FUNDAMENTOS DE SEGURANÇA DA INFORMAÇÃO

Jeanine dos Santos Barreto

Normas de segurança em TI

Objetivos de aprendizagem

Ao final deste texto, você deve apresentar os seguintes aprendizados:

- Identificar as principais normas associadas à segurança em TI.
- Reconhecer os procedimentos recomendáveis na gestão de risco em TI.
- Avaliar o planejamento para evitar riscos de incidentes em TI.

Introdução

Seguir as diretrizes estabelecidas por uma norma ISO, ou mesmo conseguir uma certificação ISO, é algo que traz destaque para uma organização, melhorando sua imagem perante seus púbicos interno e externo.

As normas ISO tratam de assuntos de diferentes áreas, estabelecendo diretrizes que devem ser adotadas pelas empresas para fazer uma gestão de riscos eficiente e, por consequência, trabalhar de forma efetiva a segurança dos seus dados e de suas informações. As normas que se iniciam pela ISO 27000 consistem em uma família de normas que visa à criação, à manutenção, à melhoria, à revisão, ao funcionamento e à análise de um Sistema de Gestão de Segurança da Informação; a ISO 27005, por exemplo, trata da gestão de riscos desse sistema. Elas oferecem a certificação de empresas e profissionais. As normas que se iniciam pela ISO 31000 também formam uma família e tratam da gestão de riscos, podendo ser aplicadas a empresas de qualquer tamanho e apresentando um guia para sua aplicação. Já a norma ISO 22301 abrange os requisitos para planejamento, estabelecimento, implementação, operação, monitoramento, revisão, manutenção e melhoria contínua do sistema de gestão de continuidade de negócios, com o objetivo de proteger a empresa e evitar riscos de incidentes disruptivos.

Neste capítulo, você vai estudar em detalhes essas normas e seu contexto de aplicação, tendo como base o Sistema de Gestão de Segurança da Informação e seus princípios básicos – confidencialidade, autenticidade, disponibilidade e integridade.

Normas de segurança: ISO 27000 e 27005

Quando o assunto é ISO 27000, deve-se ter a compreensão de que ela compõe uma família de normas ISO, que trata sobre o **Sistema de Gestão de Segurança da Informação** (SGSI). Essas normas se relacionam com a segurança de dados digitais e de sistemas de armazenamento eletrônico de dados.

Fique atento

As normas ISO foram criadas pela Organização Internacional de Padronização (ISO), visando a melhorar a qualidade de produtos e serviços. Essas normas internacionais se aplicam a várias áreas de interesse econômico e técnico. Elas fazem a certificação de produtos e serviços em várias organizações no mundo todo, oferecendo documentação com modelos padronizados para a implantação da gestão da qualidade.

No Brasil, essas normas são compostas pela sigla NBR, sendo criadas e gerenciadas pela Associação Brasileira de Normas Técnicas (ABNT).

São as empresas que escolhem seguir ou não as normas ISO, mas, uma vez que optem por segui-las, deverão estipular metas para que os requisitos das normas sejam cumpridos e a certificação seja obtida. É importante ressaltar que nem todas as normas resultam em uma certificação e que as empresas podem utilizar o modelo da norma para trabalhar seguindo as melhores práticas existentes no mercado.

Fernandes (2014) aponta que o conceito **de segurança da informação** é algo muito mais amplo do que simplesmente a garantia da integridade de dados e informações de maneira tecnológica. O SGSI trata da segurança de todos os tipos de dados e informações, trazendo como princípios básicos a confidencialidade, a autenticidade, a disponibilidade e a integridade.

Fique atento

- **Confidencialidade** é quando a informação só é divulgada para aqueles indivíduos, processos e máquinas que têm autorização para acessá-la.
- **Autenticidade** é quando se tem a certeza de que a informação está vindo do remetente informado e não sofreu alterações por outras pessoas no meio do caminho.
- **Disponibilidade** é quando a informação é disponibilizada pelo máximo de tempo possível, de maneira resistente a falhas de equipamento e a falhas de energia.
- **Integridade** é quando a informação chega ao destinatário da maneira como o remetente queria, de forma sigilosa e somente com as alterações permitidas.

Cada norma da família ISO 27000 tem uma função específica, mas todas visam à criação, à manutenção, à melhoria, à revisão, ao funcionamento e à análise de um SGSI. Essas normas podem ser adotadas pelas organizações, seja qual for o seu tamanho ou tipo, pois suas diretrizes visam a garantir que tanto os sistemas quanto as organizações estejam seguros, por meio de estratégias e orientações que fazem com que o SGSI se adapte à empresa que deseja fazer a sua implementação (INTENATIONAL ORGANIZATION FOR STANDARDIZATION, 2018).

As diretrizes traçadas pelas ISO 27000 estabelecem o que deve ser feito durante todo o processo de implementação de um SGSI e tratam também de assuntos mais específicos, como requisitos e orientações que servirão para as empresas que vão prestar serviços de certificação ou de auditoria em empresas que desejem implementar um SGSI.

A família de normas ISO 27000 oferece certificação para empresas e para profissionais. Quando uma empresa é certificada pela norma ISO 27000, ela tem o reconhecimento de uma organização de padrão internacional, sendo que somente essa ideia já traz confiabilidade e boa imagem para todas as partes interessadas, sejam clientes, fornecedores, colaboradores, parceiros, etc.

Outro grande benefício da implementação das ISO 27000 é que o processo auxilia a empresa a localizar seus pontos fracos e corrigir de maneira mais rápida e fácil as falhas no SGSI, fazendo suas revisões e atualizações com mais facilidade, o que trará também maior conscientização e envolvimento para o público interno da organização.

A família de normas ISO 27000 é grande e possui diversas normas que se relacionam com um SGSI. Vejamos algumas delas abaixo:

- ISO 27000: traz informações básicas sobre as normas da família ISO 27000 e também um glossário sobre o assunto “segurança da informação”.
- ISO 27001: traz os fundamentos para a implementação de um SGSI em uma organização.
- ISO 27002: trata sobre a certificação do profissional, estabelecendo códigos de boas práticas para profissionais.
- ISO 27003: traz diretrizes específicas para a implementação do SGSI.
- ISO 27004: traz normas sobre as métricas e os relatórios do SGSI.
- ISO 27005: traz a norma sobre a gestão de riscos do SGSI.
- ISO 27006: traz a norma sobre requisitos para a acreditação de organizações que oferecem serviços de certificação de SGSIs.
- ISO 27007: traz diretrizes para fazer a auditoria de SGSIs.

Em uma organização, as **ameaças** podem se relacionar tanto com a utilização de sistemas informatizados quanto com aspectos físicos e ambientais. As ameaças podem trazer, como consequência, impactos negativos nos negócios, perdas financeiras, paralisação de atividades essenciais, queda na imagem perante os clientes, entre outras.

Segundo Bezerra (2013), no âmbito da norma ISO 27005, que trata sobre a gestão de riscos da área de segurança da informação, um **risco** é a possibilidade de uma ameaça específica explorar vulnerabilidades existentes em um ativo ou conjunto de ativos, de maneira que possa prejudicar ou trazer impactos negativos para a organização. Já uma **medida de risco** é o resultado da combinação entre a probabilidade de um evento indesejável acontecer e a consequência que ele trará.

A **descrição dos riscos** de forma qualitativa e quantitativa permite aos gestores das organizações a priorização dos riscos, de acordo com a sua severidade ou com os critérios estabelecidos pela própria organização, com base em suas características e prioridades. A ISO 27005 estabelece diretrizes para o gerenciamento dos riscos de segurança de informação que vão auxiliar na implementação e na certificação dos sistemas de gestão.

A **gestão de riscos** é um dos aspectos do processo de segurança da informação de uma organização. Ela colabora para que o processo de segurança da informação aconteça de forma eficiente, eficaz e contínua, ao longo do tempo. A norma ISO 27005 é o desdobramento de um requisito para a segurança e traz o seguinte procedimento para a implementação da gestão de riscos e da segurança da informação, de acordo com Bezerra (2013):

- **Contextualizar os riscos**: nessa fase é preciso que se definam os detalhes para a gestão de riscos na organização e também a área que ficará responsável pelo processo de gerenciamento de riscos e segurança da informação.
- **Analisar os riscos**: essa fase envolve a identificação dos eventos que podem trazer perdas para a organização, ou seja, as ameaças. Depois disso, devem ser identificados os controles existentes, se houverem, e a eficácia de cada um desses controles ao evitar que uma ameaça explore efetivamente uma vulnerabilidade da empresa. É a partir da informação sobre as ameaças e da efetividade dos controles que é possível identificar o **nível dos riscos**. Conhecendo o seu nível de riscos, a organização pode decidir entre reduzir o risco, criando novos controles, aceitar os riscos, evitar ou até mesmo transferir a responsabilidade pelos riscos.

- **Avaliar os riscos**: essa fase envolve a priorização dos riscos por critérios estabelecidos pela própria organização. Essa avaliação deve considerar impactos ambientais, operacionais, financeiros, oportunidades de negócio, cumprimento de requisitos legais, entre outros aspectos.

Gestão de riscos: ISO 31000

As organizações, sejam elas privadas ou públicas, de todos os tipos e tamanhos, estão frequentemente expostas a todos os tipos de riscos, desde danos à sua imagem ou marca, até crimes cibernéticos ou terroristas, como afirma Fernandes (2014).

A ISO 31000 também constitui uma família, formada por normas que iniciam com essa numeração. As normas da família ISO 31000 tratam do assunto da gestão de risco. Elas não são normas que visam a certificar as organizações que as utilizarem, e podem ser implementadas em qualquer empresa, independentemente da sua área ou setor de atuação, do seu tamanho, ou da quantidade de funcionários que possui. A família ISO 31000 é formada pelas seguintes normas correspondentes e conexas:

- ISO 31000: traz informações básicas, princípios e diretrizes ou melhores práticas para a implementação da gestão de riscos.
- ISO 31010: traz técnicas de avaliação e gestão de riscos.
- ISO Guia 73: traz um vocabulário com expressões relacionadas à gestão de riscos.

Fique atento

A gestão de riscos é o processo de organização e planejamento de recursos humanos e materiais de uma organização, que visa a reduzir ao mínimo possível os impactos dos riscos, utilizando um conjunto de técnicas e ferramentas que ajudam a minimizar os efeitos dos danos e tratando os riscos que possam afetar as pessoas, os projetos, os processos, o ambiente interno da empresa e a sua imagem perante a sociedade.

A família de normas ISO 31000 serve de guia, trazendo informações e recomendações que ajudam aquelas organizações que optaram por implementá-

-la, e fornece informações básicas que auxiliam em todos os tipos de gestão de riscos, inclusive na tomada de decisão em todos os níveis organizacionais.

As normas ISO 31000 têm como principal objetivo fazer com que as organizações tenham a devida compreensão do que é a gestão de risco. Elas auxiliam a prever possíveis crises e a tornar o prejuízo o menor possível, caso uma crise se concretize, servindo como normas mais genéricas e oferecendo diretrizes para que a empresa saiba que rumo tomar e como se comportar para se prevenir de riscos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009).

Como essas normas não têm como propósito fazer a certificação das organizações, as ISO 31000 procuram fazer com que cada organização elabore a sua própria maneira de fazer a gestão de riscos, de acordo com as suas necessidades e características particulares, fazendo funcionar o processo de forma eficiente.

Fique atento

Um **risco** é um evento ou uma situação incerta que, caso ocorra, pode provocar um impacto positivo ou negativo em algum projeto, área ou processo de uma organização.

Quando os eventos podem acarretar em um impacto positivo, eles representam as **oportunidades**, algo que pode influenciar de forma favorável no atingimento de algum objetivo, preservar valor agregado, ou ainda agregar valor a algo.

Quando os eventos podem acarretar em impactos negativos, eles representam as **ameaças**, algo que pode influenciar de maneira desfavorável nos negócios da empresa, podendo trazer prejuízos de diversos tipos, inclusive financeiros e de imagem.

As **normas ISO** foram criadas, então, para indicar o caminho correto, isto é, as melhores práticas na gestão de riscos. Por conta disso, elas oferecem diretrizes e orientações que as empresas podem seguir para desenvolver a sua própria gestão de riscos. As diretrizes e melhores práticas estabelecidas pelas ISO 31000 tratam sobre (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009):

- a noção sobre os riscos e as oportunidades em uma empresa;
- a remoção das fontes de risco;
- a alteração das consequências e das probabilidades;
- a atualização constante das informações sobre os riscos.

A Figura 1 apresenta um processo de gestão de riscos.

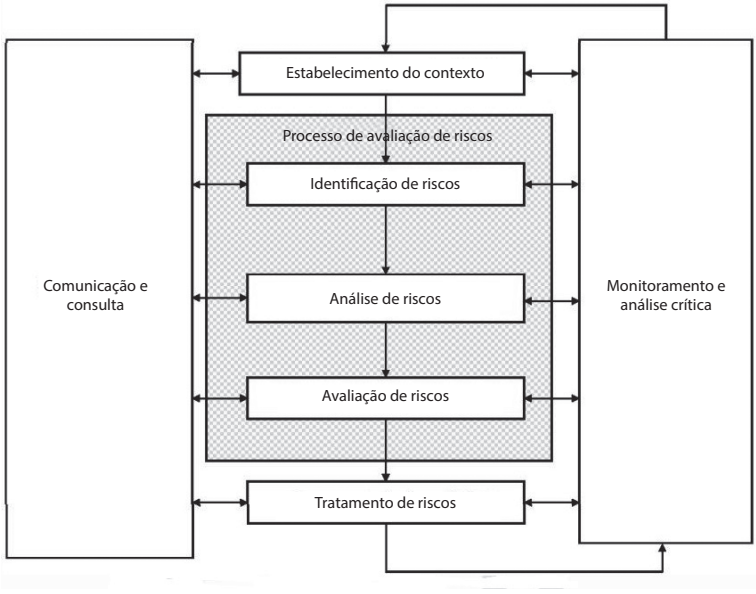

Figura 1. Processo de gestão de riscos.

Fonte: Adaptada de ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (2009, p. 14).

Para uma **gestão de riscos de sucesso**, é preciso que a organização cumpra os seguintes requisitos, de acordo com a norma ISO 31000 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009):

- **Comunicação e consulta**: consiste na consulta das partes interessadas, que deve ocorrer em todas as fases seguintes. Um bom plano de comunicação entre as partes interessadas e a organização a respeito dos riscos deve ser planejado e definido ainda nas etapas iniciais da gestão de riscos.
- **Estabelecimento do contexto**: definição dos critérios para a gestão de riscos e o escopo da gestão, isto é, as áreas e os setores envolvidos. Deve envolver questões a respeito de estrutura organizacional, responsabilidades, processos, sistemas a serem utilizados, legislação, política, finanças, tecnologia disponível, entre outras.
- **Identificação de riscos**: identificação de um conjunto de riscos, com o objetivo de gerar uma lista de riscos que possam afetar a realização dos

objetivos da organização, tanto de maneira positiva quanto negativa. É importante lembrar que um risco não identificado nessa fase não será tratado nas demais.

- **Análise de riscos**: envolve a compreensão sobre os riscos da organização, suas causas, fontes, consequências positivas e negativas, e ainda a probabilidade de ocorrerem. Essa análise pode ser feita em diversos graus de detalhamento, a critério da empresa, e ainda pode ser quantitativa ou qualitativa.
- **Avaliação de riscos**: envolve identificar quais riscos precisam ser tratados e a prioridade na implementação do seu tratamento.
- **Tratamento de riscos**: envolve a seleção de uma ou mais opções para modificar os riscos, e a implementação dessas opções. Nessa fase pode ser decidido se um risco deve ser reduzido, evitado, removido, aumentado (caso seja uma oportunidade), compartilhado com terceiros, ou, ainda, retido.
- **Monitoramento e análise crítica**: deve ser feito de forma contínua, modificando aspectos da gestão de riscos que sejam julgados necessários.

A implementação das normas ISO 31000 na organização permitirá uma gestão de riscos efetiva, que trará **vantagens** como (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2009):

- aumento na probabilidade de atingir objetivos;
- atenção para a necessidade de identificação e tratamento de riscos ao longo dos processos de toda a organização;
- melhoria na identificação de oportunidades e ameaças;
- melhoria na governança e na gestão da empresa;
- aumento da confiança das partes interessadas;
- utilização eficaz dos recursos para o tratamento dos riscos;
- aumento da aprendizagem e da resiliência organizacional;
- minimização das perdas e prejuízos causados pela efetivação dos riscos.

Fique atento

Para uma organização, as partes interessadas correspondem a todos os elementos que afetam ou são afetados pela organização, pelas suas atividades e pelas decisões tomadas por ela. Entre as partes interessadas estão os funcionários, os clientes, as empresas parceiras, os fornecedores, o governo, entre outras.

Planejamento contra incidentes: norma ISO 22301

Todas as organizações, independentemente da sua área de atuação ou do seu porte, estarão eventualmente sujeitas a sofrer interrupções nos seus processos ou passar por alguma situação adversa que possa dificultar ou impedir suas operações e sua produção.

Segundo Fernandes (2014), esse tipo de evento ou de interrupção nos serviços, apesar de se apresentar raramente, pode acontecer a qualquer momento, de maneira inesperada, e pode ser causado por diversos tipos de ameaças. Essas ameaças podem vir do **ambiente interno** da empresa, por meio de fraudes financeiras e falhas nos processos ou nos sistemas informatizados, ou ainda do **ambiente externo** da empresa, por meio de desastres naturais, incêndios, queda da economia, entre outros motivos.

Em vista disso, as empresas precisam tomar precauções e estar preparadas para que possam garantir a continuidade de seu negócio, independentemente do tipo de desafios que se apresentem a elas. Por isso, a implementação de um plano ou sistema de gestão de continuidade de negócios, e também de um plano de recuperação de incidentes, torna as empresas capazes de lidar com qualquer tipo de situação indesejada e de manter o pleno funcionamento dos serviços essenciais da organização, até que a situação se normalize por completo.

Um **plano de gestão de continuidade de negócios** eficiente contém os principais elementos necessários para a gestão de risco e para a análise de impacto para os negócios. A etapa da identificação dos riscos e dos impactos relacionados a eles é seguida pelo planejamento das políticas, dos objetivos, dos planos e das responsabilidades que proporcionarão as características de **resiliência** e **adaptação** para a organização, essenciais para a recuperação em situações adversas.

O processo de continuidade de negócios auxilia no entendimento de como a empresa trabalha e onde podem ocorrer falhas, tornando possível aprimorar os processos de negócio. A continuidade do negócio é um compromisso para todas as organizações, pois é estabelecida por requisitos legislativos, de regulamentação, setoriais, de produtos e de serviços.

O plano de gestão de continuidade de negócios deve ser idealizado e implementado de maneiras diferentes para cada empresa, sempre levando em conta as características e necessidades próprias do negócio. Por isso, é preciso que os profissionais responsáveis pela gestão da continuidade do negócio levem em consideração três elementos essenciais na definição desse plano (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013):

- analisar os riscos, identificando tudo o que pode vir a acontecer de aspecto negativo para os processos da organização, ou seja, quais são as principais ameaças ao negócio da empresa;
- analisar os impactos, identificando de que forma as ameaças poderão impactar nos negócios da organização;
- elaborar o planejamento estratégico, que vai estabelecer quais são as atitudes a serem tomadas e as ações que se farão necessárias caso uma ameaça se apresente, visando à retomada normal das operações da organização.

Normalmente, um plano de gestão de continuidade de negócios é composto por quatro planos, que são interligados e vinculados entre si:

- **Plano de contingência ou emergência**: esse é o plano que deve ser utilizado quando as ações de prevenção de incidentes tiverem falhado, e o incidente disruptivo tiver acontecido de fato. Ele é utilizado para definir as ações mais imediatas a serem tomadas.
- **Plano de administração ou gerenciamento de crises**: nesse plano são definidas as funções e as responsabilidades de cada equipe envolvida no acionamento das ações de contingência, que vão acontecer antes, durante e após a ocorrência do incidente.
- **Plano de recuperação de desastres**: é o plano que determina o planejamento que será utilizado, uma vez que o incidente esteja controlado e a crise tenha passado, para que a organização retome os seus níveis originais de operação e produção.
- **Plano de continuidade operacional**: o objetivo desse plano é o de restabelecer o funcionamento dos principais processos que suportam a operação da empresa, a fim de reduzir o tempo de paralisação e os impactos provocados pelo incidente.

A norma ISO 22301 traz a especificação dos requisitos para o planejamento, o estabelecimento, a implementação, a operação, o monitoramento, a revisão, a manutenção e a melhoria contínua do sistema de gestão de continuidade de negócios, com o objetivo de proteger a empresa, reduzindo a probabilidade de ocorrência e o tempo necessário para a resposta e a recuperação da empresa, em casos de incidentes que provoquem a paralisação temporária de processos, os chamados **incidentes disruptivos**.

Um evento disruptivo significativo, que cause a paralisação não programada em processos de negócio, pode trazer impactos negativos severos e importantes para uma organização, entre eles:

- prejuízos financeiros e fiscais;
- interrupção da produção;
- exposição da imagem da empresa, prejudicando-a perante clientes e demais partes interessadas;
- perda da confiança e da credibilidade perante os públicos interno e externo à organização.

A resposta adequada a um evento desse tipo necessita da mobilização de toda a organização, de forma estruturada, rápida, coerente e assertiva, para que possa diminuir ou evitar os impactos negativos. Por isso, a gestão da continuidade de negócios planeja, implanta e mantém atualizados e disponíveis, para todos os envolvidos, os planos e procedimentos fundamentais para uma recuperação efetiva depois de a empresa ter enfrentado o evento.

Dessa forma, a norma ISO 22301 oferece a melhor estrutura possível para a gestão da continuidade de negócios em uma organização, uma vez que uma organização pode obter a certificação por meio de uma entidade reconhecida e, assim, comprovar essa conformidade aos seus clientes e demais partes interessadas (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013).

Essa norma faz com que a organização entenda e priorize as ameaças ao seu negócio e especifique os requisitos para que o sistema de gestão proteja o negócio contra incidentes e reduza a possibilidade de eles ocorrerem, garantindo que a empresa se recupere caso eles se efetivem.

Quando a gestão da continuidade de negócios é implementada de maneira correta, ela possibilita a redução da probabilidade de incidentes que provocam a interrupção ou ameaçam o seguimento normal dos processos da organização. Caso algum evento desse tipo ocorra, a organização estará pronta para tratá-lo e respondê-lo de forma adequada, reduzindo de forma drástica os possíveis danos gerados.

Qualquer organização, independentemente de ser grande ou pequena, privada ou pública, que tenha ou não fins lucrativos, pode implementar o padrão da norma ISO 22301. Esse padrão foi idealizado de uma forma que possa ser aplicado em organizações de qualquer tipo ou tamanho.

A certificação com a norma ISO 22301 ajuda a melhorar a forma como a organização, como um todo, administra as suas eventualidades. Essa norma

garante um sistema de gerenciamento de continuidade de negócios planejado e efetivo, que permite responder de modo eficaz a qualquer perturbação que surja.

O plano de continuidade de negócios tem como objetivo principal a criação de padrões de procedimentos que devem ser adotados em situações adversas, para que a organização possa se recuperar, retomar seus processos e dar prosseguimento às atividades mais importantes para o negócio, evitando que ocorram danos mais profundos, que possam provocar prejuízos financeiros e de imagem.

O programa geral de um gerenciamento de continuidade de negócios deve envolver o planejamento de atividades como treinamentos, exercícios e revisões regulares. Mesmo que a organização nunca tenha passado por um incidente grave, implantar um gerenciamento de continuidade de negócios fundamentado na norma ISO 22301 pode ajudar a definir os processos que serão fundamentais para tratar esse tipo de evento, caso ocorra, e seus possíveis impactos na organização.

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *ABNT/CEE/ISO 22301*: segurança da sociedade: sistema de gestão de continuidade de negócios: requisitos. 2013. Disponível em: <https://pt.scribd.com/document/356801706/ISO-22301-Portugues-pdf>. Acesso em: 26 maio 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR/ISO 31000*: gestão de riscos: princípios e diretrizes. 2009. Disponível em: <https://gestravp.files.wordpress.com/2013/06/ iso31000-gestc3a3o-de-riscos.pdf>. Acesso em: 8 jun. 2018.

BEZERRA, E. K. *Gestão de riscos de TI*: NBR 27005. Rio de Janeiro: RNP/ESR, 2013.

FERNANDES. A. A. *Implantando a governança de TI*: da estratégia à gestão de processos e serviços. Rio de Janeiro: Brasport, 2014.

INTENATIONAL ORGANIZATION FOR STANDARDIZATION – ISO. *ISO/IEC 27000*: information technology: security techniques: information security management systems: overview and vocabulary. 2018. Disponível em: <https://www.sis.se/api/document/preview/ 80001198/>. Acesso em: 8 jun. 2018.

Encerra aqui o trecho do livro disponibilizado para esta Unidade de Aprendizagem. Na Biblioteca Virtual da Instituição, você encontra a obra na íntegra.

Conteúdo: