

NÃO PODE FALTAR

GESTÃO E POLÍTICAS DE SEGURANÇA

Emilio Tissato Nakamura

[Ver anotações](#)

O QUE É LGPD?

A Lei Geral de Proteção de Dados Pessoais (LGPD) é uma lei que visa proteger os direitos fundamentais de privacidade dos dados dos cidadãos brasileiros.



Fonte: Shutterstock.

Deseja ouvir este material?

Áudio disponível no material digital.

CONVITE AO ESTUDO

Caro aluno, nesta unidade serão apresentados aspectos normativos e de cultura da segurança da informação, que tratam, de uma forma integrada, de processos, pessoas e tecnologias.

Muitos casos de incidentes de segurança são resultados de exploração de vulnerabilidades nestas três frentes, o que exige que as empresas tenham que tratá-las de uma forma integrada. Em 2008, houve a exploração de falhas de

sistemas internos de um banco europeu, causando prejuízo de US\$ 7 bilhões (SPAMFIGHTER, 2008). Este exemplo reforça a importância de controles de segurança que considerem os aspectos de processos, pessoas e tecnologias. No caso do banco, o funcionário que fez a exploração tinha acesso a sistemas internos e se aproveitou da falta de segurança que poderia ser tratada com processos que envolvessem, por exemplo, limites e aprovações de instâncias superiores. Para que ele não explorasse os sistemas internos de uma forma ilícita, uma política de segurança clara também seria fundamental. E, para complementar, os sistemas internos deveriam ser protegidos com controles de segurança envolvendo monitoramento, controle de acesso e desenvolvimento seguro, por exemplo.

Ver anotações

Este caso mostra também a importância da cultura de segurança, que é particular de cada organização, construída com medidas e comportamentos de todos os funcionários, e no relacionamento com clientes, parceiros e fornecedores. É por meio da soma das ações de todos que uma cultura de segurança da informação é construída, de modo que é fundamental a representatividade e a formalização de instrumentos importantes, como um Sistema de Gestão de Segurança da Informação (SGSI). Discutiremos a cultura de segurança e a construção de um SGSI, juntamente com a política de segurança da informação, que é um dos controles primordiais das empresas, e um dos pontos iniciais para a consolidação de uma cultura de segurança da informação forte.

Há um conjunto de *frameworks* e normas que guiam as ações de segurança da informação, como as da família NBR ISO/IEC 27000 (ABNT, 2020), que você deve conhecer para organizar e otimizar sua estratégia de segurança da informação. Você terá uma abordagem da família NBR ISO/IEC 27.000 e verá que há outras fontes relevantes, como o *Cybersecurity Framework do National Institute of Standards and Technology* (NIST) (NIST, 2018) e o CIS Controls, do Center for Internet Security (CIS) (CIS, 2020).

Não podemos esquecer que, na Era da Informação, reforçada pela transformação digital, a proteção dos princípios da segurança da informação (confidencialidade, integridade e disponibilidade) deve fazer parte direta dos negócios, seja para

proteger transações, dados pessoais, documentos confidenciais, processos de negócios em que o fluxo de dados envolve diferentes áreas da empresa, ou dados que trafegam por equipamentos de fábricas.

A segurança da informação é, assim, direcionada por aspectos de negócios e cada organização com a sua missão e seus valores. E a segurança da informação é direcionada também por aspectos legais, regulatórios e contratuais, como os do setor médico, de telecomunicações ou financeiro.

o

Ver anotações

No Brasil, a Lei nº. 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD) (BRASIL, 2020), a Lei Nº 12.965, o Marco Civil da Internet (BRASIL, 2014) e a Lei Nº 12.737, a Lei Carolina Dieckmann (BRASIL, 2012) também reforçam a necessidade de segurança da informação.

A política e cultura de segurança devem tratar de todos os aspectos de sua empresa, incluindo desde a forma e as responsabilidades de funcionários que recebem equipamentos, até as necessidades de proteção nas relações com parceiros e fornecedores, passando pela forma como os acessos físicos e lógicos são gerenciados. Além disso, é importante também que a aquisição e o desenvolvimento de sistemas considerem aspectos de segurança da informação.

Você deve considerar que as empresas estão em constante evolução, assim como os riscos de segurança da informação, o que resulta em uma natural evolução da própria área de segurança da informação, que deve ser sempre acompanhada. Iremos discutir nesta unidade algumas tendências em segurança da informação que moldarão o seu futuro.

Nesta unidade também discutiremos aspectos importantes de segurança da informação envolvidos com o uso de nuvem computacional e iremos nos aprofundar um pouco mais nos dados que têm o seu ciclo de vida e precisam ser seguros, envolvendo o uso de criptografia e técnicas como anonimização e pseudonomização, importantes principalmente para a conformidade com a LGPD.

Bons estudos!

PRATICAR PARA APRENDER

Caro aluno, nesta seção será abordado um dos aspectos mais complexos da segurança da informação: como trabalhar com segurança da informação integrando aspectos relacionados a pessoas, processos e tecnologias. Uma cultura de segurança da informação forte é construída pelas pessoas, com seus hábitos do dia a dia nas empresas, e um dos principais instrumentos para esta construção é a Política de Segurança. Muitos tratam as pessoas como o elo mais fraco da segurança da informação das empresas. Você já passou por aquela situação em que os usuários questionam sobre o que é permitido ou não, e onde isto está escrito?

Porém, a Política de Segurança da Informação é apenas um dos controles de segurança necessários nas empresas. Para uma proteção plena da confidencialidade, integridade e disponibilidade das informações, é preciso tratar a segurança da informação de uma forma holística, que engloba a necessidade de um conjunto de diferentes controles de segurança. E a complexidade aumenta com a constante evolução das ameaças, dos negócios e das leis e regulamentações.

O estabelecimento de um Sistema de Gestão de Segurança da Informação (SGSI) é, assim, um ponto importante para uma atuação holística em segurança da informação.

Ver anotações

Para a sua orientação, há um conjunto de frameworks e normas que guiam as ações de segurança da informação, como as da família NBR ISO/IEC 27.000 (ABNT, 2020), o *Cybersecurity Framework do National Institute of Standards and Technology* (NIST) (NIST, 2018) e o *CIS Controls, do Center for Internet Security* (CIS) (CIS, 2020).

Você pode certificar o SGSI de sua empresa de acordo com a norma ABNT NBR ISO/IEC 27001, enquanto a ABNT NBR ISO/IEC 27002 foca nos objetivos de controles de segurança. O *Cybersecurity Framework* tem uma abordagem integrada de diferentes aspectos de segurança importantes, enquanto o CIS *Controls* estabelece uma forma mais prática de trabalho.

Nesta seção ainda discutiremos sobre a privacidade, que exige a proteção de dados pessoais, o que é regido pela Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709 (BRASIL, 2020).

Uma empresa é composta por uma matriz em Natal, no Rio Grande do Norte, e filial em Belo Horizonte, em Minas Gerais. Com foco em energias renováveis, o desenvolvimento de novas tecnologias é feito por também por uma equipe que fica em Santiago, no Chile. Há laboratórios conectados em Belo Horizonte e Santiago. A empresa tem projetos com militares argentinos, o que exige um alto nível de segurança, já que envolve aspectos de segurança nacional.

A empresa tem um diretor de segurança da informação, que é o responsável por uma estrutura que inclui uma gerência de governança de segurança, uma gerência de tecnologias de segurança e outra gerência de processos de segurança. Você é o gerente de processos de segurança e deve trabalhar em sinergia com os outros dois gerentes para alinhar os planos e atividades de segurança da informação da empresa.

O diretor de segurança da informação da empresa solicitou um status dos aspectos normativos da empresa e você deve preparar uma apresentação com esse material. É preciso fazer um alinhamento com o gerente de governança de segurança e o gerente de tecnologias de segurança.

Ver anotações

Estruture uma apresentação descrevendo os tópicos com detalhes. Os tópicos a ser abordados são listados a seguir:

- *Frameworks* de segurança disponíveis e qual a empresa segue.
- Aspectos de negócios, legais, normativos e contratuais que devem ser considerados pela empresa.
- Controles de segurança da empresa: quais são e como são definidos.
- Estrutura normativa, considerando políticas, normas, diretrizes, procedimentos, guias.

o

Ver anotações

Nesta seção, você terá acesso a instrumentos que farão a diferença em sua jornada em segurança da informação, ao integrar aspectos de pessoas, processos e tecnologias, com a possibilidade de aplicar normas e frameworks importantes como a família ISO 27000, *Cybersecurity Framework* do NIST e o CIS *Controls* do CIS.

Boa aula!

CONCEITO-CHAVE

Um dos principais instrumentos para a aplicação de segurança da informação nas empresas são as normas e *frameworks*, os quais apresentam uma visão mais abrangente das necessidades e implementações de segurança da informação, e devem ser seguidos, na medida do possível.

Um dos principais desafios da segurança da informação é o tratamento dos variados riscos, que englobam aspectos de pessoas, processos e tecnologias. Eles devem ser tratados de uma forma integrada, todas as pessoas devem conhecer os elementos de segurança da informação das empresas onde trabalham, criando assim uma cultura de segurança da informação que guie e influencie diretamente os negócios e dite o dia a dia das atividades de todos.

A Política de Segurança da Informação é um dos principais e fundamentais controles de segurança necessários nas organizações, independentemente de sua natureza. Ela faz parte de normas e frameworks de segurança da informação, como as descritas a seguir.

o

Ver anotações

| CYBERSECURITY FRAMEWORK, DO NIST

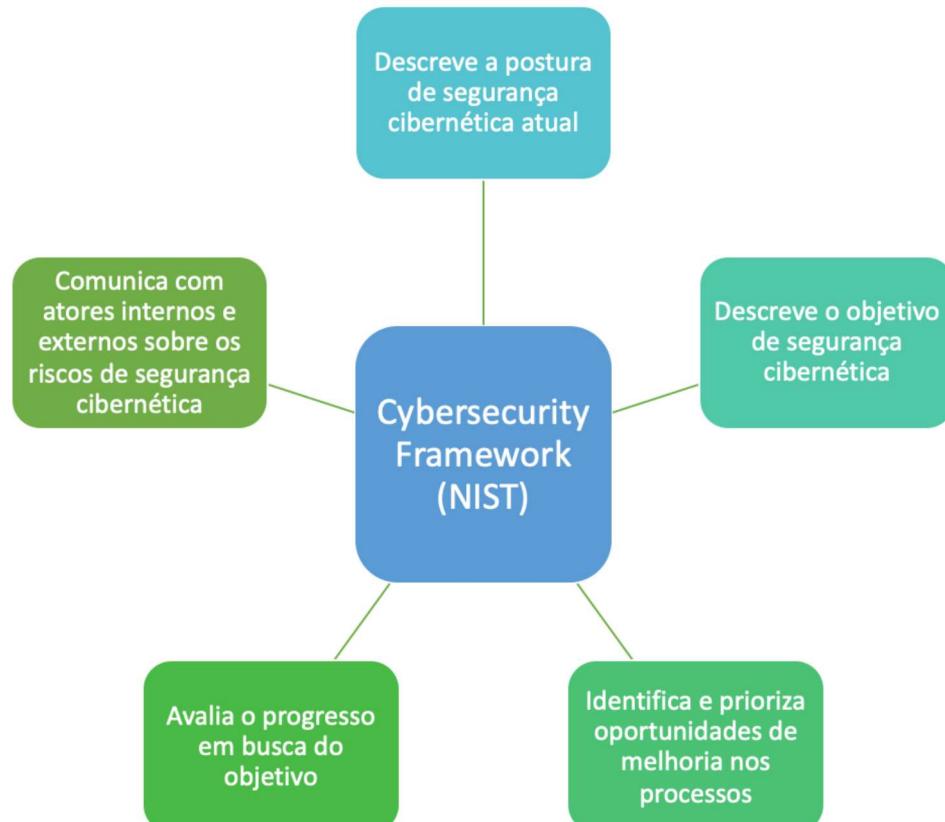
O *Cybersecurity Framework do National Institute of Standards and Technology* (NIST) (NIST, 2018) organiza diferentes elementos da segurança da informação, focando no uso de direcionadores de negócios para guiar atividades de segurança cibernética, considerando os riscos de segurança da informação. O *framework* faz a ponte entre o nível executivo com o operacional (Figura 2.1) e provê uma taxonomia e determinados mecanismos para as organizações alcançarem variados objetivos de segurança da informação (Figura 2.2). O nível executivo tem foco nos riscos organizacionais, enquanto o nível de negócios e processos faz o gerenciamento dos riscos do ambiente, com o nível de implementação e operações implementando a segurança. O *framework* trabalha com os elementos importantes para as atividades destes três níveis, incluindo objetivos, priorizações, orçamentos, métricas e comunicação.

Figura 2.1 | Integração entre visões e os riscos de segurança da informação



Fonte: adaptada de NIST (2020).

Figura 2.2 | Objetivos do *Cybersecurity Framework* do NIST

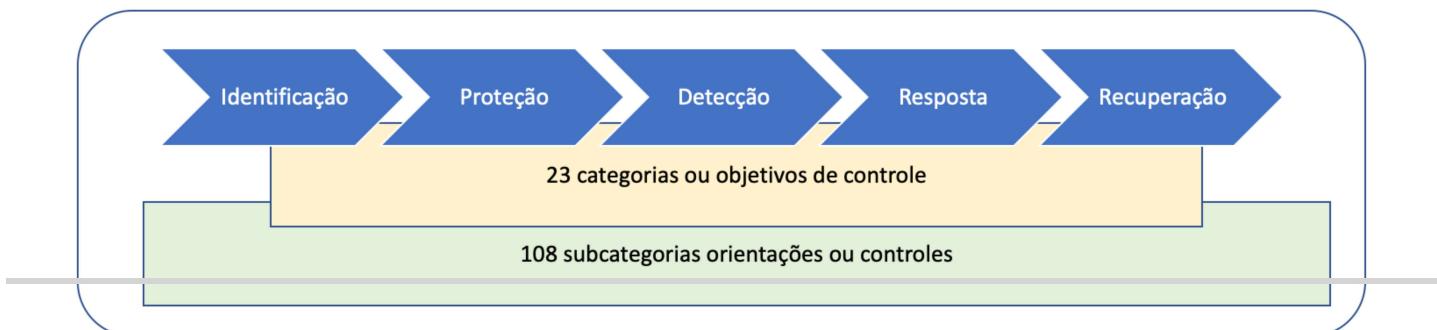


Fonte: adaptado de NIST (2018).

As três partes do *Cybersecurity Framework* são:

- **Núcleo (*Framework Core*)**, com guias detalhadas para desenvolver perfis organizacionais, que prioriza as atividades de segurança de acordo com requisitos de negócios, missão, tolerância a riscos e recursos disponíveis. Envolve as cinco funções (identificar, proteger, detectar, responder e recuperar) (Figura 2.3), que provê uma visão estratégica do ciclo de vida dos riscos de segurança da informação. As funções têm categorias (23 no total), abrangendo resultados cibernéticos, físicos, pessoais e comerciais. Há ainda 108 subcategorias, divididas nas 23 categorias, que são orientações para criar ou melhorar um programa de segurança cibernética, com referências a outros padrões de segurança da informação, como a ABNT NBR ISO/IEC 27001 (ISO 27001, 2013), COBIT (COBIT, 2020), NIST SP 800-53 (NIST, 2020), ANSI/ISA-62443 (ISA, 2020) e CIS *Controls* (CIS, 2020);
- **Camadas de implementação**, que proveem um mecanismo para ver e entender as características da abordagem para o gerenciamento de riscos da organização, para priorizar e alcançar os objetivos de segurança da informação. As camadas vão de parcial (*Tier 1*) a adaptativo (*Tier 4*), refletindo as respostas informais e reativas iniciais até a agilidade e a resposta formal baseada na visão de riscos;
- **Perfis**, que são os alinhamentos de padrões, guias e práticas em um cenário de implementação. Os perfis podem identificar as oportunidades de melhoria da postura de segurança, comparando um perfil atual ("as is") com um perfil alvo ("to be").

Figura 2.3 | As cinco funções do *Cybersecurity Framework*



Fonte: adaptado de NIST (2018).

Ver anotações

CIS CONTROLS, DO CENTER FOR INTERNET SECURITY (CIS)

O CIS *Controls* é um conjunto priorizado de ações que, de uma forma integrada, estabelecem a defesa em camadas para mitigar os ataques mais comuns contra sistemas e redes. Com objetivo de melhorar o estado de segurança, o CIS *Controls* muda a discussão de “o que minha empresa faz?” para “o que devemos todos fazer?” para melhorar a segurança e fortalecer uma cultura de segurança da informação (CIS, 2020). Ele foi desenvolvido pela comunidade de segurança da informação e tem as seguintes características:

- **O ofensivo direciona a defesa:** uso de controles para atuar sobre ataques reais;
- **Priorização:** investe primeiramente em controles que proveem a maior redução do risco e proteção contra as ameaças mais perigosas;
- **Medidas e métricas:** estabelece uma linguagem comum para executivos, especialistas de TI, auditores e profissionais de segurança para medir a eficiência das medidas de segurança, de modo a identificar e implementar rapidamente os ajustes necessários;
- **Diagnóstico e mitigação contínua:** mede continuamente a efetividade das medidas de segurança atuais para direcionar a priorização das próximas etapas;
- **Automação:** automatiza defesas para que a organização alcance confiabilidade, escalabilidade e medição contínua da aderência dos controles e métricas.

O CIS *Controls* define um conjunto de seis controles considerados básicos ou higiênicos:

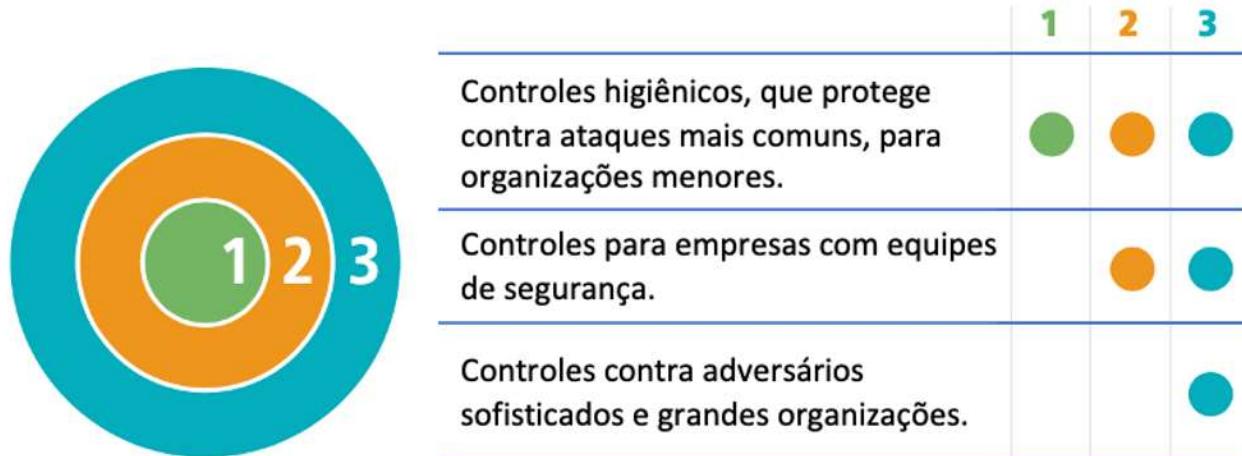
- Inventário e controle de ativos de *hardware*.
- Inventário e controle de ativos de *software*.

- Gestão de vulnerabilidades.
- Uso controlado de privilégios administrativos.
- Configuração segura para *hardware* e *software* de dispositivos móveis, laptops, *workstations* e servidores.
- Manutenção, monitoramento e análise de logs de auditoria.

Ver anotações

Porém, considerando que estes controles podem ser difíceis de serem implementados por organizações com recursos limitados, a base para as priorizações são os grupos de implementação (*CIS Controls Implementation Groups, IGs*), que são categorias de avaliação própria a partir de alguns atributos relevantes de segurança da informação. A Figura 2.4 apresenta os 3 grupos de implementação, com o IG1 focando nos dados críticos e sendo considerados os controles higiênicos, capazes de proteger contra os ataques mais comuns. O IG2 foca em organizações com equipes de segurança, enquanto o IG3 busca a proteção contra adversários sofisticados. Eles são complementares, ou seja, IG1 deve ser implementado, depois IG2 e depois o IG3.

Figura 2.4 | CIS *Controls Implementation Groups, IGs*



Fonte: adaptado de CIS(2020).

Um exemplo de classificação como IG1 são empresas familiares com 10 funcionários. Já uma organização regional provendo um serviço poderia ser classificada como IG2, e uma grande corporação com milhares de funcionários

pode ser classificado como IG3 (CIS, 2020).

O conjunto de controles de segurança do CIS *Controls* pode ser visto na Figura 2.5.

Figura 2.5 | Controles de segurança do CIS *Controls*

0

Ver anotações

Básico	Fundamental	Organizacional
Inventário e controle de ativos de hardware	Proteção de e-mail e web browser	Programa de conscientização e treinamento em segurança
Inventário e controle de ativos de software	Proteção contra malware	Segurança de aplicações
Gestão de vulnerabilidades	Controle de portas, protocolos e serviços de rede	Gestão e resposta a incidentes
Controle do uso de privilégios administrativos	Capacidade de recuperação de dados	Testes de segurança
Configuração segura para hardware e software em dispositivos móveis, laptops, workstations e servidores	Configuração segura de dispositivos de rede	
Manutenção, monitoramento e análise de logs	Defesa de borda	
	Proteção de dados	
	Controle de acesso baseado no <i>need to know</i>	
	Controle de acesso sem fio	

Monitoramento e controle de contas

Fonte: adaptado de CIS (2020).

o

Ver anotações

I FAMÍLIA ISO 27000

Quando falamos sobre segurança da informação, devemos conhecer a família de normas da ISO 27000. Estas normas abarcam ainda a certificação de segurança da informação, realizada por auditores líderes ISO 27001.

ASSIMILE

Certificação em segurança da informação pode ser concedida para uma organização que segue a norma ABNT NBR ISO/IEC 27001 (ISO 27001, 2013), que trata dos requisitos de um Sistema de Gestão de Segurança da Informação (SGSI). O auditor líder faz a auditoria de certificação (BSI, 2020).

A certificação é sobre o Sistema de Gestão de Segurança da Informação (SGSI), tratado pela ABNT NBR ISO/IEC 27001. Os auditores líderes fazem a auditoria do SGSI, em um escopo bem definido da organização. Há ainda auditoria interna, que prepara a organização para a auditoria externa, realizada por um auditor líder certificado, que ao final do processo certifica a organização em ISO 27001 naquele escopo definido.

O SGSI é composto por elementos-chave da ABNT NBR ISO/IEC 27001, estabelecendo uma abordagem organizacional para proteger a informação e seus critérios de confidencialidade, integridade e disponibilidade. Ele será discutido mais adiante.

REFLITA

Os sistemas de gestão não são tecnológicos ou, necessariamente, sistemas automatizados. O sistema é no seu sentido mais amplo, com o SGSI incluindo estratégias, planos, políticas, medidas, controles e diversos

instrumentos usados para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar a segurança da informação.

o

Ver anotações

A ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) é uma norma importante para os profissionais de segurança da informação, ao definir o código de prática para controles de segurança da informação. De uma forma geral, a ABNT NBR ISO/IEC 27001 se relaciona com a ABNT NBR ISO/IEC 27002 da seguinte forma:

- Escopo da aplicação da ABNT NBR ISO/IEC 27001 é definido.
- Análise de riscos é realizado.
- Aplicabilidade dos controles de segurança é formalizado.
- Controles de segurança são implementados, com base na ABNT NBR ISO/IEC 27002.

Os controles de segurança apropriados devem ser selecionados e implementados para que os riscos da organização sejam reduzidos a um nível aceitável, a partir dos requisitos de segurança da informação e da estratégia de tratamento dos riscos. A Figura 2.6 mostra os objetivos de controle definidos na ABNT NBR ISO/IEC 27002.

Figura 2.6 | Objetivos de controles de segurança da informação da ABNT NBR ISO/IEC 27002



Fonte: adaptado de ISO 27002 (2013).

Além das normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002, a família conta com outras normas importantes, sintetizadas no Quadro 2.1. Algumas normas não foram traduzidas para o português, como é o caso da ISO/IEC 27000, que trata do vocabulário.

Quadro 2.1 | Normas da família ISO 27000

Ver anotações

Normas da família ISO 27000

ISO/IEC 27000:2018	<i>Information technology — Security techniques — Information security management systems -- Overview and vocabulary</i>
ABNT NBR ISO/IEC 27001:2013	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2013	Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação
ABNT NBR ISO/IEC 27003:2020	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Orientações
ABNT NBR ISO/IEC 27004:2017	Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Monitoramento, medição, análise e avaliação
ABNT NBR ISO/IEC 27005:2019	Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação
ISO/IEC 27006:2015	<i>Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems</i>

Normas da família ISO 27000

Ver anotações

ABNT NBR ISO/IEC 27007:2018	Tecnologia da informação — Técnicas de segurança — Diretrizes para auditoria de sistemas de gestão da segurança da informação
ISO/IEC TS 27008:2019	<i>Information technology — Security techniques — Guidelines for the assessment of information security Controls</i>
ISO/IEC 27009:2020	<i>Information security, cybersecurity and privacy protection — Sector-specific application of ISO/IEC 27001 – Requirements</i>
ISO/IEC 27010:2015	<i>Information technology — Security techniques — Information security management for inter-sector and inter-organizational communications</i>
ISO/IEC 27011:2016	<i>Information technology — Security techniques — Code of practice for Information security Controls based on ISO/IEC 27002 for telecommunications organizations</i>
ISO/IEC 27013:2015	<i>Information technology — Security techniques — Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1</i>
ABNT NBR ISO/IEC 27014:2013	Tecnologia da Informação — Técnicas de Segurança — Governança de segurança da informação
ISO/IEC TR 27016:2014	<i>Information technology — Security techniques — Information security management — Organizational economics</i>
ABNT NBR ISO/IEC 27017:2016	Tecnologia da informação - Técnicas de segurança — Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem

Normas da família ISO 27000

ABNT NBR ISO/IEC 27018:2018	Tecnologia da informação — Técnicas de segurança — Código de prática para proteção de informações de identificação pessoal (PII) em nuvens públicas que atuam como processadores de PII	Ver anotações
ISO/IEC 27019:2017	<i>Information technology — Security techniques — Information security Controls for the energy utility industry</i>	
ISO/IEC 27031:2011	<i>Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity</i>	
ABNT NBR ISO/IEC 27032:2015	Tecnologia da Informação — Técnicas de segurança — Diretrizes para segurança cibernética	
ISO/IEC 27033-1:2015	<i>Information technology — Security techniques — Network security — Part 1: Overview and concepts</i>	
ISO/IEC 27033-2:2012	<i>Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security</i>	
ISO/IEC 27033-3:2010	<i>Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues</i>	
ISO/IEC 27033-4:2014	<i>Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways</i>	

Normas da família ISO 27000

0

Ver anotações

ISO/IEC 27033-5:2013	<i>Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)</i>
ISO/IEC 27033-6:2016	<i>Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access</i>
ISO/IEC 27034-1:2011/Cor 1:2014	<i>Information technology — Security techniques — Application security — Part 1: Overview and concepts — Technical Corrigendum 1</i>
ISO/IEC 27034-2:2015	<i>Information technology — Security techniques — Application security — Part 2: Organization normative framework</i>
ISO/IEC 27034-3:2018	<i>Information technology — Application security — Part 3: Application security management process</i>
ISO/IEC 27034-5:2017	<i>Information technology — Security techniques — Application security — Part 5: Protocols and application security Controls data structure</i>
ISO/IEC TS 27034-5-1:2018	<i>Information technology — Application security — Part 5-1: Protocols and application security Controls data structure, XML schemas</i>
ISO/IEC 27034-6:2016	<i>Information technology — Security techniques — Application security — Part 6: Case studies</i>
ISO/IEC 27034-7:2018	<i>Information technology — Application security — Part 7: Assurance prediction framework</i>

Normas da família ISO 27000

ISO/IEC 27035-1:2016	<i>Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management</i>	Ver anotações
ISO/IEC 27035-2:2016	<i>Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response</i>	
ISO/IEC 27035-3:2020	<i>Information technology -- Information security incident management — Part 3: Guidelines for ICT incident response operations</i>	
ISO/IEC 27036-1:2014	<i>Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts</i>	
ISO/IEC 27036-2:2014	<i>Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements</i>	
ISO/IEC 27036-3:2013	<i>Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security</i>	
ISO/IEC 27036-4:2016	<i>Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services</i>	
ABNT NBR ISO/IEC 27037:2013	Tecnologia da informação — Técnicas de segurança — Diretrizes para identificação, coleta, aquisição e preservação de evidência digital	

Normas da família ISO 27000

0

Ver anotações

ABNT NBR ISO/IEC 27038:2014	Tecnologia da informação — Técnicas de segurança — Especificação para redação digital
ISO/IEC 27039:2015	<i>Information technology — Security techniques — Selection, deployment and operations of intrusion detection and prevention systems (IDPS)</i>
ISO/IEC 27040:2015	<i>Information technology — Security techniques — Storage security</i>
ISO/IEC 27041:2015	<i>Information technology — Security techniques — Guidance on assuring suitability and adequacy of incident investigative method</i>
ISO/IEC 27042:2015	<i>Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence</i>
ISO/IEC 27043:2015	<i>Information technology — Security techniques — Incident investigation principles and processes</i>
ISO/IEC 27050-1:2019	<i>Information technology — Electronic discovery — Part 1: Overview and concept</i>
ISO/IEC 27050-2:2018	<i>Information technology — Electronic discovery — Part 2: Guidance for governance and management of electronic discovery</i>
ISO/IEC 27050-3:2020	<i>Information technology — Electronic discovery — Part 3: Code of practice for electronic discovery</i>

Normas da família ISO 27000

ABNT NBR ISO/IEC 27701:2019 Versão Corrigida:2020	Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes	o Ver anotações
ABNT NBR ISO 27799:2019	Informática em saúde — Gestão de segurança da informação em saúde utilizando a ISO/IEC 27002	

Fonte: ABNT (2020).

EXEMPLIFICANDO

Algumas normas ainda estão sendo trabalhadas, como para forense digital e segurança cibernética. E há casos curiosos, como a norma ABNT NBR ISO 27020:2014 ser da área de odontologia e a ISO 27048 ser da área de radiação.

Além das normas da família ISO 27000, que focam na segurança da informação, há outras normas que tratam de diferentes aspectos de segurança, como classificação da informação, segurança na área de saúde e privacidade. O Quadro 2.2 apresenta algumas dessas normas.

Quadro 2.2 | Normas que envolvem aspectos de segurança da informação

Normas que envolvem aspectos de segurança da informação

ABNT NBR 16167:2013	Segurança da Informação — Diretrizes para classificação, rotulação e tratamento da informação
ABNT NBR 16386:2015	Tecnologia da informação — Diretrizes para o processamento de interceptação telemática judicial

Normas que envolvem aspectos de segurança da informação	
ABNT ISO/TR 18638:2019	Informática em saúde — Orientações sobre educação da privacidade das informações em saúde em organizações de assistência à saúde
ABNT ISO/TS 21547:2016	Informática em saúde — Requisitos de segurança para arquivamento de registros eletrônicos de saúde — Princípios
ABNT NBR ISO 25237:2020	Informática em saúde — Pseudonimização
ABNT NBR ISO/IEC 29100:2020	Tecnologia da informação — Técnicas de segurança — Estrutura de Privacidade

Ver anotações

Fonte: ABNT (2020).

| SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (SGSI)

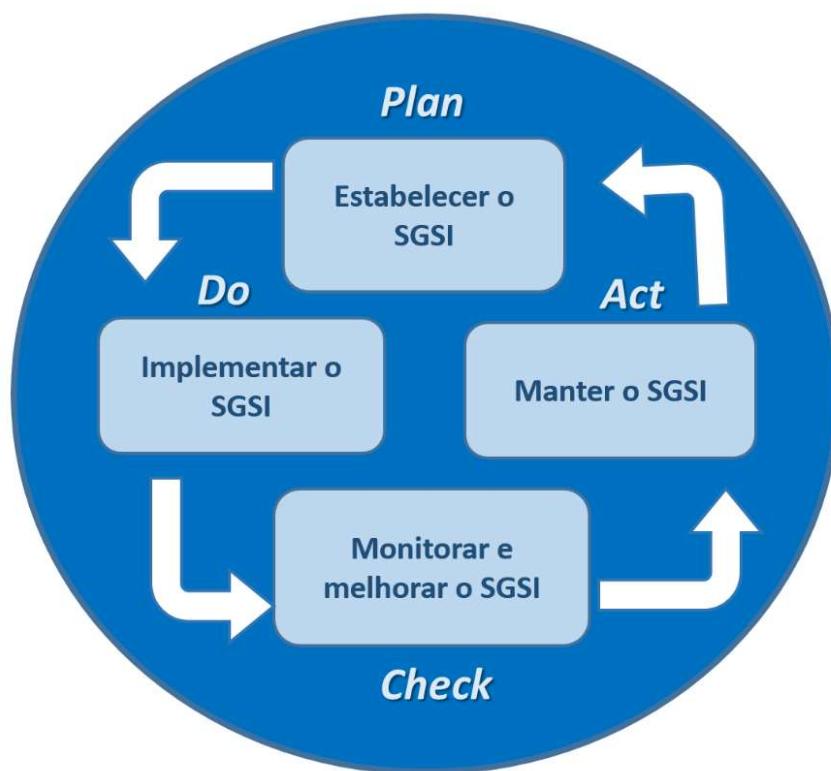
O SGSI é um elemento-chave para o fortalecimento da cultura de segurança da informação das organizações. E você pode, uma vez estabelecido um SGSI, certificar a sua empresa na ISO 27001. A norma ABNT NBR ISO/IEC 27001 estabelece os requisitos para o estabelecimento de um sistema de gestão de segurança da informação (ISO 27001, 2013).

O sistema de gestão da segurança da informação preserva a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

É importante que um sistema de gestão da segurança da informação seja parte e esteja integrado com os processos da organização e com a estrutura de administração global e que a segurança da informação seja considerada no projeto dos processos, sistemas de informação e controles (ISO 27001, 2013).

Você deve especificar e implementar o SGSI de acordo com as características específicas da sua organização, que apresenta necessidades e objetivos, requisitos de segurança, processos organizacionais, funcionários, tamanho e estrutura da organização. Como estes fatores evoluem com o tempo, é preciso estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta é uma das características principais dos sistemas de gestão, o processo de melhoria contínua, ou PDCA (Plan, Do, Check, Act), que pode ser visto na Figura 2.7.

Figura 2.7 | Melhoria contínua e PDCA do SGSI



Fonte: Palma (2016).

A Figura 2.8 mostra alguns requisitos de um SGSI que formam os fatores críticos de sucesso:

- **Contexto da organização**, incluindo questões internas e externas relevantes para o seu propósito, os requisitos das partes interessadas, incluindo requisitos legais, regulatórios e contratuais. Escopo do SGSI.

- **Liderança**, com comprometimento da alta direção, estabelecimento de uma política de segurança da informação e atribuição de papéis, autoridades e responsabilidades.
- **Planejamento**, com ações para contemplar riscos e oportunidades, avaliação de riscos de segurança da informação, tratamento de riscos de segurança da informação e estabelecimento de objetivos de segurança da informação para as funções e níveis relevantes.
- **Apoio**, com provimento de recursos, criação de competências, conscientização e comunicação.
- **Operação**, com planejamento operacional e controle, avaliação de riscos de segurança da informação, tratamento de riscos de segurança da informação.
- **Avaliação de desempenho**, com monitoramento, medição, análise e avaliação, além de auditoria interna e análise crítica pela direção,
- **Melhoria**, com tratamento de não conformidades e ação corretiva, além de melhoria contínua.

o

Ver anotações

Figura 2.8 | Requisitos de um SGSI



Fonte: elaborada pelo autor.

O contexto da organização está relacionado com as evoluções que ocorrem no ambiente de negócio, tecnológico e operacional.

| LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A LGPD (BRASIL, 2020) é uma lei que entrou em vigor no Brasil em setembro de 2020, visando proteger os direitos fundamentais de privacidade dos cidadãos brasileiros. A lei estabelece medidas para que haja a transparência na coleta e no tratamento de dados pessoais pelas organizações, que deve então prover a proteção adequada destes dados para garantir a privacidade dos seus usuários.

Ver anotações

No Capítulo I, Art. 5º da LGPD define alguns elementos importantes (Planalto, 2018):

- **Dado pessoal:** informação relacionada a pessoa natural identificada ou identificável.
- **Dado pessoal sensível:** dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
- **Dado anonimizado:** dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento.
- **Banco de dados:** conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
- **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
- **Controlador:** pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
- **Operador:** pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
- **Encarregado:** pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
- **Agentes de tratamento:** o controlador e o operador.
- **Tratamento:** toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

o

Ver anotações

O que devemos pensar é que, de acordo com a LGPD, os dados pessoais podem ser coletados mediante finalidade e base legal. O titular dos dados pessoais tem direitos, e a empresa que faz o tratamento dos dados pessoais passa a ser a responsável pelos dados pessoais coletados. E essa responsabilidade envolve, principalmente, a proteção, já que qualquer uso irregular, incluindo o seu vazamento, afeta a privacidade do titular. As empresas devem, assim, implementar controles de segurança da informação para evitar incidentes de segurança que podem levar ao vazamento de dados pessoais.

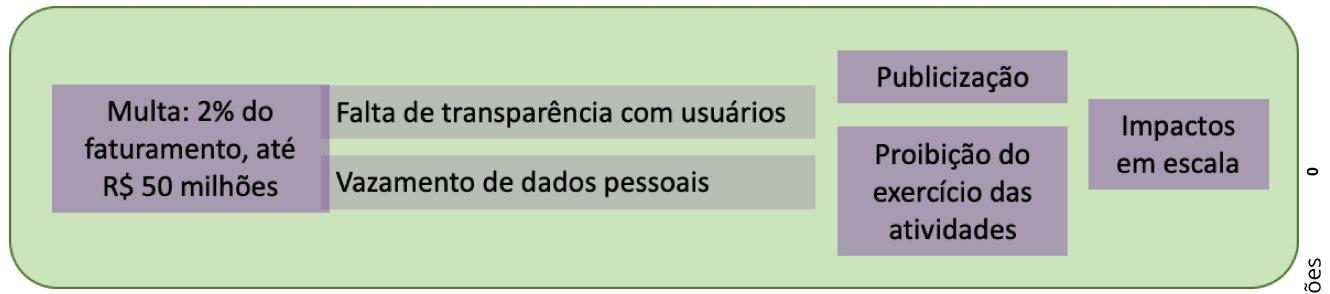
Ver anotações

EXEMPLIFICANDO

Uma empresa que coleta dados de uma pessoa, como nome e CPF, deve dizer de uma forma explícita a finalidade daquela coleta, incluindo a forma como aqueles dados coletados serão protegidos, por quanto tempo, e se haverá compartilhamento com terceiros. A pessoa pode ou não aceitar estes termos, e terá direito a revisões dos dados sendo tratados pela empresa, podendo solicitar a remoção do banco da empresa. Há casos, como em hotéis, em que há a coleta de dados pessoais no momento do check-in, como número de documentos e endereço. A coleta deve obedecer à finalidade relacionada à hospedagem, de acordo com a legislação do setor. No caso de uso destes dados para outros fins, como o compartilhamento para um parceiro comercial do hotel, o hóspede deve ser informado sobre ele e dar um consentimento explícito. Além deste aspecto de transparência nas relações com as pessoas, o hotel deve proteger todas os dados coletados. Em caso de vazamento destes dados, sejam eles em papel ou em meio digital, o hotel estará sujeito às sanções previstas na lei.

A lei estabelece sanções para quaisquer organizações, sejam elas grandes ou pequenas empresas, que não cumpram os requisitos estabelecidos, envolvendo a transparência nas relações com as pessoas, e vazamentos de dados pessoais, que comprometem a privacidade das pessoas (Figura 2.9).

Figura 2.9 | Sanções previstas na LGPD



Fonte: elaborada pelo autor.

Ver anotações

A Figura 2.10 ilustra uma visão do que é necessário para a proteção dos dados pessoais. A visão de riscos é importante para guiar as ações de segurança da informação. Um ponto adicional da LGPD é que a sua adequação é obrigatória, envolvendo fortemente aspecto de conformidade. Do nosso ponto de vista, a de segurança da informação, devemos implementar os controles de segurança para proteção de vazamentos, que podem ser decorrentes de ataques cibernéticos. Há uma estratégia possível de ser adotada para a adequação à LGPD, como a descrita em Garcia (2020).

Figura 2.10 | Visão integrada da privacidade e da proteção de dados pessoais



Fonte: elaborada pelo autor.

REFLITA

A LGPD trata da privacidade e da proteção de dados pessoais. Do ponto de vista da segurança, qual é o princípio que deve ser trabalhado, considerando a tríade CID (confidencialidade, integridade, disponibilidade)? Privacidade tem relação com a confidencialidade. Assim, empresas já com nível de maturidade mais alto em segurança da informação já têm maior aderência com a lei, já que tratam as informações em todos os princípios da CID. Alguns exemplos de controles de segurança são a criptografia e o controle de acesso a sistemas e banco de dados. Outro ponto importante da LGPD é que os dados pessoais devem ser protegidos, logo, esses dados devem ser primeiramente mapeados. Já os Dados confidenciais e dados corporativos não fazem parte do escopo da LGPD.

Ver anotações

SAIBA MAIS

A Lei Geral de Proteção de Dados Pessoais (LGPD) foca na proteção da privacidade dos cidadãos brasileiros, que passam a ter direitos sobre seus próprios dados. As empresas devem estabelecer uma relação de transparência para a coleta dos dados pessoais, com princípios importantes como a minimização para a coleta somente dos dados estritamente necessários, e a finalidade para definir a razão daquela coleta. Além disso, as organizações estarão sujeitas a sanções que vão de multas à paralização das atividades em caso de vazamento de dados pessoais. Para evitar os vazamentos e proteger os dados pessoais, as empresas precisam de controles de segurança da informação.

MARCO CIVIL DA INTERNET

A Lei nº 12.965, o Marco Civil da Internet (BRASIL, 2014) é a lei que regula o uso da internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

O Marco Civil da Internet trata de temas como neutralidade da rede, privacidade e retenção de dados, além de impor obrigações de responsabilidade civil aos usuários e provedores.

A lei ainda trata, ainda, da confidencialidade das comunicações privadas, e dá especial atenção aos dados de registros de acesso, como endereços de IP e *logins*.

Ver anotações

LEI CAROLINA DIECKMANN

A Lei nº 12.737, também conhecida como Lei Carolina Dieckmann (BRASIL, 2012), altera o código penal brasileiro, tornando crime a invasão de aparelhos eletrônicos para obtenção de dados particulares, a interrupção de serviço telemático ou de informática de utilidade pública. Os exemplos de crime, penalidade e agravante podem ser observados nos Quadros 2.3 e 2.4.

Quadro 2.3 | Lei Carolina Dieckmann

Crime	Pena	Exemplo
Invasão de um dispositivo. Pode estar conectado ou não a rede, mediante a violação de segurança com o objetivo de obtenção de informações sem autorização.	Detenção de 3 meses a 1 ano e multa.	Invasão de um computador para roubar informações, sem consentimento do proprietário.

Fonte: elaborado pelo autor.

Quadro 2.4 | Lei Carolina Dieckmann: agravantes

Agravante	Pena	Exemplo
Roubo de informação causando prejuízo econômico.	Aumenta a pena de detenção de 3 meses a 1 ano e 4 meses.	Cibercriminoso rouba conteúdo sigiloso de uma pessoa e apaga a informação, causando perda financeira.

Agravante	Pena	Exemplo	
Obtenção de conteúdo de comunicações privadas de forma não autorizada.	Aumenta a pena de detenção de 6 meses a 2 anos.	Roubo de conteúdos sigilosos de e-mails ou controle de computadores, tornando-os "zumbis".	
Divulgação e comercialização de conteúdo roubado de dispositivo.	Reclusão de 8 meses a 3 anos e 4 meses.	Roubo de informações sigilosas e venda ou divulgação na internet.	Ver anotações

Fonte: adaptado de UOL (2013).

POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

As políticas de segurança da informação constituem um dos principais controles de segurança da informação. Com a definição de elementos como regras, orientações, diretrizes, responsabilidades e sanções, as políticas de segurança da informação guiam as ações de todos da organização, incluindo os terceiros, prestadores de serviços, parceiros e fornecedores.

As políticas de segurança da informação devem tratar de todos os aspectos cotidianos da organização, incluindo os relacionados às pessoas, aos processos e às tecnologias.

EXEMPLIFICANDO

Quando um funcionário é contratado por uma empresa, ele deve saber quais são seus papéis e responsabilidades quanto à segurança da informação. Os aspectos de segurança envolvidos, por exemplo, com acessos remotos usando dispositivos da própria empresa devem estar bem definidos, claros e comunicados adequadamente. O mesmo para acessos remotos a partir de dispositivos pessoais. E quanto ao uso de aplicações de nuvem, aqueles não homologados pela área de segurança da empresa

podem ser utilizados? Todas as informações referentes às políticas de segurança devem ser informadas para todos da empresa de maneira clara e no que diz respeito a qualquer tipo de aplicações e dispositivos etc.

o

Ver anotações

Você deve construir as políticas de segurança com o apoio da alta direção da empresa. A própria norma ABNT NBR ISO/IEC 27001 (ISO 27001, 2013) diz que a alta direção deve estabelecer uma política de segurança da informação que:

- Seja apropriada ao propósito da organização.
- Inclua os objetivos de segurança da informação ou forneça a estrutura para estabelecer os objetivos de segurança da informação.
- Inclua um comprometimento para satisfazer os requisitos aplicáveis, relacionados com segurança da informação.
- E inclua um comprometimento para a melhoria contínua do sistema de gestão da segurança da informação.

Outro ponto importante que a norma ABNT NBR ISO/IEC 27001 estabelece é que a política de segurança da informação deve:

- Estar disponível como informação documentada.
- Ser comunicada dentro da organização.
- E estar disponível para as partes interessadas conforme apropriado.

Já a ABNT NBR ISO/IEC 27002 (ISO 27002, 2013) define como objetivo das políticas de segurança da informação o provimento de orientação da direção e apoio para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes, com dois controles:

- **Políticas para segurança da informação:** um conjunto de políticas de segurança da informação deve ser definido, aprovado pela direção, publicado e comunicado para os funcionários e partes externas relevantes.

- **Análise crítica das políticas para segurança da informação:** as políticas de segurança da informação devem ser analisadas criticamente a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

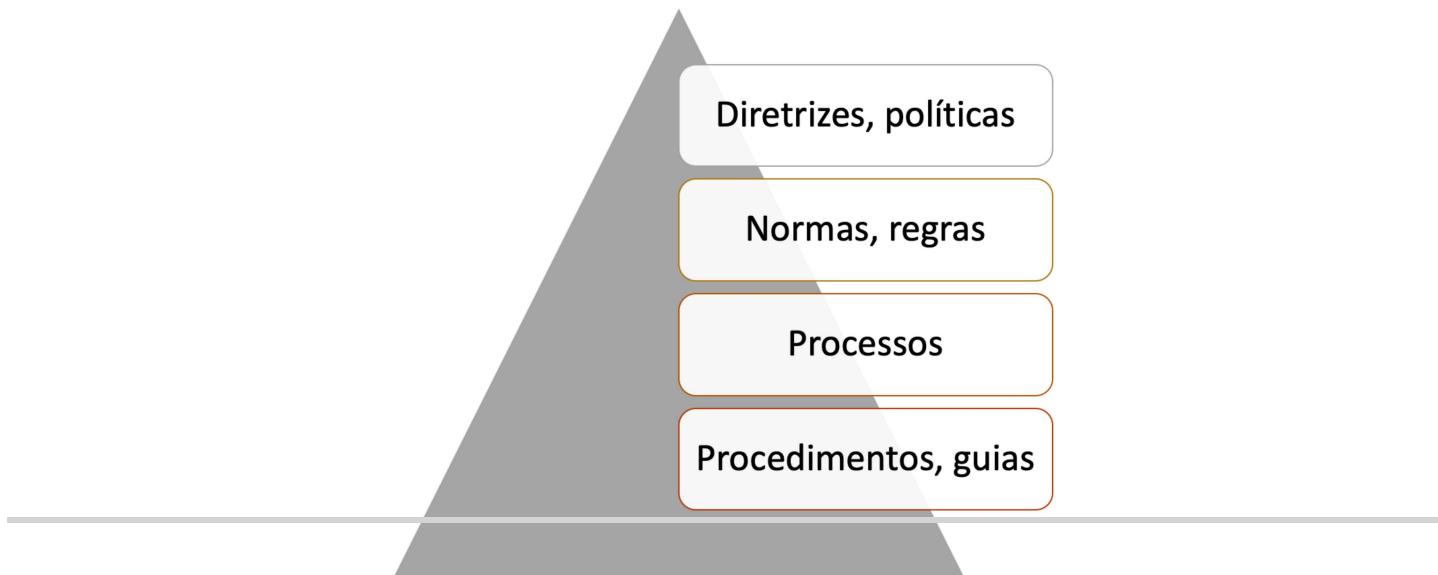
o

Ver anotações

Uma definição que irá ajudar você na definição, aprovação e publicação de políticas de segurança é o entendimento de que elas constituem um conjunto de documentos com regras, papéis e responsabilidades que devem ser seguidos por todos os funcionários e partes externas relevantes. Este conjunto de documentos pode ser definido em partes, pensando em quem irá ler. Por exemplo, uma política de senhas pode apresentar as regras para a definição de senhas de usuários para acesso aos serviços corporativos. Mas e as senhas administrativas, utilizadas pelos administradores de sistemas que possuem acesso privilegiado? Nesse caso, para acessos privilegiados, seria melhor ficar em uma mesma política, ou seria melhor uma política de senhas diferenciada? Esta definição depende de cada empresa, e daí a importância do SGSI.

Outra questão aparece quanto à forma de cumprimento das políticas de segurança pelos funcionários. Muitas vezes há a necessidade de procedimentos específicos, que dizem, além “do que” deve ser feito, o “como” deve ser feito. Assim, a estrutura de documentos que constitui as políticas de segurança da informação das empresas poderia ser como a Figura 2.11.

Figura 2.11 | Árvore de documentos que formam a política de segurança da informação



Fonte: elaborada pelo autor.

Ver anotações

Assim, uma política de segurança poderia ser um documento mais diretivo, que coloca os aspectos gerais da segurança da informação, com os assuntos relativos desmembrados em normas. Um exemplo importante diz respeito às senhas, com normas e as regras de escolha e renovação. Destas regras há desdobramentos para os usuários, que podem seguir os processos para a escolha de senhas, junto dos guias. E, para os administradores de sistemas, os processos de configuração dos serviços devem seguir as regras definidas na norma.

TECNOLOGIAS DE SEGURANÇA DA INFORMAÇÃO

Os controles de segurança da informação devem ser definidos de acordo com uma avaliação de riscos, que leva em consideração aspectos próprios de cada organização. Os frameworks de segurança e a família ISO 27000 são de extrema importância para a definição destes controles de segurança, os quais podem ser físicos, tecnológicos ou processuais, e uma fonte importante para você seguir é a norma ABNT NBR ISO/IEC 27002 (ISO 27002, 2013), com os objetivos de controle de controle e os controles de segurança da informação.

Para visualizar o objeto, acesse seu material digital.

Fonte: adaptado de ISO 27002 (2013).

PESQUISE MAIS

Vale a pena você ler a Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais (BRASIL, 2020). Há no texto elementos importantes para a sua evolução como profissional de segurança da informação, e o que está na lei será aplicado por você tanto como pessoa física quanto como profissional da área.

- BRASIL. Lei Geral de Proteção de Dados Pessoais. Presidência da República – Secretaria-Geral – Subchefia para Assuntos Jurídicos. **Lei nº**

13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

Ver anotações

Chegamos ao final desta seção, que tratou da gestão de segurança da informação e da integração entre visões que levam em consideração os contextos particulares de cada organização. O conhecimento de *frameworks* e normas de segurança da informação é importante para a sua formação como profissional da área, principalmente porque direciona as ações e possibilita uma visão holística dos aspectos da segurança da informação que precisam ser compreendidos.

FAÇA VALER A PENA

Questão 1

A família ISO 27000 é composta por um conjunto de normas que trata de segurança da informação, incluindo assuntos como sistema de gestão de segurança da informação, controles de segurança, segurança na área de saúde, segurança em comunicações, segurança de redes, resposta a incidentes, segurança de aplicações e privacidades, entre outros.

Assinale as normas que certificam uma empresa em segurança da informação.

a. ABNT NBR ISO/IEC 27001.

b. ABNT NBR ISO/IEC 27002.

c. ABNT NBR ISO/IEC 27003.

d. ABNT NBR ISO/IEC 27004.

e. ABNT NBR ISO/IEC 27005.

Questão 2

Sobre as políticas e os controles de segurança da informação, analise as afirmativas a seguir:

- I. O contexto da organização, como seus objetivos de negócios, não influencia na segurança da informação.

II. Os controles de segurança da informação podem tratar de aspectos relacionados às pessoas, aos processos e às tecnologias.

III. A família ISO 27000 trata de segurança da informação, sendo composta por uma série de normas como a ABNT NBR ISO/IEC 27001 e a ABNT NBR ISO/IEC 27003.

É correto o que se afirma em:

a. I e II, apenas.

b. I e III, apenas.

c. II, apenas.

d. II e III, apenas.

e. III, apenas.

Questão 3

A Lei Geral de Proteção de Dados Pessoais (LGPD) visa a privacidade dos cidadãos brasileiros, com as organizações públicas e privadas tendo que estabelecer relações transparentes para a coleta e o tratamento de dados pessoais, e a proteção destes dados pessoais.

Assinale a alternativa que corresponde ao princípio de segurança da informação envolvido com a LGPD, com o motivo que a segurança da informação é necessária.

a. Integridade e controles de segurança para evitar vazamentos.

b. Disponibilidade e controles de segurança para evitar vazamentos.

c. Confidencialidade e controles de segurança para evitar vazamentos.

d. Integridade e controles de segurança para evitar privacidade.

e. Confidencialidade e controles de segurança para evitar privacidade.

REFERÊNCIAS

Ver anotações

ABNT. Associação Brasileira de Normas Técnicas. **ABNT Catálogo**. Disponível em:

<https://bit.ly/3b9isIE>. Acesso em: 25 out. 2020.

ABNT – Associação Brasileira de Normas Técnicas. **NBR ISO/IEC 27001:2013**

Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos.

ABNT – Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:2013**

Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação.

AGUILERA-FERNANDES, E. **Padrões, Normas e Políticas de Segurança da Informação**. São Paulo: Senac São Paulo, 2017. Disponível em:

<https://bit.ly/2O2o3kR>. Acesso em: 13 out. 2020.

BRASIL. Lei Carolina Dieckmann. Presidência da República – Casa Civil – Subchefia para Assuntos Jurídicos. **Lei nº 12.737, de 30 de novembro de 2012**. Disponível em: <https://bit.ly/3uOC32d>. Acesso em: 8 nov. 2020.

BRASIL. Marco Civil da Internet. Presidência da República – Casa Civil – Subchefia para Assuntos Jurídicos. **Lei nº 12.965, de 23 de abril de 2014**. Disponível em: <https://bit.ly/3bWwEgV>. Acesso em: 8 nov. 2020.

BRASIL. Lei Geral de Proteção de Dados Pessoais. Presidência da República – Secretaria-Geral – Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://bit.ly/2NXIssh>. Acesso em: 25 out. 2020.

BSI – British Standards Institution. **Formação de Auditor Líder em Sistema de Gestão de Segurança da Informação ISO/IEC 27001:2013 – IRCA**. Disponível em: <https://bit.ly/2MJx41L>. Acesso em: 24 out. 2020.

CIS – Center for Internet Security. **CIS Controls**. Disponível em: <https://bit.ly/30cBNMx>. Acesso em: 24 out. 2020.

COBIT. COBIT 5. **ISACA**. Disponível em: <https://bit.ly/2NQCBEp>. Acesso em: 25 out. 2020.

GARCIA, L. R.; AGUILERA-FERNANDES, E.; GONÇALVES, R. A. M.; PEREIRA-BARRETTO, M. R. **Lei Geral de Proteção de Dados Pessoais (LGPD) – Guia de Implantação.** São Paulo: Editora Edgard Blücher Ltda., 2020. Disponível em: <https://bit.ly/3uOGlqp>. Acesso em: 8 nov. 2020.

ISA – International Society of Automation. **ANSI/ISA-62443:** Security for industrial automation and control systems. Disponível em: <https://bit.ly/3baMMfA>. Acesso em: 25 out. 2020.

NIST – National Institute of Standards and Technology. **Framework for Improving Critical Infrastructure Cybersecurity.** Version 1.1, 16 abr, 2018. Disponível em: <https://bit.ly/2Oo9zeT>. Acesso em: 24 out. 2020.

NIST – National Institute of Standards and Technology. **SP 800-53 Rev. 5 - Security and Privacy Controls for Information Systems and Organizations**, set. 2020. Disponível em: <https://bit.ly/2NXISPD>. Acesso em: 25 out. 2020.

PALMA, F. Sistema de Gestão de Segurança da Informação (SGSI). **Portal GSTI**. Disponível em: <https://bit.ly/38oO05p>. Acesso em: 24 out. 2020.

SPAMFighter. Societe Generale Employee Confesses to Trading through Hacked Systems, **News**, 5 fev. 2008. Disponível em: <https://bit.ly/3kOxznJ>. Acesso em: 24 out. 2020.

UOL. "Lei Carolina Dieckmann" sobre crimes na internet entra em vigor. **Tilt**, 2 abr. 2013. Disponível em: <https://bit.ly/3rdJo9z>. Acesso em: 8 nov. 2020.