ISO/IEC 27001:2013 – SISTEMAS DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Gestão da Segurança da Informação

Nesta aula, vamos apresentar a família de normas mais comumente cobradas da família 27000, normas que versam sobre segurança da informação.

Siglas

Siglas utilizadas em normativos e padrões:

ISO: é um padrão internacional de organização – International Organization for Standardization – que padroniza vários assuntos no que diz respeito, inclusive, a sistemas de gestão da segurança da informação.

IEC: é a comissão internacional eletrotécnica – International Electrotechnical Commission – que também tem como finalidade a padronização e criação de padrões técnicos para a área de equipamentos elétricos e eletrônicos.

ABNT: Associação Brasileira de Normas Técnicas.

NBR: Norma Brasileira.

Por vezes, uma norma ISO não está ainda no padrão brasileiro, ou seja, não se tornou uma norma brasileira, uma NBR, por isso, ela ainda não é uma norma vigente. Acontece, por exemplo, quando sai uma nova versão de alguma norma e, dentro do Brasil, não foi normatizada, reconhecida como uma norma brasileira.

SI: Segurança da Informação.

SGSI: Sistema de Gerenciamento de Segurança da Informação.

DIRETO DO CONCURSO

1. (2021/FGV/IMBEL/ANALISTA ESPECIALIZADO ANALISTA DE SISTEMAS REAPLICAÇÃO) A Associação Brasileira de Normas Técnicas, ABNT, é responsável pela elaboração das Normas Brasileiras como, por exemplo, a ABNT NBR ISO/IEC 27001 2013 sobre aspectos da Segurança da Informação

   Dado que a sigla ISO deriva de International Organization for Standardization assinale a correta natureza das normas NBR ISO.

ANOTAÇÕES

a. São normas brasileiras que passam a ser adotadas pela ISO.
b. São normas definidas em conjunto com a ISO.
c. São traduções de normas da ISO que passam a ser adotadas pela ABNT.
d. São normas da ISO adaptadas pela ABNT às práticas brasileiras.
e. São normas brasileiras compiladas a partir da combinação de outras normas da ISO.

5m

COMENTÁRIO

NBR ISO são traduções da norma da ISO, que passam a ser adotadas pela ABNT.

Bibliografia – Família 27000

- ABNT NBR ISO/IEC 27000

Objetiva dar uma visão geral e o vocabulário, termos e conceitos relacionados ao Sistema e Gerenciamento da Segurança de Informação – SGSI – e, também, é uma referência às normas da família 27000. Os termos e conceitos são utilizados nas outras normas da família 27000.

- ABNT NBR ISO/IEC 27001

Norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um SGSI.

Determina o que deve ser feito para se estabelecer um SGSI.

Caso a organização queira demonstrar que ela está em conformidade, em compliance, com a 27001, ela precisa utilizar todos os controles existentes, não podendo excluir nenhum. Dessa forma, estará em conformidade com a 27001, comprovando e conseguindo, assim, obter a certificação.

- ABNT NBR ISO/IEC 27002

Concede as práticas para a gestão de SI, ou seja, na 27002 estão as recomendações em relação às boas práticas, às diretrizes para o Sistema de Gestão de Segurança da Informação.

A diferença entre as duas é que a 27001 dá requisitos, aquilo que deve ser feito; a 27002 traz as boas práticas, as recomendações.

ANOTAÇÕES

- ABNT NBR ISO/IEC 27003

Atribui as diretrizes para a implantação de um SGSI.

A norma descreve o processo de especificação e projeto do SGSI e de design, desde a concepção até a elaboração dos planos de implantação.

Ela descreve o processo para obter a aprovação da direção da organização para implementar o SGSI.

- ABNT NBR ISO/IEC 27004

É a norma que orienta sobre monitoramento, medição, análise e avaliação.

- ABNT NBR ISO/IEC 27005

10m

É a norma que define as diretrizes sobre gestão de riscos de segurança da informação (Diretrizes). Não é uma norma de gestão de riscos corporativa.

- ABNT NBR ISO/IEC 27006

Norma que especifica os requisitos para as empresas de auditoria e de certificação de SGSI.

- ABNT NBR ISO/IEC 27007

Norma que fornece as diretrizes para auditoria de SGSI.

Norma ISO 27001:2013

O que é?

- É a norma que provê REQUISITOS para estabelecer, implementar, manter e melhorar continuamente um SGSI. Os requisitos devem ser cumpridos pela organização.
- A adoção de SGSI é uma decisão estratégica para a organização. Não é uma decisão tática gerencial nem operacional. Está no topo da pirâmide organizacional.

ANOTAÇÕES

- "O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização."

Para que serve?

- Um SGSI preserva as propriedades da segurança da informação: Confidencialidade, Integridade e Disponibilidade (CID) das informações.
- Isso é feito por meio da aplicação de um processo de gestão de riscos. Faz-se a gestão de riscos, para preservar os pilares importantes para a organização.
- Visa fornecer confiança aos *stakeholders,* as partes interessadas, pois os riscos estão sendo gerenciados adequadamente.

15m

Todos aqueles que tem influência em relação à organização – cliente, sócio, funcionários, parceiros – ao saberem que tem implementado um sistema de gestão de segurança da informação, vão entender que os riscos estão sendo gerenciados adequadamente.

Pilares da segurança da informação:

- Confidencialidade;
- Integridade;
- Disponibilidade.

DIRETO DO CONCURSO

2. (2021/SELECON/EMGEPRON/ANALISTA TÉCNICO – SEGURANÇA DA INFORMAÇÃO) Entre as Normas da ISO/IEC 27000, a ISO 27001 é uma norma relacionada ao Sistema de Gerenciamento da Segurança da Informação (ISMS) no que diz respeito ao seguinte aspecto:

a. guia para auditoria do ISMS;
b. processo de certificação e registro do ISMS;
c. especificação formal associada aos requisitos do ISMS;
d. diretriz de ISMS para empresas de telecomunicações.

ANOTAÇÕES

COMENTÁRIO

A ISO 27001 é a norma da família 2700 da ISO no que diz respeito à especificação formal associada aos requisitos do ISMS (SGSI).

- A norma pode ser usada por partes internas e externas, no que diz respeito ao atendimento dos requisitos de SI.
- A norma também contempla os requisitos para realizar a avaliação e o tratamento de riscos de segurança da informação.
- Apresenta requisitos genéricos. Não são requisitos específicos.
- São aplicáveis a TODAS as organizações, independentemente do tipo, tamanho ou natureza.

DIRETO DO CONCURSO

3. (IESES/MSGÁS/ANALISTA DE TECNOLOGIA DA INFORMAÇÃO) A norma que especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização é a:

a. ABNT NBR ISO/IEC 27004:2010.
b. ABNT NBR ISO/IEC 27001:2013.
c. ABNT NBR ISO/IEC 27003:2011.
d. ABNT NBR ISO/IEC 27002:2013.

COMENTÁRIO

20m

A norma que especifica tais requisitos é a ABNT NBR ISO/IEC 27001/2013.
Por vezes, as organizações se utilizam de normativos para se estabelecer e até implementar, mas não levam as boas práticas para manter o sistema que foi implementado de acordo com a realidade da organização. Manter é fazer com que aquilo que foi realizado esteja sempre de acordo com a realidade da organização. Manter e melhorar continuamente é responsabilidade da organização.

ANOTAÇÕES

4. (CESPE/TCU/AUDITOR FEDERAL DE CONTROLE EXTERNO – TECNOLOGIA DA INFORMAÇÃO) De acordo com a NBR ISO/IEC 27001:2013, a organização deve estabelecer, implementar, manter e continuamente melhorar um sistema de gestão da segurança da informação (SGSI). A esse respeito, julgue o item subsequente.
Na especificação e na implementação do SGSI, devem-se considerar as necessidades, os objetivos e os requisitos de segurança da organização, mas elas não devem ser influenciadas por seu tamanho nem por sua estrutura.

( ) Certo
( ) Errado

COMENTÁRIO

O estabelecimento e a implementação do SGSI de uma organização são influenciados pelas suas necessidades e objetivos, requisitos de segurança, processos organizacionais usados, tamanho e estrutura da organização.

- Anexo A – preconiza os controles e objetivos de controle, alinhados com a Norma ABNT NBR ISO/IEC 27002:2013, que deverão ser aplicados na organização.

GABARITO

1. c
2. c
3. b
4. E

25m

Este material foi elaborado pela equipe pedagógica do Gran Cursos Online, de acordo com a aula preparada e ministrada pelo professor Jósis Alves.
A presente degravação tem como objetivo auxiliar no acompanhamento e na revisão do conteúdo ministrado na videoaula. Não recomendamos a substituição do estudo em vídeo pela leitura exclusiva deste material.

ANOTAÇÕES