Introdução

O objetivo deste documento é apoiar os profissionais em fase de revisão e atualização sobre o tema, bem como instrutores no Brasil na adaptação de seus materiais de curso à versão mais recente do EXIN Information Security Foundation com base na certificação ISO/IEC 27001. Trata-se de um complemento ao Change Document.

Na literatura do exame de certificação, as mudanças na ISO/IEC 27002 estão claramente descritas em dois capítulos. Por cortesia da Van Haren Publishing, podemos disponibilizar esses dois capítulos em português. Os capítulos são: Prefácio dos autores e 1.1 Principais alterações na ISO/IEC 27002:2022

Prefácio dos autores

Esta é a quarta edição deste livro que foi criado para ajudá-lo a aprender mais sobre segurança da informação e pode ajudá-lo a obter a certificação ISFS do EXIN. A diferença em relação à edição anterior (3ª) é que esta edição se baseia em uma versão totalmente revisada da norma ISO 27002, lançada em 2022.

Uma revisão da norma ISO 27002 geralmente se limita a alguns tópicos novos, à remoção de certos termos ou técnicas obsoletas e a ajustes às mudanças da época. Por exemplo, o disquete, mencionado na primeira edição, desapareceu com o tempo e, na edição de 2013, o tópico de criptografia foi adicionado como um novo capítulo.

No entanto, **a nova versão 2022 da norma ISO 27002 foi uma grande revisão da versão anterior. Ela mesclou 24 tópicos e adicionou 13 novas medidas (controles).** As maiores mudanças, no entanto, foram a **redução de 14 capítulos para 4 capítulos** nos quais as medidas foram reagrupadas. **Esses quatro capítulos agora são chamados de Temas**. Isso significa que o padrão foi completamente reescrito e reorganizado. A estrutura da descrição das medidas também foi abordada. Houve dois motivos para isso:

1. A versão de 2013 da norma ISO 27002 havia se tornado cada vez mais uma lista de verificação nos últimos anos. O objetivo de cada medida, especificado nessa versão, não era mais considerado cuidadosamente, mas sim limitado à questão de saber se a medida havia sido implementada e, em seguida, assinalada como "concluída". No entanto, há uma diferença entre implementar o antivírus mais barato e não atualizá-lo diariamente ou descobrir qual antivírus oferece a melhor proteção em sua situação específica e garantir que ele seja mantido atualizado em um ciclo de atualização diário. Podemos pensar em um exemplo semelhante para quase todas as questões desta norma.

2. As pessoas começaram a ver as coisas de forma diferente após a introdução da norma ISO 27002 na década de 1990. As pessoas agora pensam mais em termos de temas, atributos e KPIs. A versão 2022 da norma ISO 27002 responde a isso e permite que os profissionais de segurança pensem mais e melhor sobre a maneira como desejam moldar a segurança de sua empresa. No entanto, muitos terão de se acostumar com o novo formato.

Esta quarta edição adota a nova norma ISO 27002:2022 e servirá como um guia nos próximos anos para aqueles que vão se aprofundar no assunto e, certamente, para aqueles que vão se (re)certificar para a ISO 27001.

A ISO 27002 foi renomeada. O título antigo era "Tecnologia da Informação - Técnicas de Segurança - Código de Prática para Controles de Segurança da Informação". O título da **edição de 20**22 é: **"Segurança da informação, segurança cibernética e proteção da privacidade - Controles de segurança da informação". A frase "Código de Prática" foi removida do título deste documento para refletir melhor a finalidade do documento. Trata-se de um conjunto de referência de controles de segurança da informação.**

O objetivo da norma ISO 27002:2022 não foi alterado em relação às versões antigas de 2013-2020. A intenção da norma ISO/IEC 27002 ainda é a mesma: **ajudar as organizações a garantir que as medidas necessárias não sejam negligenciadas.**

Um dos objetivos da norma ISO/IEC 27002 é que as organizações ajustem seu próprio gerenciamento de segurança da informação. Como sempre, **os conceitos de Disponibilidade, Integridade e Confidencialidade são parte integrante da ISO 27002. No entanto, a eles agora se juntaram os cinco atributos da ISO 27103, que descreve uma estrutura de segurança cibernética, introduzida em 2018: Identificar, Proteger, Detectar, Responder e Recuperar.** Esse valor é precedido por um "#", o que facilita a localização de um atributo ou a filtragem desse atributo. Isso, entre outras coisas, tornou a nova versão da norma ISO/IEC 27103, introduzida em 2018, uma parte integrante da ISO/IEC 27002.

O Time de Autores
Hans Baars, Jule Hintzbergen, Kees Hintzbergen

1.1 Principais alterações na ISO/IEC 27002:2022

1.1.1 ISO/IEC 27002: 2013 Estrutura de Controle

A versão 2013 da ISO/IEC 27002 e as atualizações durante os anos até 2020 tinham quatro capítulos introdutórios e 13 capítulos, incluindo diretrizes de segurança: capítulos 5 a 18. Cada capítulo contém seções com uma "finalidade/propósito" e uma ou mais subseções, incluindo um controle e uma diretriz de implementação.

A Tabela B2 do Anexo da ISO/IEC 27002:2022 é uma tabela de comparação e fornece uma visão geral completa das alterações que ocorreram entre a versão 2013 e a versão 2022.

1.1.2 ISO/IEC 27002: 2022 Estrutura de Controle

A nova ISO/IEC 27002:2022 também contém quatro capítulos introdutórios, mas as medidas de segurança agora estão agrupadas em apenas quatro temas. Cada tema compreende um capítulo. Isso reduziu o número de capítulos de treze para quatro.

A estrutura padrão das medidas de gerenciamento foi modificado. Além do nome e dos atributos (consulte a Tabela 1.1), os quatro itens a seguir são mostrados por medida de controle:

Tabela 1.1: Aspectos de Segurança

Tipo de Controle	Propriedades de Segurança da Informação	Conceitos de segurança cibernética	Capacidades Operacionais	Domínios de Segurança
#Preventivo	#Confidencialidade #Integridade #Disponibilidade	#Identificação	#Governança	#Governança_e_Ecossistema #Resiliência

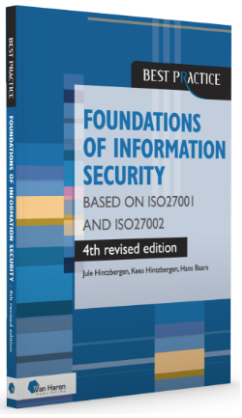
O objetivo dessa divisão é que o gestor de segurança da empresa comece a pensar nas classificações CIA (Confidencialidade, Integridade e Disponibilidade): elas continuarão sendo as principais? Ou vamos agrupar as medidas de segurança em torno dos cinco aspectos de segurança cibernética? Essa divisão tem o objetivo de evitar que a ISO 27002 se torne uma lista de verificação. O gerente de segurança agora é forçado a fazer escolhas e a comprová-las em caso de certificação. A Seção 3.5 explica esses conceitos em mais detalhes.

Como pode ser visto na Tabela 1.1, cada um dos aspectos é precedido por um #. O objetivo é permitir uma pesquisa rápida sobre tal aspecto. Se você pesquisar por "integridade", aparecerão 214 resultados. No entanto, se você pesquisar por #Integridade, restarão 177 resultados, que estão diretamente vinculados a uma medida de segurança.

- ISO/IEC 27000:2014 - fornece uma visão geral/introdução às normas ISO27000, além de um glossário para o vocabulário especializado.
- ISO/IEC 27001:2013 é o padrão de requisitos do Sistema de Gestão de Segurança da Informação (ISMS), uma especificação formal para um ISMS.
- ISO/IEC 27002:2022 Segurança da informação, segurança cibernética e proteção da privacidade - Controles de segurança da informação

Literatura do exame

Foundations of Information Security
based on ISO 27001 and ISO 27002
4th fully revised edition
Van Haren Publishing 2023
ISBN Hard copy: 978 94 018 0958 0
ISBN eBook: 978 94 018 0959 7
ISBN ePub: 978 94 018 0960 3



Nota – Inglês