ISO/IEC 27001:2022 – SISTEMA DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO – CONTEXTO DA ORGANIZAÇÃO

INTRODUÇÃO

O documento da norma 27001:2022 estabelece requisitos para criar, implementar, manter e melhorar um sistema de gestão de segurança da informação. Sua adoção é uma decisão estratégica para as organizações, e que deve se adaptar ao seu contexto específico, preservando a confidencialidade, integridade e disponibilidade das informações. Esse sistema deve ser integrado aos processos organizacionais e à administração global, considerando a segurança da informação no design de processos e sistemas.

O documento serve como uma ferramenta de avaliação da capacidade da organização em cumprir seus próprios requisitos de segurança e não apresenta uma ordem específica de implementação dos requisitos. Referencia-se à família de normas ISO/IEC 27000, que inclui definições e termos relacionados à gestão da segurança da informação.

A Norma ISO 27001 de 2022 estabelece requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). Esta norma desempenha um papel fundamental na garantia de que uma organização possa criar, implementar, manter e melhorar um sistema que proteja a segurança de suas informações.

Um aspecto importante a se destacar é que a adoção desta norma é uma decisão estratégica para uma organização. Ela deve ser adaptada ao contexto específico da organização, levando em consideração a confidencialidade, integridade e disponibilidade das informações. Além disso, o SGSI deve ser integrado aos processos organizacionais e à administração global da organização, assegurando que a segurança da informação seja considerada em todos os projetos e processos.

A implementação da ISO 27001 não segue uma ordem específica de requisitos, ou seja, as organizações têm flexibilidade para implementar os requisitos na ordem que faz mais sentido para elas. Essa norma é uma demonstração da capacidade da organização em cumprir seus próprios requisitos de segurança e, consequentemente, proporciona credibilidade aos clientes, pacientes, colaboradores e usuários da organização.

Em resumo, a ISO 27001 é uma norma que define requisitos para a criação e implementação de um SGSI, sendo uma decisão estratégica para a organização. Ela proporciona confiabilidade e credibilidade, contribuindo para a segurança das informações e a integração da segurança da informação em todos os processos organizacionais. Vale destacar que a ordem de implementação dos requisitos pode variar de acordo com a organização, proporcionando flexibilidade na implementação.

ESCOPO

O documento especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

Ele também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização. Os requisitos estabelecidos neste documento são genéricos e destinam-se a ser aplicáveis a todas as organizações, independentemente do tipo, tamanho ou natureza.

5m

A exclusão de quaisquer dos requisitos especificados nas Seções 4 a 10 não é aceitável quando a organização busca a conformidade com este documento.

A norma ISO 27001 estabelece requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). A melhoria contínua é um componente essencial desse sistema, garantindo que o SGSI esteja sempre atualizado e adequado à realidade da organização, bem como em conformidade com as leis, regulamentos e contratos da organização.

É importante observar que, na norma 27001, os requisitos são considerados obrigatórios, ao contrário das boas práticas e diretrizes que são recomendadas (como na norma 27002). Requisitos são elementos que devem ser cumpridos, enquanto as recomendações são opções que a organização pode escolher seguir.

Além disso, a norma 27001 inclui requisitos para a avaliação e tratamento de riscos de segurança da informação, que devem ser realizados de acordo com as necessidades da organização. Esses requisitos são genéricos e aplicáveis a todas as organizações, independentemente do seu tamanho ou natureza. A norma enfatiza que a exclusão de qualquer um dos requisitos especificados nas seções de 4 a 10 não é aceitável quando uma organização busca conformidade com o documento, ou seja, todos os requisitos devem ser atendidos para estar em conformidade com a ISO 27001.

1. Contexto da Organização

O documento da Norma 27001:2022 foi elaborado para prover requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão de segurança da informação.

Ele especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização.

Agora vamos entender o contexto da organização.

1.1 Entendendo a organização e seu contexto

A organização deve determinar as questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade de alcançar os resultados pretendidos do seu sistema de gestão da segurança da informação.

1.2. Entendendo as necessidades e as expectativas das partes interessadas

A organização deve determinar:

a. as partes interessadas que são relevantes para o sistema de gestão da segurança da informação;

b. os requisitos relevantes dessas partes interessadas;

c. quais desses requisitos serão endereçados pelo sistema de gestão da segurança da informação.

1.3. Determinando o escopo do sistema de gestão da segurança da informação

A organização deve determinar os limites e a aplicabilidade do sistema de gestão da segurança da informação para estabelecer o seu escopo. Ao determinar este escopo, a organização deve considerar:

a. as questões internas e externas referenciadas em 4.1;

b. os requisitos referenciados em 4.2;

c. as interfaces e dependências entre as atividades desempenhadas pela organização e aquelas que são desempenhadas por outras organizações.

1.4 Sistema de gestão da segurança da informação

A organização deve estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação, incluindo os processos necessários e suas interações, de acordo com os requisitos deste documento.

A norma ISO 27001, elaborada em 2002, tem como principal objetivo fornecer requisitos para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI). Ela enfatiza a importância de atender a esses requisitos para garantir a segurança das informações dentro do contexto da organização.

Para alcançar esse objetivo, a norma destaca que a organização deve realizar uma análise abrangente de questões internas e externas que sejam relevantes para a consecução de seus objetivos e que possam afetar sua capacidade de alcançar os resultados desejados com o SGSI. Isso inclui a identificação das partes interessadas e dos requisitos relevantes dessas partes interessadas. A organização também deve determinar quais desses requisitos serão abordados pelo SGSI.

Além disso, a norma exige que a organização defina limites e aplicabilidades para o SGSI. Isso significa estabelecer até onde o SGSI se aplica e quais são as interfaces e interações entre as atividades desempenhadas pela organização e as atividades realizadas por outras organizações. A organização deve considerar, por exemplo, as fontes de energia elétrica necessárias para suas operações e garantir que essas dependências sejam abordadas no SGSI.

10m

Em resumo, a ISO 27001 destaca a importância de entender o contexto da organização, identificar as partes interessadas, determinar requisitos relevantes e estabelecer limites e aplicabilidades para o SGSI. Essas diretrizes visam garantir que o SGSI seja eficaz na proteção das informações e na melhoria contínua da segurança da informação na organização.

EXERCÍCIOS DE FIXAÇÃO

1. Qual dos seguintes pontos NÃO é mencionado como parte das considerações ao determinar o escopo do sistema de gestão da segurança da informação de acordo com a Norma 27001:2022? A) As questões internas e externas relevantes.

B. Os requisitos das partes interessadas.

C. As interfaces e dependências entre as atividades desempenhadas pela organização e aquelas que são desempenhadas por outras organizações.

D. O tamanho da organização.

E. Nenhuma das anteriores.

A norma ISO 27001:2022 estabelece considerações importantes ao determinar o escopo de um Sistema de Gestão de Segurança da Informação (SGSI). Entre essas considerações, a norma menciona:

Questões internas e externas relevantes: Isso envolve entender o ambiente em que a organização opera, incluindo fatores internos e externos que possam afetar a segurança da informação.

Requisitos das partes interessadas: As necessidades e expectativas das partes interessadas, como clientes, acionistas, funcionários e reguladores, devem ser identificadas e consideradas.
Interfaces e dependências entre as atividades desempenhadas pela organização e aquelas realizadas por outras organizações: É fundamental entender como as atividades internas se relacionam com as atividades externas, como fornecedores e parceiros.
No entanto, o tamanho da organização não é mencionado como parte das considerações ao determinar o escopo.

15m

---

2. A norma 27001:2022 estabelece requisitos para:

A. Criar, implementar, manter e melhorar um sistema de gestão da segurança da informação.
B. Criar um plano de negócios estratégico.
C. Implementar um sistema de gestão de qualidade.
D. Desenvolver um novo produto.
E. Estabelecer um sistema de gestão de recursos humanos.

A norma ISO 27001:2022 estabelece requisitos para a criação, implementação, manutenção e melhoria contínua de um Sistema de Gestão de Segurança da Informação (SGSI). Esses requisitos visam garantir que a organização possa eficazmente proteger a segurança da informação e atender às necessidades de segurança, tanto internas quanto externas.
A norma não trata de questões como a criação de um plano de negócios estratégico, a implementação de um sistema de gestão de qualidade, o desenvolvimento de um novo produto ou o estabelecimento de um sistema de gestão de recursos humanos. Ela se concentra exclusivamente na segurança da informação e nos procedimentos necessários para garantir sua integridade, confidencialidade e disponibilidade.
Portanto, é fundamental entender que essa norma não aborda questões de negócios, qualidade, produtos ou recursos humanos, mas sim a segurança da informação. Essa é a sua área de foco.

---

3. Segundo a Norma 27001:2022, para determinar o contexto da organização é necessário:

A. Estabelecer o escopo do sistema de gestão da segurança da informação.
B. Determinar as partes interessadas que são relevantes para o sistema de gestão da segurança da informação.
C. Identificar as questões internas e externas que são relevantes para o propósito da organização.
D. Todas as opções anteriores.
E. Nenhuma das opções anteriores.

Para determinar o contexto da organização de acordo com a Norma 27001:2022, é essencial realizar várias etapas. Primeiro, é necessário estabelecer os limites do Sistema de Gestão de Segurança da Informação (SGSI). Em seguida, identificar as partes interessadas relevantes para o SGSI, considerando suas necessidades e expectativas. Além disso, é fundamental identificar as questões internas e externas que possam afetar o propósito da organização.

20m

4. Exclusões de quaisquer dos requisitos especificados nas Seções 4 a 10 da Norma 27001:2022 são:

A. Aceitáveis, desde que justificadas pela organização.
B. Aceitáveis, se a organização for de pequeno porte.
C. Aceitáveis, se não se aplicarem à natureza da organização.
D. Inaceitáveis quando a organização busca conformidade com o documento.
E. Aceitáveis, se a organização não tiver uma estratégia de segurança da informação.

A questão refere-se à exclusão de requisitos especificados nas seções 4 a 10 da Norma 27001:2022. É importante lembrar que a 27001 é uma norma que define requisitos obrigatórios para um Sistema de Gestão de Segurança da Informação (SGSI). Esses requisitos devem ser cumpridos pela organização que busca conformidade com a norma.

20m

Portanto, a exclusão de quaisquer requisitos especificados nessas seções é inaceitável quando a organização busca estar em conformidade com o documento. Isso significa que a organização deve seguir todos os requisitos da norma sem exclusões se desejar ser certificada de acordo com a 27001.

Excluir requisitos tornaria impossível para a organização alegar conformidade com a norma.

GABARITO

1. d
2. a
3. d
4. d