sua estruturação no **ciclo PDCA**.

As ações de auditoria devem ser um processo minucioso de exame das atividades desenvolvidas no escopo do SGSI, com o propósito de atestar que essas atividades estão conforme o estabelecido e o planejado, o que reflete na adequada operacionalização e na identificação de desvios, bem como no levantamento das oportunidades de melhorias no SGSI.

Auditoria interna

É um dos requisitos da **"Seção 9. Avaliação do Desempenho"** da ISO/IEC 27001, o qual preconiza que a organização deve realizar auditorias internas em intervalos planejados, objetivando levantar informações sobre o SGSI no que diz respeito à conformidade com os requisitos organizacionais, assim como os requisitos da própria norma.

No âmbito do SGSI, as principais diretrizes de auditoria interna que devem ser seguidas pela organização são:

- Considerar todos os processos no escopo do sistema e resultados de auditorias anteriores.
- Estabelecer critérios adequados.
- Selecionar auditores e conduzir auditorias objetivas e imparciais durante todo o processo.
- Garantir que os resultados da auditoria cheguem à alta gestão ou diretoria.
- Documentar os resultados de forma a produzir evidências.

Auditoria externa

Vimos que a norma ISO/IEC 27001 é passível de certificação acreditada. Essa certificação traz diversos benefícios para a organização, por exemplo:

- Vantagem competitiva
- Redução de custos
- Organização empresarial
- Conformidades legais

Portanto, convém que as organizações busquem a certificação, o que é obtido por meio de **auditoria do SGSI** realizada por **órgãos de certificação externos**.

Processo de auditoria

A norma ABNT NBR ISO 19011 – Diretrizes para Auditorias de Sistema de Gestão elenca cinco princípios que um processo de auditoria deve obedecer. Vejamos!

Condução ética

Tem como foco o profissionalismo, evidenciado pela diligência e imparcialidade, bem como a discrição, a correta observância dos princípios de confidencialidade e o zelo pelas informações obtidas por meio da auditoria, não usando as informações em benefício próprio.

Apresentação justa

Envolve a obrigação de reportar com veracidade e exatidão as constatações, as conclusões e os relatórios da auditoria, refletindo de forma fidedigna a realidade dos fatos.

Cuidado profissional

Envolve a xecução da auditoria, considerando a importância da atividade e a confiança depositada pelas partes interessadas.

Independência

É a base da imparcialidade. A atividade deve ser livre de conflitos de interesses, e os atores envolvidos devem ser independentes e não manifestar opiniões pessoais.

Abordagem baseada em evidências

É importante destacar que as conclusões de auditoria devem ser verificáveis e reproduzíveis.

A atividade de auditoria é balizada nesses princípios, que devem ser seguidos pelo auditor e pela equipe de auditoria.

Esses princípios proporcionam eficácia e confiabilidade à atividade no suporte de políticas de gestão, apontando oportunidades de melhorias e identificando desvios, bem como fornecendo subsídios para a organização implementar a melhoria contínua em seu SGSI.

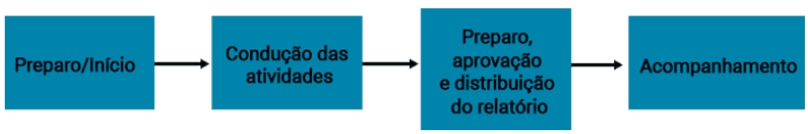
A observância desses princípios garante que os resultados e as conclusões de auditoria reflitam a realidade e sejam relevantes para a alta gestão, além de permitir que os resultados obtidos sejam semelhantes, independentemente da pessoa auditora e da equipe.

Etapas do processo de auditoria

Confira as etapas da auditoria!

Conteúdo interativo

Acesse a versão digital para ver mais detalhes da imagem abaixo.



Processo de auditoria.

Agora, vamos explorar cada uma dessas etapas.

Preparo/Início

É realizado o levantamento de toda a documentação para apoiar a atividade de auditoria e garantir o entendimento de todas as operações e processos de negócio auditado.

Lembrando que essas informações podem ser obtidas a partir de listas de verificação físicas ou digitais, coleta por amostragem ou informação audiovisual.

Atenção

É essencial que o levantamento das documentações inclua documentos e registros do SGSI, bem como relatórios de auditorias anteriores.

Para a definição da melhor estratégia, do escopo, dos critérios e dos objetivos da auditoria, devemos considerar o **contexto da organização auditada**, por exemplo:

- Tamanho
- Natureza e complexidade
- Riscos
- Oportunidades

Outras subetapas do processo de preparo incluem:

Designação do líder e equipe de auditoria
Assegura a independência da equipe em relação às atividades e evita conflitos de interesse.

Definição de objetivos, escopo e critérios da auditoria
No contexto de um SGSI (escopo), as metas (objetivos) podem ser a avaliação do SGSI quanto à conformidade com os requisitos (critérios) da ISSO/IEC 27001, avaliação da eficácia do SGSI em relação aos objetivos definidos e apontamentos de oportunidades de melhorias.

Definição de viabilidade
É o levantamento de informações para o planejamento da atividade, a cooperação adequada com o auditado e a disponibilidade adequada de tempo e de recursos (humanos, materiais e financeiros).

Condução das atividades

Nesta etapa, são realizadas as ações de coleta de informações a partir das **fontes**. Essas informações são, então, registradas como **evidências**. As evidências são analisadas de acordo com os critérios estabelecidos, transformando-se em **constatações**, que, por sua vez, tornam-se **conclusões** após a análise adequada.

Confira a seguir outras subetapas que fazem parte da etapa de condução das atividades.

Reunião de abertura

São confirmados os detalhes do planejamento, o resumo das atividades previstas, o estabelecimento de canais de comunicação e a abertura para tirada de dúvidas pelo auditado.

Coleta e verificação de informações

Envolve as informações referentes aos objetivos, ao escopo e ao critério da auditoria, que são coletadas, armazenadas e registradas como **evidências de auditoria**. Essas evidências são, então, avaliadas sob o crivo dos requisitos da ISO/IEC 27001, gerando **constatações de auditoria**.

Obs.: constatações podem indicar tanto conformidade quanto não conformidade com os critérios da auditoria. Quando definidas nos objetivos, as constatações podem trazer informações sobre oportunidades de melhorias.

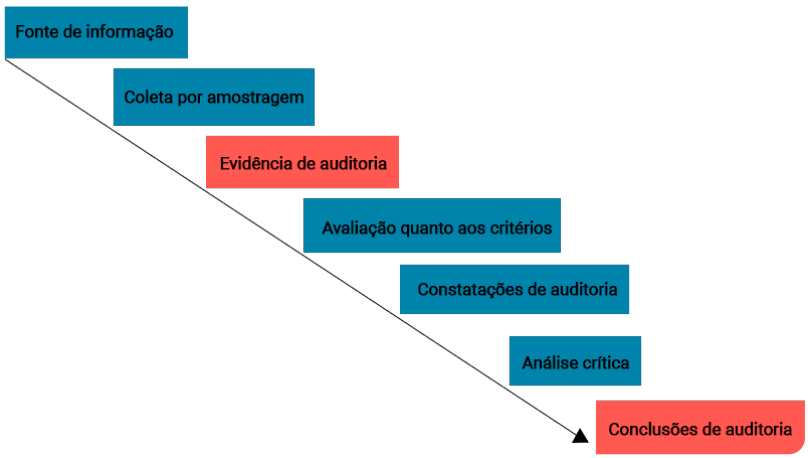
Reunião de encerramento

São apresentadas as constatações e as conclusões da auditoria para todas as partes envolvidas.

O esquema a seguir apresenta o processo sequencial que envolve a coleta e a verificação de informações. Observe!

Conteúdo interativo

Acesse a versão digital para ver mais detalhes da imagem abaixo.



Processo de coleta e verificação de informação.

Preparo, aprovação e distribuição dos relatórios

Auditorias são, em sua essência, baseadas em informações levantadas por **amostragem**. Logo, há um risco de que as evidências de auditoria não sejam representativas. Por isso, é conveniente que os relatórios possuam elevado grau de objetividade. Nessa etapa, o líder deverá relatar, a partir de subsídios da equipe de auditoria, todos os aspectos observados e levantados durante a condução das atividades.

Todo e qualquer detalhe que a liderança julgar pertinente deve ser incluído nos relatórios, como: resumo do processo, obstáculos encontrados, confirmação dos objetivos alcançados, áreas do escopo que não puderam ser cobertas e motivos relacionados, boas práticas verificadas e classificação da informação, quando couber.

Obs.: para garantir que os relatórios de auditoria sejam objetivos, completos e úteis para a tomada de decisões, é importante seguir etapas bem definidas após a conclusão dos trabalhos de campo.

Acompanhe a seguir os principais cuidados que devem ser observados nas fases de preparo, aprovação e distribuição dos relatórios, assegurando clareza, precisão e alinhamento com os procedimentos estabelecidos pela auditoria.

Preparo

O relatório deve fornecer um registro completo, preciso, sucinto e claro da auditoria, descrevendo o objetivo, o escopo, o cliente, a composição da equipe, o local e a data, os critérios, as constatações e as conclusões.

Aprovação

O relatório da auditoria deverá ser datado, analisado criticamente e aprovado de acordo com os procedimentos definidos para a auditoria.

Distribuição

O relatório deve ser distribuído às partes interessadas definidas pelo cliente da auditoria, ou seja, o proprietário do relatório.

Acompanhamento

Quando definido nos objetivos da auditoria, o resultado obtido pode indicar correções ou oportunidades de melhorias nos aspectos evidenciados. Essas ações posteriores ficam a cargo do auditado e podem demandar, quando estabelecido nos objetivos, uma nova auditoria de validação.

Requisitos auditados em um SGSI

De acordo com a **ABNT NBR ISO/IEC 27007:2013**, os seguintes tópicos podem ser usados como uma referência com base na qual a conformidade ou não conformidade é determinada:

- Política, objetivos e procedimentos de segurança da informação adotados.
- Requisitos legais e contratuais e outros requisitos relevantes (conformidade).
- Critérios, processo de avaliação e tratamento dos riscos de segurança da informação.
- Definição de controles para tratar os riscos de forma adequada.
- Métodos e critérios usados para o monitoramento, a medição, a análise e a avaliação do desempenho da segurança da informação e da eficácia do SGSI.
- Requisitos de segurança da informação fornecidos e aplicados por um cliente, fornecedor ou terceirizado.

Todos esses requisitos podem ser suportados por controles e seus respectivos objetivos, os quais estão descritos no **Anexo A da ABNT NBR ISO/IEC 27001:2022**. Esses controles são derivados e alinhados com os listados na **ABNT NBR ISO/IEC 27002:2022**.

Atividade 1

Em uma auditoria de sistemas de gestão, como a realizada em um SGSI com base na norma ISO/IEC 27001, é muito importante seguir um processo estruturado que garanta a confiabilidade dos resultados. Quais das etapas a seguir fazem parte do processo de auditoria?

I. Preparo/Início

II. Continuidade

III. Condução das atividades

IV. Acompanhamento

A I, II e IV.

B I, III e IV.

C I e IV.

D I somente.

E II e III.

A alternativa B está correta.

Segundo a ABNT NBR ISO 19011, as etapas de um processo de auditoria são: preparo/início; condução das atividades; preparo, aprovação e distribuição do relatório; acompanhamento.

Técnicas de auditoria de segurança

A segurança da informação é fundamental para proteger os ativos digitais da organização e atender às normas internacionais, como a ABNT NBR ISO/IEC 27001:2022. Nesse cenário, a auditoria de segurança se torna uma ferramenta estratégica para verificar se os controles estão funcionando bem, identificar falhas, garantir o cumprimento de regras internas e externas, e promover melhorias no sistema de gestão da segurança da informação (SGSI).

Vamos analisar agora as principais técnicas usadas na auditoria para coletar evidências, e compreender como os controles de segurança são classificados em gerenciais, operacionais e técnicos, destacando suas características e formas de avaliação.

Neste vídeo, vamos explorar as principais técnicas de auditoria utilizadas na coleta de evidências. Além disso, veremos a classificação dos controles, com ênfase em suas particularidades e formas de avaliação.

> Conteúdo interativo
>
> Acesse a versão digital para assistir ao vídeo.

A **ABNT NBR ISO/IEC 27001:2022** constitui-se de diversos requisitos suportados por controles de segurança descritos no Anexo A da mesma norma e na **ABNT NBR ISO/IEC 27002:2022**, que apresenta os códigos de prática para a aplicação desses controles. Essencialmente, os objetivos desses controles e requisitos visam garantir a preservação da **confidencialidade**, **integridade** e **disponibilidade** da informação por meio da aplicação de um processo adequado de gestão de riscos.

Nesse sentido, a auditoria de segurança também avalia os aspectos técnicos de como as políticas, as normas e os procedimentos estão sendo operacionalizados por meios desses controles.

Para alcançar esse objetivo, durante o processo de auditoria, auditores realizam coletas de evidências por meio de:

- Entrevistas pessoais
- Varredura de vulnerabilidades
- Análise de configurações dos sistemas
- Análises de rede de dados
- Análise de dados históricos
- Requisitos criptográficos
- Conformidade de hosts (servidores)
- Outros aspectos técnicos

Avaliações de segurança

De forma geral, as coletas de evidências de auditoria, no que se refere aos aspectos humanos, processuais e ambientais, são obtidas por meio de entrevistas e outras ferramentas administrativas.

Os ativos de tecnologia que suportam o SGSI são avaliados quanto a sua conformidade por meio de ferramentas e técnicas específicas. Essas avaliações ajudam a determinar se esses ativos estão atendendo aos requisitos de conformidade definidos na política de segurança.

Atenção

As avaliações de segurança tipicamente são realizadas por meio de ferramentas automatizadas, que examinam os sistemas, os aplicativos e os dispositivos de uma organização para determinar seu estado de operação atual e a eficácia de todos os controles de segurança.

Os resultados típicos de uma avaliação de segurança identificarão:

- Erros comuns de configuração.
- Ausência de controles de segurança
- Outras falhas relacionadas

Embora tipicamente não seja uma avaliação invasiva, ainda pode ter algum impacto nas operações do negócio e, dessa forma, requerer a autorização da alta gestão para sua utilização.

Na sequência, vamos conhecer os dois tipos de controle de segurança.

Controles de segurança gerenciais

Envolvem um sistema de informação que foca a gestão do risco e a operacionalização segura SGSI. São controles essencialmente administrativos e podem ser políticas, normas e procedimentos. No contexto de uma auditoria, as evidências são coletadas por meio de **entrevistas**, **revisão** e **análise documental**.

Controles de segurança operacionais

Buscam garantir que os requisitos de legislação, regulamentações, códigos e normas do setor e normas organizacionais sejam atendidos.

Alguns exemplos desses requisitos regulatórios envolvem:

PCI-DSS

É a regulamentação do setor que define como as empresas podem processar informações de pagamento por cartão de crédito, bem como reforçar as práticas de segurança que precisam cumprir para proteger esses dados de pagamento.

HIPAA

É o conjunto de normas derivadas de uma lei federal dos Estados Unidos que protege o armazenamento, a leitura, a modificação e a transmissão de dados pessoais de saúde.

LGPD e GDPR

São o conjunto de normativos legais nacional e europeu, respectivamente, que regulam o uso e o tratamento de dados pessoais.

O impacto das leis e regulamentações na aplicação de controles de segurança pode ser significativo.

Portanto, as organizações devem revisar de forma cuidadosa todas as leis e regulamentações pertinentes ao seu setor de atuação e ao escopo das operações que precisam ser protegidas. Muitas dessas normas impõem exigências legais específicas sobre sistemas de dados, processos, controles e infraestrutura.

Essas regulamentações influenciam como os dados são armazenados, transmitidos e processados. Em auditorias, a verificação da conformidade ocorre por meio da coleta de evidências, que incluem entrevistas, revisões e análises documentais, bem como a avaliação do alinhamento com os requisitos legais aplicáveis.

Controles de segurança técnicos

O foco desses controles é proteger os hosts e os sistemas operacionais/plataformas que eles executam, ativos de rede e componentes criptográficos. Em outras palavras, seu enfoque é salvaguardar e tratar riscos relacionados aos ativos de tecnologia da organização.

No contexto de auditoria, as evidências podem ser obtidas por meio de **ferramentas específicas e documentadas em relatórios técnicos**.

Confira as principais técnicas de coleta de evidências de auditoria desses controles!

Relatório de baseline

Conjunto de configurações de segurança que devem ser aplicadas a um sistema ou à rede em particular na organização, determinando se a configuração atual combina com a configuração ideal *(baseline)*.

Revisões de código

Devem ser realizadas manualmente por um integrante especialista da equipe de auditoria ou automaticamente, usando uma ferramenta de análise de código-fonte. Os dois métodos são úteis na identificação de desvios.

Varredura de vulnerabilidades

Identifica e avalia vulnerabilidades conhecidas em sistemas, redes e aplicações.

Varredura de porta lógica

Avalia o estado atual de todas as portas na rede da organização. Com isso, é possível detectar potenciais portas abertas e serviços ativos sem uma finalidade de negócio.

Testes de invasão
Empregam diversas ferramentas ativas e utilitários de segurança para avaliar a segurança e simular um ataque real.

Atividade 2

Em uma auditoria de segurança da informação, o auditor utiliza ferramentas automatizadas para escanear sistemas e identificar erros de configuração, ausência de controles e outras falhas técnicas. Esse tipo de procedimento é caracterizado como

A entrevista operacional.

B análise documental.

C avaliação de segurança.

D controle gerencial.

E conformidade legal.

A alternativa C está correta.

Avaliações de segurança são procedimentos técnicos realizados, geralmente, com o auxílio de ferramentas automatizadas que analisam sistemas, aplicativos e dispositivos para identificar vulnerabilidades, erros de configuração e falhas de segurança. Esse tipo de abordagem foca a eficácia dos controles técnicos. As demais alternativas referem-se a atividades administrativas e não técnicas.

Considerações finais

O que você aprendeu neste conteúdo?

- O que é a ISO.
- A relação entre normas ISO/IEC e a segurança da informação.
- O que determina a ISO/IEC 27001:2022.
- O que determina a ISO/IEC 27002:2022.

Explore +

Para saber mais sobre os assuntos tratados neste conteúdo, procure na internet:

- **Estudos de Caso ISO 27001 - Segurança da Informação, Intel**.
- **ISO/IEC 27001 Information security management, ISO**.
- **ISO 27001 Information Security Management (ISMS), ISO**.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. **ABNT NBR ISO/IEC 27001:2022** - Versão Corrigida: 2023 – Tecnologias da informação e Transformação Digital — Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação – Requisitos. Publicado em: 23 nov. 2022. Consultado na internet em: 25 de março de 2025.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT. **ABNT NBR ISO/IEC 27002:2022** – Tecnologia da informação — Segurança da informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação. Publicado em: 5 dez. 2022. Consultado na internet em: 25 de março de 2025.

DEUTSCHE BANK. **WetFeet Insider Guide Deutsche Bank**. Consultado na internet em: 5 maio 2022.

INTERNATIONAL ORGANIZATION FOR STANDARDIATION. ISO. **ISO/IEC 27000:2018**. Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO, 2018. Publicado em: fev. 2018. Consultado na internet em: 5 maio 2022.

KUROSE, J. F.; ROSS, K. W. **Redes de computadores e a Internet** - Uma abordagem top-down. 5. ed. São Paulo: Pearson/Addison-Wesley, 2010.

LAUREANO, M. A. P. **Segurança da Informação**. Curitiba: Lt, 2012.

MACHADO, F. N. R. **Segurança da Informação** - Princípios e Controle de Ameaças - Série Eixos. São Paulo: Érica, 2014.

NAKAMURA, E. T.; GEUS, P. L. **Segurança de Redes em Ambientes Cooperativos**. Rio de Janeiro: Novatec, 2007.

SÊMULA, M. **Gestão da Segurança da Informação**: Uma Visão Executiva. São Paulo: ST, 2013.

STALLINGS, W. **Criptografia e segurança de redes** – Princípios e práticas. 4. ed. São Paulo: Pearson/Addison-Wesley, 2007.

ZMOGINSKI, F. **AT&T processa falsos clientes por roubo de dados**. Publicado em: 9 out. 2008. Consultado na internet em: 5 maio 2022.