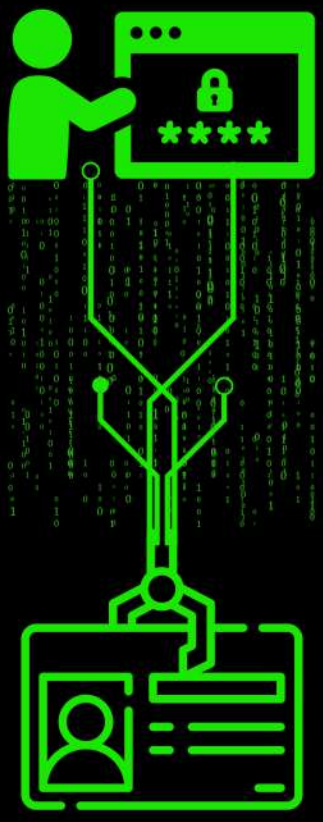
COMITÊ DE CIBERSEGURANÇA

ANADD

Associação Nacional de
Advogadas e Advogados de Direito Digital

Introdução à Cibersegurança



ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital
Registro ISBN nº 978-65-999397-0-9

Sumário

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

COMITÊ DE CIBERSEGURANÇA

ANADD

Associação Nacional de
Advogadas e Advogados de Direito Digital

GT Cibersegurança

Coautores:

Andreza Sobreira
Crystine Joranhezon
Eduardo Dias
Everton Lopes
Izaac Alencar
Maria Santos

Coordenação:

Andreza Sobreira e Izaac Alencar

Arte e Design:

Ricardo Castro Cajazeira

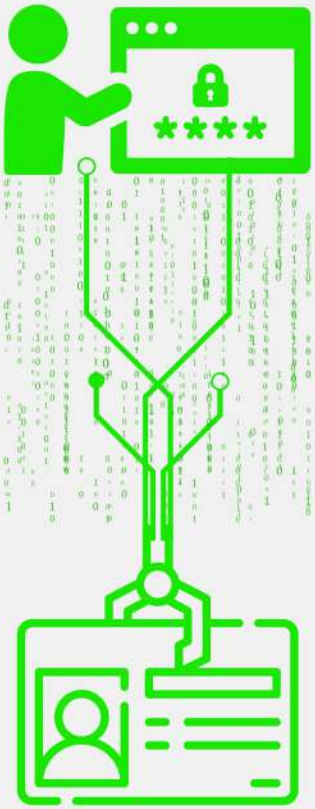
Revisão:

Andreza Sobreira, Fábio Uema e Ricardo Castro Cajazeira

ISBN registrado sob nº: 978-65-999397-0-9
Título: Introdução à Cibersegurança
Subtítulo: Principais Aspectos da Segurança da Informação
Formato: Livro Digital
Veiculação: Digital

ANADD.ORG

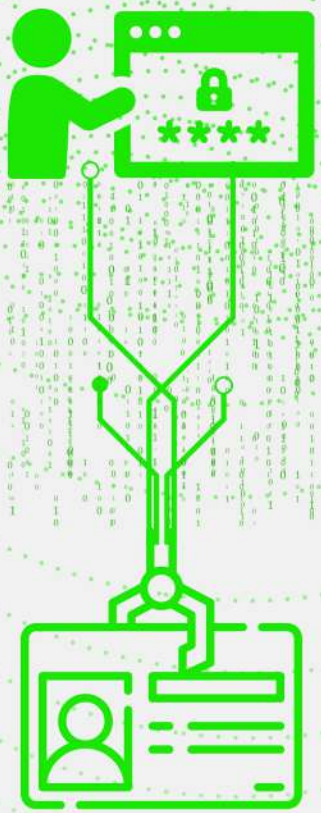
Introdução



A expressão "Segurança da informação" em que pese não ser tema novo, tem ganhado destaque nos últimos anos, seja pela crescente de ameaças cibernéticas, pelos aumentos de incidentes, por imposições legais como a Lei nº 13.709/18 Lei Geral de Proteção de Dados Pessoais (LGPD), por exigência de mercado, avanços tecnológicos, dentre outros motivos. Ocorre que para uma melhor compreensão acerca da segurança da informação é necessário revisar e entender alguns conceitos que permeiam não só a segurança da informação propriamente dita, mas as definições de outras palavras que se correlacionam diretamente com o tema.

Outrossim, é necessário compreender que a segurança da informação está presente em todas as organizações, que a informação pode ser o ativo mais valioso e que está muito além de dados pessoais.

Introdução



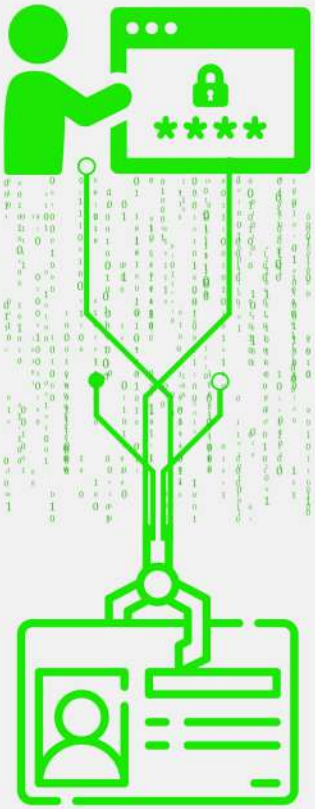
A informação pode ser mais ou menos valiosa a depender do modelo de negócio, que por consequência, deve haver uma classificação dessas informações enquanto ativos. Isso porque a informação pode necessitar de mais ou menos proteção, e quem irá determinar o valor da informação é o dono do ativo, mas para isso é necessário compreender o que é, para que serve, e quanto vale a informação.

Trataremos ainda neste *e-book*, temas introdutórios sobre incidentes de segurança, planos de resposta, seus conceitos e de que forma é possível iniciar a elaboração de documentos necessários, normas, *frameworks* aplicáveis a temática, dentre outros assuntos.

A ideia aqui é trazer os principais aspectos conceituais e objetivos sobre segurança da informação, governança, riscos de forma relacionada às principais normas e referências sobre o assunto para estudantes, advogados, consultores e demais interessados em Segurança da Informação.

Sumário

1. Princípios, conceitos e definições

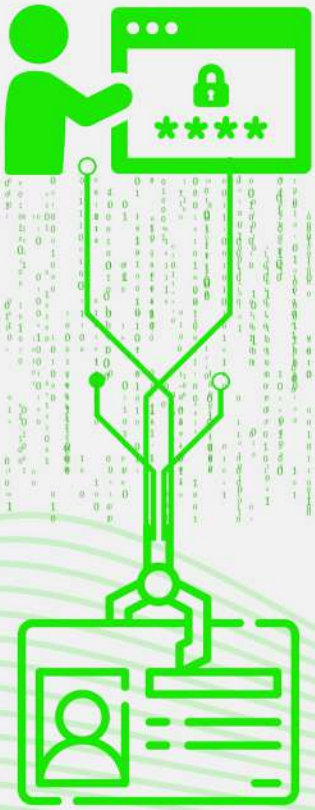


Também chamados de pilares e compondo ainda o conceito de segurança da informação a Confidencialidade, Integridade e Disponibilidade são os princípios críticos da Segurança da Informação que podem variar de acordo com cada modelo de negócio o nível de segurança a ser empregado para cada um destes princípios.

1.1 Segurança da Informação: É a proteção de informações contra uma ampla gama de ameaças, a fim de garantir a continuidade do negócio, minimizar o risco do negócio e maximizar o retorno sobre os investimentos e oportunidades do negócio. Portanto, é a preservação da confidencialidade, disponibilidade e integridade.

1.2 Confidencialidade ou exclusividade: propriedade de que as informações não são disponibilizadas ou divulgadas a indivíduos, entidades ou processos não autorizados (ISO 27000). Compõem a confidencialidade o contexto da organização, liderança e comprometimento, objetivos de segurança da Informação, política de segurança da informação, documentação; [1] FERREIRA, Fernando Nicolau Freitas. Política de Segurança da Informação – Guia Prático para Elaboração e Implementação 2ª edição. Rio de Janeiro: Editora Moderna, 2008. p.36

1. Princípios, conceitos e definições

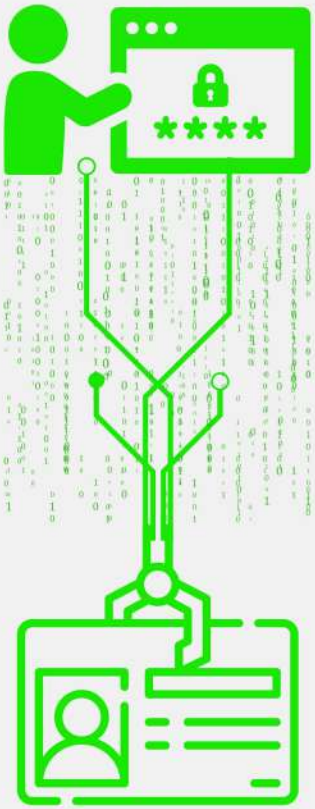


1.3 Integridade: Propriedade de precisão e completude (ISO 27000). Compõem a integridade a gestão de incidentes, papéis, responsabilidades e competências, gerenciamento de riscos, monitoramento de desempenho de KPIs, melhoria contínua;

1.4 Disponibilidade: propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada (ISO 27000). A disponibilidade tem como características a oportunidade, a continuidade e a robustez. Compõem a disponibilidade a comunicação, conscientização dos usuários, gestão de fornecedores, auditoria interna e melhoria contínua.

1.5 Sistema de Gestão/Gerenciamento da Segurança da Informação (SGSI) ou *Information Security Management System* (ISMS): é o resultado do gerenciamento e aplicação de objetivos, procedimentos, políticas, e diretrizes dentre outras medidas administrativas que objetivam a proteção dos ativos de informação e redução dos riscos que permeiam a segurança da informação. Portanto, é a interligação de vários processos de segurança. (ISO 27001 e Política de Segurança da Informação – Guia prático para elaboração e implementação, 2008).

1. Princípios, conceitos e definições

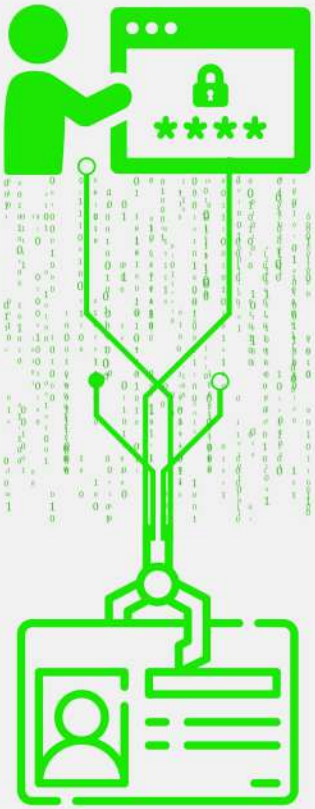


1.6 Ciclo PDCA ou Clico de *Deming* ou Ciclo de *Shewhart*: consiste em metodologia de melhoria de processos. O ciclo PDCA remete a 4 (quatro) etapas, quais sejam, Planejar (*plan*), Implementar/executar/fazer (*Do*), Verificar/Checar (*Check*) e, Agir (*Act*). Através do ciclo PDCA é possível mapear os processos ou revisitar aprendendo com ele, aprimorando, aplicando as melhorias e fazendo uma gestão contínua dos processos. Para percorrer o Ciclo PDCA é necessário entender que dentro de cada fase há ainda subfases que permitem alcançar o objetivo. São elas:

FASE 1 - Planejar (*Plan*): localizar problemas e estabelecer planos de ação. Estruturação do SGSI, plano diretor de segurança, diagnóstico de segurança, avaliação de tratamento dos riscos e seleção dos controles de segurança e declaração de aplicabilidade;

FASE 2 - Fazer/Executar (*Do*): execução do plano, colocar em prática. Comitê de segurança da informação, política de segurança da informação, classificação da informação, plano de continuidade dos negócios e de TI, treinamento e conscientização, implementação dos controles especificados na declaração de aplicabilidade;

1. Princípios, conceitos e definições



FASE 3 - Verificar/Checar (*Check*): verificar atingimento de meta, acompanhar indicadores. Monitoramento dos controles de segurança, gestão de incidentes, revisão do nível do risco residual e auditoria inte

FASE 4 - Agir (*Act*): Ação corretiva no insucesso, padronizar a treinar no sucesso. Implementação de melhorias, ações corretivas e preventivas, comunicação das ações e resultados para a alta administração e partes interessadas e assegurar que as melhorias foram implementadas e atenderam as expectativas.

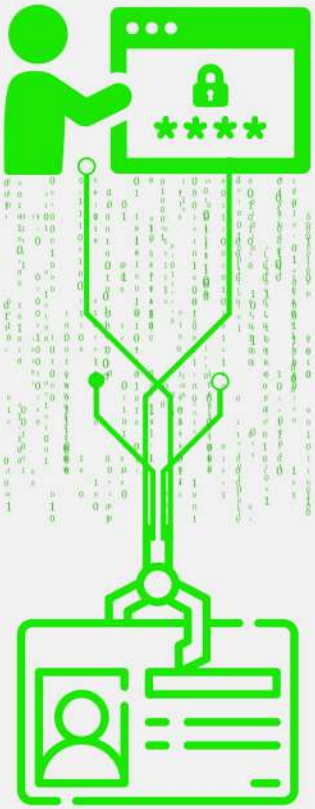
1.7 Ameaça: potencial causa de um incidente.

1.8 Vulnerabilidade: fraqueza, um ponto fraco.

1.9 Risco: probabilidade de um agente de ameaça tirar vantagem de uma vulnerabilidade em um ativo e o impacto no negócio correspondente.

1.10 Análise de riscos: é o processo que leva a compreensão do nível de risco (importância) e apoio para as decisões (justificar escolhas rentáveis). Essa análise auxilia a esclarecer as ameaças e selecionar as medidas necessárias.

1. Princípios, conceitos e definições



1.11 Dados: se tornam informação quando processados e ganham significado (modelo DICS – Dados – Informação – Conhecimento – Sabedoria).

1.12 Informação: é um conjunto de dados que tem relação (significado). Por sua vez, o Valor da Informação é determinado por quem a recebe, ou seja, é o beneficiário quem determina o valor da informação em um processo de negócio.

1.13 Informática: é o processo para converter dados em informação.

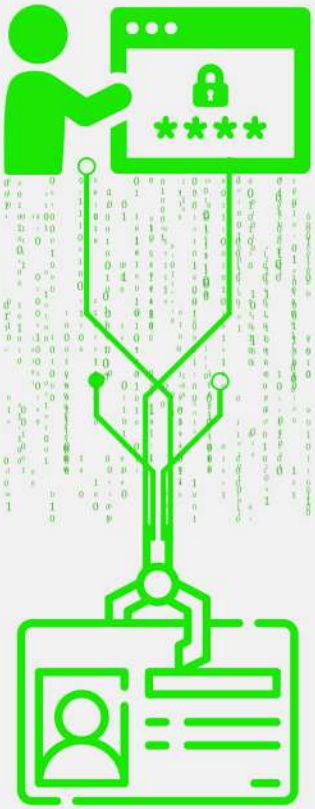
1.14 Aspectos da Confiabilidade (CID): a) confidencialidade que deve ser restrito a um grupo definido e autorizado; b) integridade em sua completeza; e, c) disponibilidade na linha do tempo, continuidade e robustez.

1.15 Política de Segurança da Informação (PSI): é o documento formal e que dá a orientação e suporte sobre segurança da informação. Deve ser amplamente divulgada para todos funcionários e parceiros relevantes.

1.16 Código de conduta: é o documento formal que estabelece as regras para os colaboradores em relação uso de ativos.

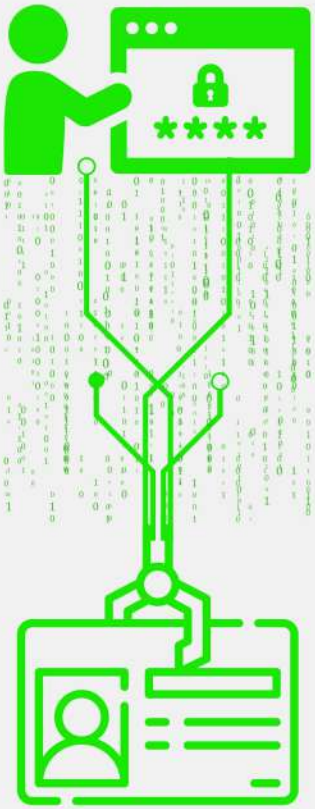
1. Princípios, conceitos e definições

1.18 Classificação de informação: é essencial para determinar o nível de proteção adequado ou como processar determinada informação e é ou deve ser feita pelo dono do ativo.



Sumário

2. Aspectos da Segurança da Informação

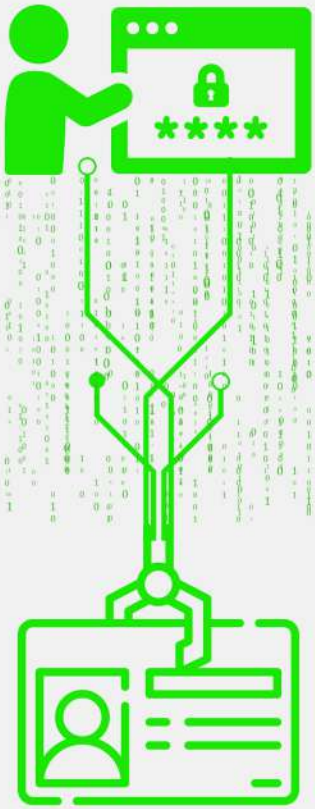


Inicialmente, antes de falar sobre o tema em si, é importante relembrarmos o conceito de Segurança da Informação, pois está relacionado diretamente com os pilares apresentados.

Segurança da Informação é a proteção da informação contra diversos tipos de ameaças, garantindo a continuidade do negócio, minimização dos riscos e maximização dos investimentos. Para tanto, são necessários controles, políticas, processos, procedimentos, estruturas e funções implementadas que garantam um nível adequado de proteção e que possibilitem a preservação da confidencialidade, integridade e disponibilidade da informação (NBR ISO/IEC 27002:2013).

Em resumo, segurança da informação é o conjunto de elementos que visa proteger as informações, especialmente baseadas em 3 (três) pilares essenciais e outros adicionais que falaremos abaixo.

2. Aspectos da Segurança da Informação



2.2 Elementos da Segurança da Informação

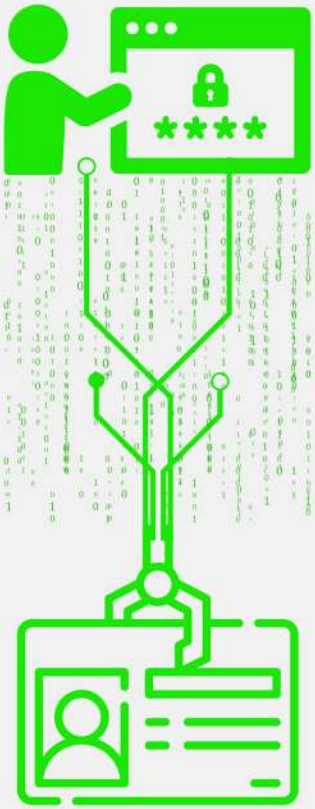
O conjunto de elementos que compõem a segurança da informação varia conforme autor e mesmo a necessidade da empresa, entretanto, destacam-se os principais (e complementares), que são: o triângulo CIA (*Confidentiality, Integrity and Availability*, ou Confidencialidade, Integridade e Disponibilidade - CID), considerado por muitos o conjunto de elementos/pilares essenciais, e o Hexagrama Parkeriano, que engloba o triângulo CIA, mas inclui os elementos 'Posse ou controle', 'Autenticidade' e 'Utilidade'.

2.3 Triângulo Cia (*Confidentiality, Integrity And Availability*)

Não se sabe ao certo a origem do Triângulo CIA, mas representa a tríade dos principais atributos que orientam preliminarmente a segurança da informação. Em resumo, o triângulo é composto por:

I. Confidencialidade (*Confidentiality* - C);
II. Integridade (*Integrity* - I);
III. Disponibilidade (*Availability* - A).

2. Aspectos da Segurança da Informação



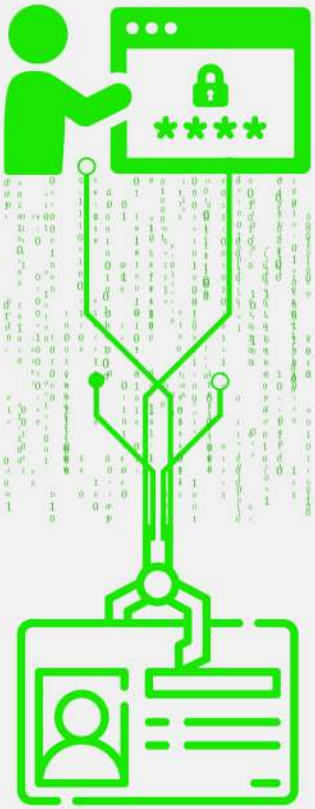
2.4 Hexagrama Parkeriano

O Hexagrama Parkeriano é um conjunto de 6 (seis) elementos da segurança da informação proposto por *Donn B. Parke*r em 1988, somando três elementos aos do triângulo CIA, já explicado acima. Os elementos do hexagrama Parkeriano são:

I. Confidencialidade;
II. Posse ou controle;
III. Integridade;
IV. Autenticidade;
V. Disponibilidade; e
VI. Utilidade.

2. Aspectos da Segurança da Informação

2.5 Outros Elementos



Além dos elementos dispostos no Triângulo CIA e no Hexagrama Parkeriano, alguns elementos adicionais, dispostos na doutrina[1][2] e em normas internacionais, merecem atenção, como:

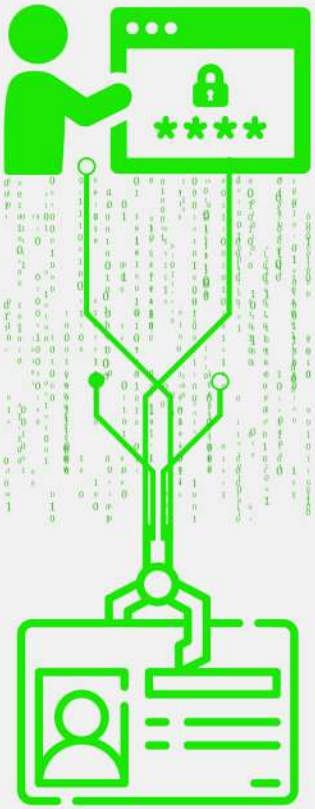
I. Autenticidade: capacidade de identificação da origem da informação, ou seja, garantia de que o remetente seja realmente quem quem alega ser.

II. Confiabilidade: garantia de que a informação é resistente a falhas e pode ser confiada.

III. Não repúdio: habilidade de vincular uma informação a alguém de maneira irretratável, ou seja, sem possibilidade do remetente da informação negar sua autoria.

IV. Responsabilidade: Atribuição de ações e decisões a uma entidade.

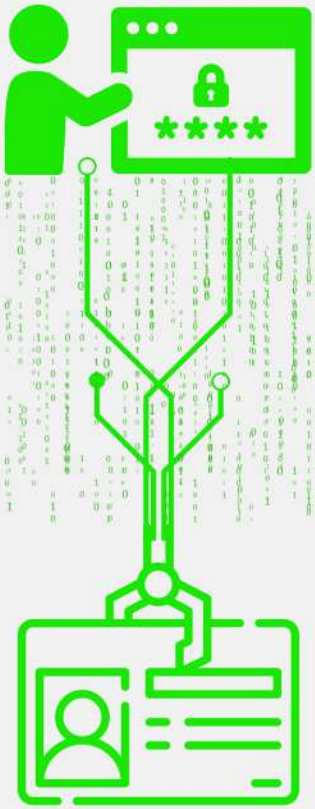
2. Aspectos da Segurança da Informação



Um programa de segurança da informação pode ter diversos objetivos e nuances de aplicação, mas os princípios mais importantes em todos os programas de segurança são a confidencialidade, integridade e disponibilidade. Outros princípios adicionais podem ser aplicados e possuem sua importância e relevância no processo, dependendo das especificidades do caso concreto e necessidades, sejam estruturais/organizacionais e/ou normativas/regulatórias.

O nível de segurança requerido para executar esses princípios é diferente para cada empresa, pois cada uma tem sua própria combinação de objetivos e requisitos de negócio e de segurança. Todos os controles de segurança, mecanismos e proteções são implementados para prover um ou mais desses princípios, e todos os riscos, ameaças e vulnerabilidades são medidos pela sua capacidade potencial de comprometer um ou todos os princípios do triângulo CIA. (*HINTZBERGEN, Jule; HINTZBERGEN*)

2. Aspectos da Segurança da Informação



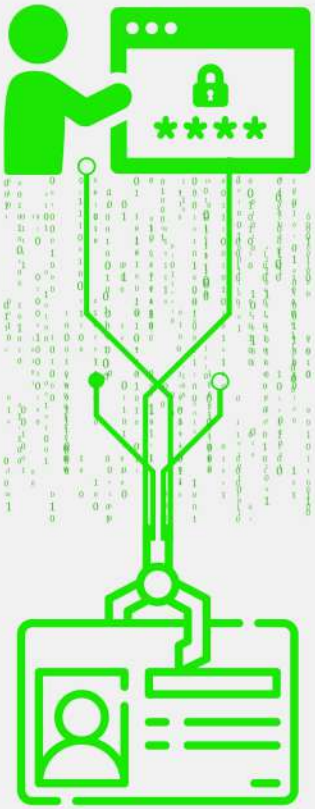
2.6 O Triângulo Cia e os Principais Pilares da Segurança da Informação - o Triângulo CIA é o conjunto mais utilizado e básico para elementos da segurança da informação, portanto, daremos um destaque especial e nos aprofundaremos mais na confidencialidade, integridade e disponibilidade, que são princípios críticos de segurança.

2.7 Confidencialidade - a confidencialidade, também chamada de exclusividade ou mesmo privacidade, é o princípio que determina que a informação é divulgada apenas àqueles que possuem autorização para acessá-la. Como exemplo, informações confidenciais de uma empresa não devem ser divulgadas e nem estarem disponíveis para público em geral ou funcionários sem autorização ou função relacionada a elas, para isso, é necessário que a informação possua um nível necessário de sigilo em cada elemento de processamento de dados, impedindo a divulgação não autorizada.

2. Aspectos da Segurança da Informação

Em resumo, confidencialidade busca prevenir que a Informação seja exposta à visualização não autorizada.

2. Aspectos da Segurança da Informação

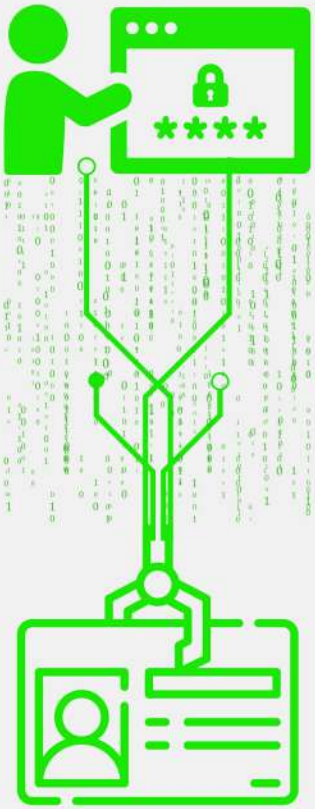


2.8 Integridade - a integridade se refere à garantia de que a informação será exata e íntegra, sem qualquer tipo de alteração ou tratamento não pretendido e autorizado. Espera-se que a informação não possua ruídos e seja estável, bem como não possa ser alterada aleatoriamente, havendo, ainda, uma garantia de que os meios onde a informação estará armazenada sejam confiáveis (HINTZBERGEN, Jule; HINTZBERGEN).

Uma determinada informação, como, por exemplo, o cadastro interno de clientes, não deve estar disponível livremente para edição, correndo o risco de haver alterações indesejadas, substituição de dados ou mesmo exclusão, é necessário que apenas os responsáveis por alimentar aquelas informações tenham acesso e permissões para modificação.

Integridade significa que a informação é completa, perfeita e intacta, assim, a integridade garante que ela não seja exposta ao manuseio não autorizado, utilizando-se de técnicas de criptografia, bem como políticas e controles internos e externos para proteção e segurança da informação.

2. Aspectos da Segurança da Informação



2.9 Disponibilidade - as características do princípio da disponibilidade são:

Oportunidade: a informação está disponível quando necessário.

Continuidade: a equipe consegue continuar trabalhando no caso de falha.

Robustez: existe capacidade suficiente para permitir que toda a equipe trabalhe no sistema (HINTZBERGEN, Jule; HINTZBERGEN - Fundamentos da Segurança da Informação).

O princípio da disponibilidade visa prevenir que a informação deixe de estar acessível no momento necessário à sua utilização, sendo, portanto, necessário que se estabeleçam mecanismos e procedimentos emergenciais para garantir que a informação seja acessada e/ou recuperada em caso de incidentes. Neste sentido, vale a menção dos procedimentos de *backup*.

Sumário

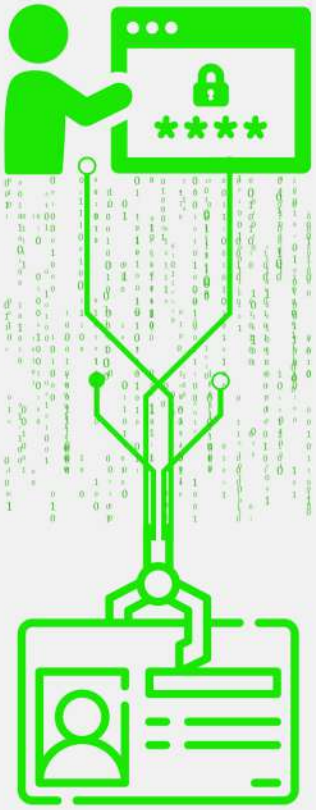
ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

3. Normas/Legislações/*Frameworks*

A Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD), em sua Seção II, Das Boas Práticas e da Governança, informa, no Art. 50 § 2º sobre as características mínimas de um Programa de Governança em Privacidade – PGP.

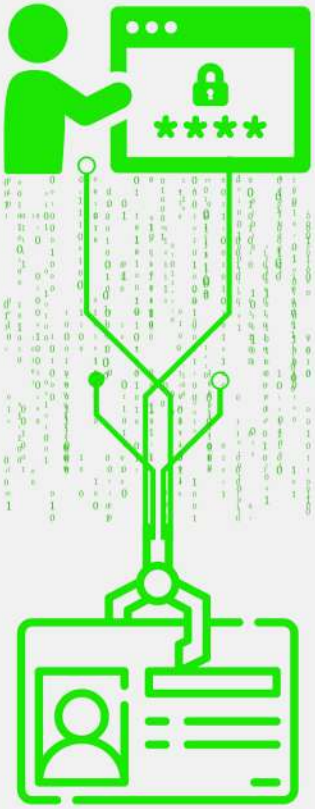
Nesse passo, a fim de cumprir a Legislação vigente, ou melhor explicitando, no que tange a fazer cumprir a lei, quanto a segurança, e as ações de prevenção e governança de dados, as normas surgem como peça fundamental.

A figura abaixo, apresentada pelo Governo Federal, com as características mínimas de um programa de Gerenciamento de Privacidade.



- Comprometimento do controlador em adotar processos e políticas internas que cumpram normas e boas práticas relativas à proteção de dados pessoais
- Aplicável a todo o conjunto de dados pessoais sob seu controle, independentemente da forma coletada.
- Adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados.
- Estabelecimento de políticas e salvaguardas adequadas, baseadas em processo de avaliação sistemático de impactos e riscos à privacidade.
- Estabelecimento de relação de confiança com o titular, por meio de atuação transparente com mecanismos de participação do titular.
- Integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos.
- Com planos de resposta a incidentes e remediação.
- Constantemente atualizado com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas.

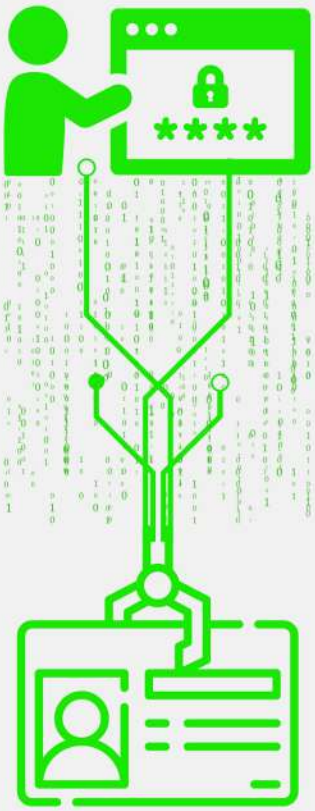
3. Normas/Legislações/*Frameworks*



Nesse sentido, a estrutura do PGP apresentada, fora justamente inspirada no ciclo PDCA (*Plan, Do, Check e Act*) bem como nas normas ABNT NBR ISO/IEC 27001:2013 e ABNT NBR ISO/IEC 27701:2019. Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação e ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

As normas ISO têm por objetivo a padronização de procedimentos de conduta, implementação de soluções, entre outras questões que elevam o patamar das empresas ao nível internacional, e mais, trazer as evidências necessárias que a legislação acerca da proteção e dados estejam sendo cumpridas, essas normas foram criadas pela Organização Internacional de Padronização (ISO), com a finalidade de melhorar a qualidade de produtos e serviços. A ISO, é uma das maiores organizações que desenvolve normas no mundo, e começou a funcionar oficialmente no ano de 1947, com sua sede em Genebra, Suíça. As normas qualificam produtos em várias organizações do mundo todo.

3. Normas/Legislações/*Frameworks*



A título de entendimento e compreensão: **I**) ABNT refere-se ao termo: Associação Brasileira de Normas Técnicas; **II**) NBR é a sigla para Norma Brasileira que é aprovada pela Associação Brasileira de Normas Técnicas (ABNT); **III**) ISO refere-se a (Organização Internacional de Normatização ou *International Organization for Standardization*), responsável por desenvolver normas.

Esse conjunto estabelece documentos padrões para a implantação do sistema de gestão de qualidade. No Brasil, é comum já termos nos deparado com ela, através da Associação Brasileira de Normas Técnicas (ABNT).

Ainda temos como as principais Normas inerentes a Segurança e Proteção de Dados:

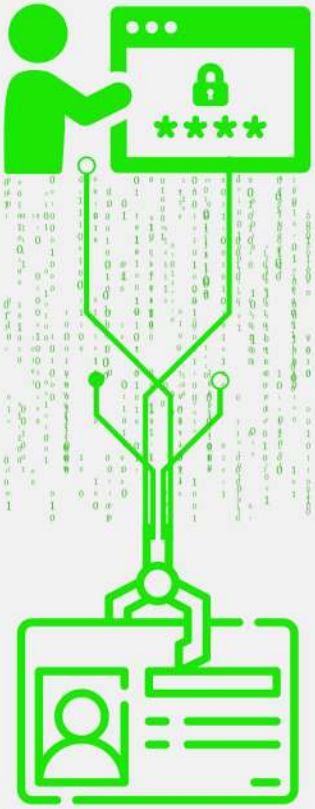
ABNT NBR ISO/IEC 27001:2013. Tecnologia da Informação - Técnicas de Segurança

A norma ABNT NBR ISO/IEC 27001:2013 foi preparada para prover um modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI). Essa norma adota o modelo conhecido como "*Plan-Do-Check-Act*".

3. Normas/Legislações/*Frameworks*

A adoção da norma ISO 27001 serve para que as organizações adotem por um modelo adequado de estabelecimento, implementação, operação, monitoramento, revisão e gestão de um Sistema de Gestão de Segurança da Informação.

A especificação e a implementação do SGSI de uma organização é influenciada pelas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização.



ABNT NBR ISO/IEC 27005:2011. Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

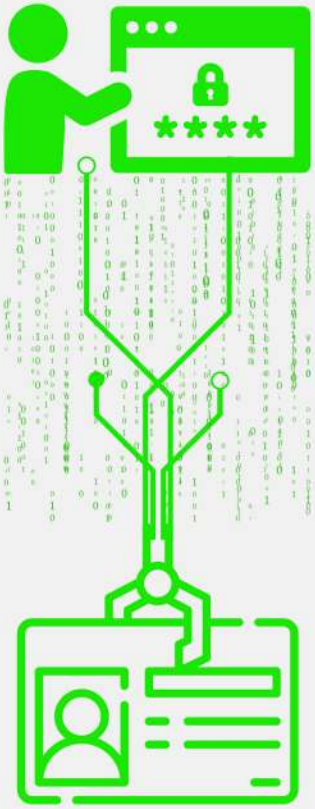
O foco principal da ISO/IEC 27005:2011 diretrizes para o processo de gestão de riscos de SI de uma organização. Direciona-se particularmente aos requisitos de um sistema de gestão de segurança da informação (SGSI). Não inclui um método específico para a gestão de riscos.

A organização irá definir sua conduta ao processo de gestão de riscos, atribuindo em conta, o modelo do seu SGSI, contexto da gestão de riscos e o seu ramo de atividade econômica.

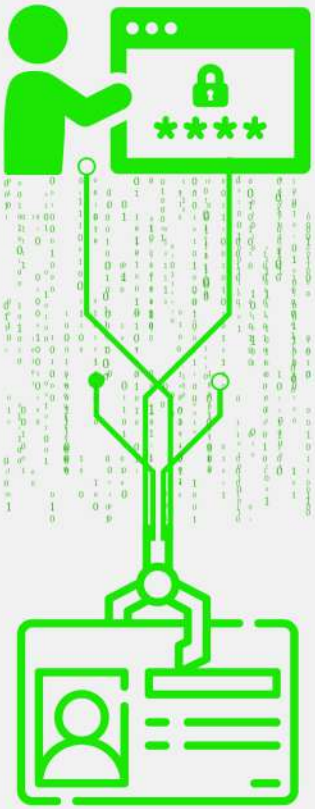
3. Normas/Legislações/*Frameworks*

Principais contribuições:

1. A identificação de riscos;
2. O processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência;
3. A comunicação e entendimento da probabilidade e das consequências destes riscos;
4. O estabelecimento da ordem prioritária para tratamento do risco;
5. A priorização das ações para reduzir a ocorrência dos riscos;
6. O envolvimento das partes interessadas quando as decisões de gestão de riscos são tomadas e para que elas sejam mantidas informadas sobre a situação da gestão de riscos;
7. A eficácia do monitoramento do tratamento de riscos;
8. O monitoramento e análise crítica periódica dos riscos e do processo de gestão de riscos;
9. A coleta de informações de forma a melhorar a abordagem da gestão de riscos e o treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los.



3. Normas/Legislações/*Frameworks*



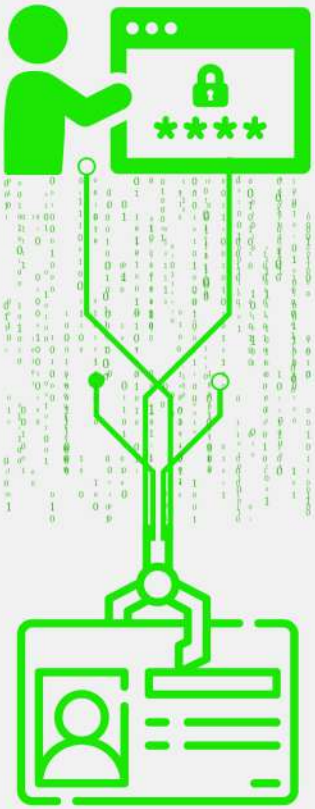
ABNT NBR ISO/IEC 27701:2019. Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001

A Norma ISO/IEC 27701 é uma extensão da norma de segurança da informação, a ISO/IEC 27001, para privacidade.

Com o advento da GDPR, que influenciou a criação da LGPD, os países do bloco Europeu, recomendaram para ISO (Organização Internacional de Normatização ou *International Organization for Standardization*) a criação de uma norma com o fito de complementar a Legislação que viesse a proteger os dados, originando, portanto, a ISO/IEC 27701.

Em 2019, essa norma foi adotada pela ABNT, que publicou a ABNT NBR ISSO/IEC 2770:2019 para gestão da privacidade da informação contendo requisitos e diretrizes para um sistema de gestão de segurança da informação e privacidade (SGPI).

3. Normas/Legislações/*Frameworks*

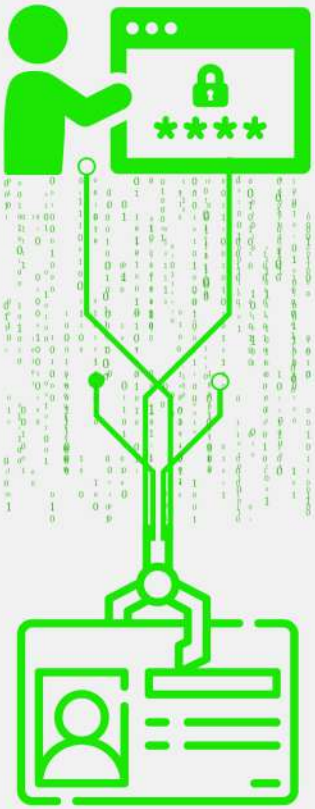


ABNT NBR ISO/IEC 27002:2013 para gestão da privacidade da informação — Requisitos e diretrizes.

O foco principal da ISO 27002 é estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados nas organizações.

A parte principal da norma se encontra distribuída por seções na norma, que correspondem a controles de segurança da informação. Vale lembrar que a organização pode utilizar essas diretrizes como base para o desenvolvimento do SGSI.

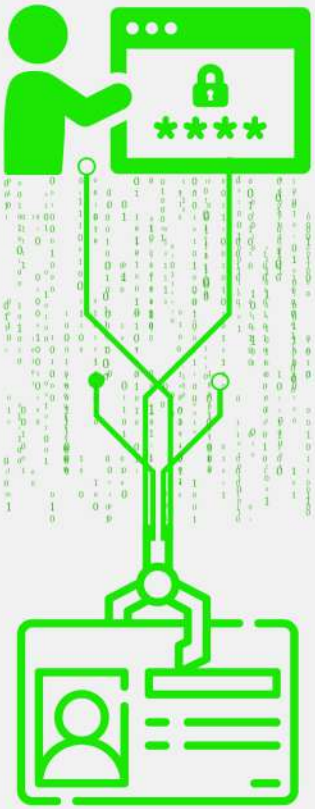
3. Normas/Legislações/*Frameworks*



ABNT NBR ISO/IEC 27002:2013 para gestão da privacidade da informação – Requisitos e diretrizes.

A norma NBR ABNT ISO/IEC 27002:2013 reforça a necessidade de uma política de *backup*. É importante que esta política, resguardando quando necessário o sigilo de informações sensíveis, seja amplamente divulgada e conhecida na organização. A definição dos requisitos de proteção e retenção passa pela avaliação da criticidade da informação para organização e deverá ser detalhada a ponto de propiciar que sejam definidos os recursos tecnológicos mais apropriados para a geração das cópias de segurança. Definições primárias e importantes serão estabelecidas tais como: o que deverá ser protegido; qual o volume de dados a ser protegido; qual crescimento estimado do volume de dados; caso exista criticidade diferenciada para sistemas ou informações distintas qual será o intervalo mínimo de realização de cópia de segurança aceitável para cada um deles, baseando-se na continuidade do negócio. (Monografia Renato Amabile).

3. Normas/Legislações/*Frameworks*



ABNT NBR ISO/IEC 29134:2017. *Information technology – Security techniques – Guidelines for privacy impact assessment.*

Tecnologia da informação — Técnicas de segurança — Diretrizes para avaliação do impacto na privacidade. A ISO/IEC 29134:2017 fornece diretrizes para um processo sobre avaliações de impacto na privacidade, e uma estrutura e conteúdo de um relatório *Privacy Impact Assessment* (PIA).

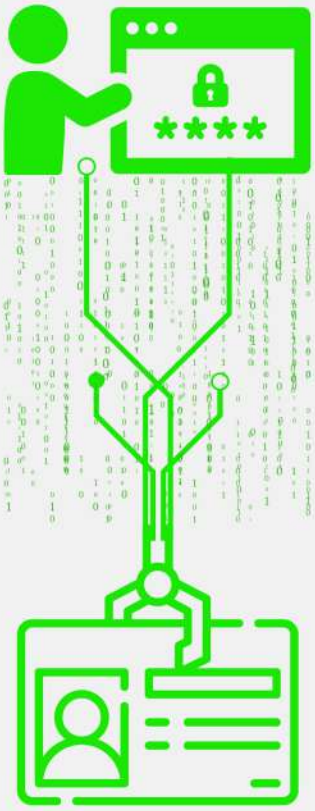
É aplicável a todos os tipos e tamanhos de organizações, incluindo empresas públicas, empresas privadas, entidades governamentais e organizações sem fins lucrativos.

A ISO/IEC 29134:2017 é relevante para aqueles envolvidos na concepção ou implementação de projetos, incluindo as partes que operam sistemas de processamento de dados e serviços que processam *Personally Identifiable Information* (PII).

ABNT NBR ISO/IEC 29151:2017. *Information technology – Security techniques – Code of practice for personally identifiable information protection.*

A norma ABNT NBR ISO/IEC 29151 – Código de prática para proteção de dados pessoais, fornece boas práticas para a proteção de tais dados.

3. Normas/Legislações/*Frameworks*

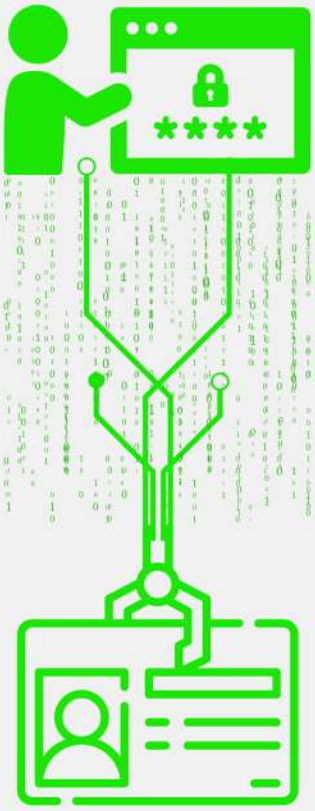


Estabelecendo objetivos de controle, controles e diretrizes para implementação de controles, para atender aos requisitos identificados por uma avaliação de risco e impacto relacionado à proteção de informações de identificação pessoal (PII). Em particular, esta recomendação.
A Norma Internacional especifica diretrizes baseadas na ISO/IEC 27002, levando em consideração os requisitos para o processamento de PII que podem ser aplicáveis no contexto do(s) ambiente(s) de risco de segurança da informação de uma organização.

ABNT NBR ISO/IEC 29151:2017. *Information technology – Security techniques – Code of practice for personally identifiable information* protection.

A ISO/IEC 29151:2017 é aplicável a todos os tipos e tamanhos de organizações que atuam como controladores de PII (conforme definido na ISO/IEC 29100), incluindo empresas públicas e privadas, entidades governamentais e organizações sem fins lucrativos que processam PII.
Os exemplos incluem estruturas de governança propostas para empresas que têm colaboradores que lidam com dados pessoais, combinadas com sugestões de colaboração eficiente com equipes jurídicas para interpretar leis e regulamentos relevantes.

3. Normas/Legislações/*Frameworks*



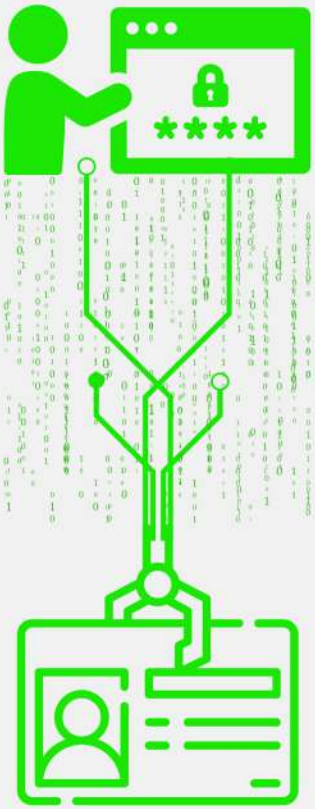
ABNT NBR ISO/IEC 31000:2018. Gestão de riscos - Diretrizes.

A primeira edição da norma brasileira de gestão de riscos – ABNT NBR 31000/2009 foi lançada, em 30/11/2009, entrando em vigor a partir de 30/12/2009. A versão brasileira tem as mesmas premissas e orientações da ISO americana. A ISO 31000 que a ABNT – Associação Brasileira de Normas. Técnicas aprovou para uso no Brasil foi baseada na norma AS/ NZS 4360, norma de gestão de risco utilizada na Austrália e na Nova Zelândia.

Em 30/11/2009 a ABNT publicou a ABNT ISO GUIA 73, que substitui a ABNT ISO/IEC GUIA 73/2005, que foi revisada. O Guia 73/2009 traz o vocabulário básico para podermos entender e falarmos a mesma língua em relação à gestão de risco.

Vale salientar que a ABNT, menciona que as Normas Brasileiras são desenvolvidas e utilizadas voluntariamente e deve se tornar obrigatória, tão somente quando explicitadas em um instrumento do Poder Público (lei, decreto, portaria, normativa etc.) ou havendo exigência contratual ou em normativa licitatória.

3. Normas/Legislações/*Frameworks*



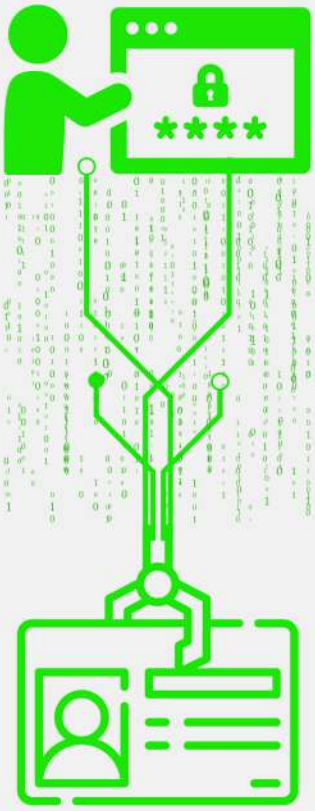
Ela apresenta uma estrutura para a gestão de risco, fornece uma abordagem comum em apoio às demais normas, sem substituí-las.

Nesse sentido, a ISO 31000 não é obrigatória, porém será referência para os gestores e tenderá a unificar a linguagem, os conceitos e estrutura de uma gestão de risco, portanto seu conhecimento e aplicação serão impostos pela própria comunidade da segurança que agora tem uma referência internacional de gestão de riscos.

Em 01 de dezembro de 2009, entrou em vigor a norma ISO/IEC 31010:2009 "*Risk management – Risk assessment techniques*" ou Gestão de riscos – Técnicas de avaliação de riscos, que fornece orientação sobre a seleção e aplicação de técnicas sistemáticas de avaliação de riscos, extremamente importante para manter e estabelecer a proteção e segurança de dados.

É uma norma genérica de gestão de riscos e todas as referências à segurança que existem no documento são de natureza informativa e ainda não tem previsão para publicação, pela ABNT no Brasil.

3. Normas/Legislações/*Frameworks*



ABNT NBR ISO/IEC 38500:2022

Seguramente nem a LGPD e nem a Autoridade Nacional de Proteção de Dados (ANPD) dirão como criar uma governança organizacional, nem tão pouco uma Governança TI. Nesse aspecto, a norma ABNT NBR ISO/IEC 38500:2018 – Tecnologia da informação – Governança da TI para a organização pode auxiliar as empresas a implementarem suas governanças.

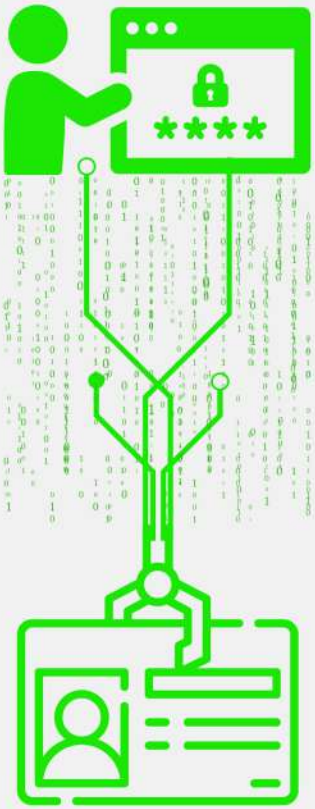
Esta Norma fornece princípios orientativos para os membros das estruturas de governança das organizações (que podem incluir proprietários, diretores, parceiros, gerentes executivos ou similares) sobre o uso efetivo, eficiente e aceitável de tecnologia da informação (TI) dentro de suas organizações. Sendo utilizada na avaliação, direção e monitoramento do uso da Tecnologia da informação de uma empresa.

Segundo a ABNT – Associação Brasileira de Normas Técnicas, a referida norma se baseia em 6 (seis) princípios: **a**) responsabilidade; **b**) estratégia; **c**) aquisições; **d**) desempenho; **e**) conformidade; e, **f**) comportamento humano.

Sumário

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

4. Controles de Segurança



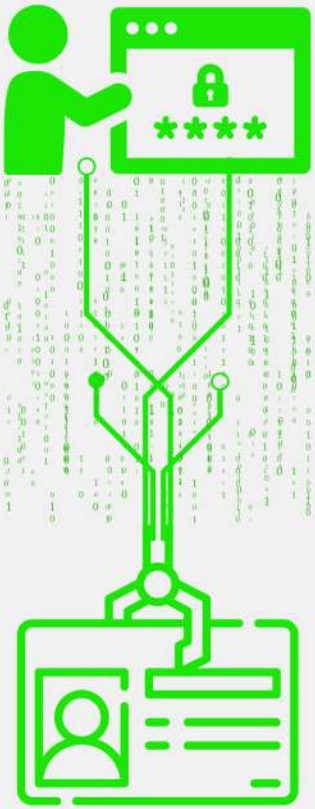
A ISO/IEC 27001:2013 é o padrão oficial de segurança da informação para organizações e infelizmente não está disponível gratuitamente.

4.1 Breve descrição da ISO 27001

Existem pelo menos duas versões da ISO/IEC 27001. As versões de 2005 e 2013. Ambas as versões são bastante semelhantes, com algumas pequenas diferenças, com base nas mudanças de opinião dos especialistas entre 2005 e 2013. A última versão de 2013 abrange os seguintes tópicos (números dos capítulos entre colchetes):

- O contexto organizacional (4)
- Envolvimento da liderança (5)
- Planejamento e objetivos (6)
- Suporte incluindo recursos e comunicação (7)
- Aspectos operacionais (8)
- Avaliação de desempenho (9)
- Melhoria contínua (10)

4. Controles de Segurança



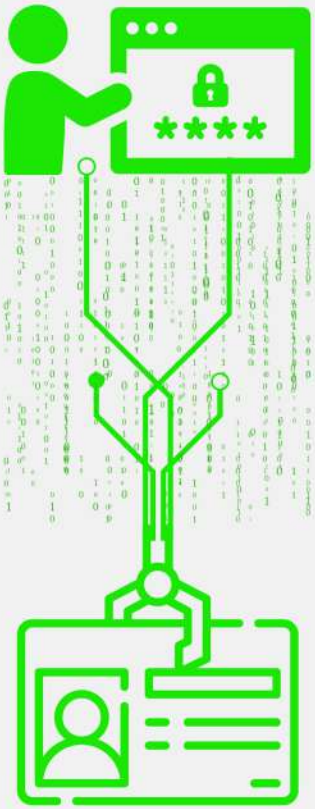
Cada um desses tópicos descreve uma parte de um sistema de gerenciamento de segurança da informação ou ISMS. A norma ISO 27001 visa atingir um nível mais alto de metas para garantir que as organizações estejam estruturadas, chamado de sistema de gestão na linguagem ISO que aumenta a segurança das informações de uma organização. Este ISMS não é um sistema de TI, mas uma descrição dos processos em sua organização. Incluiu objetivos, recursos, políticas e descrições de processos.

4.2 Os 14 domínios da ISO 27001

Políticas de Segurança da Informação - Este domínio afirma que as organizações devem documentar e atualizar suas políticas em seu ISMS. Para estar em conformidade, certifique-se de que sua organização revise e documente seus procedimentos.

Organização de Segurança da Informação - este domínio define como as responsabilidades são atribuídas em sua organização, ou seja, quem faz o quê e quando. Para ser consistente, certifique-se de que sua estrutura organizacional esteja escrita, com uma indicação clara de funções e responsabilidades.

4. Controles de Segurança

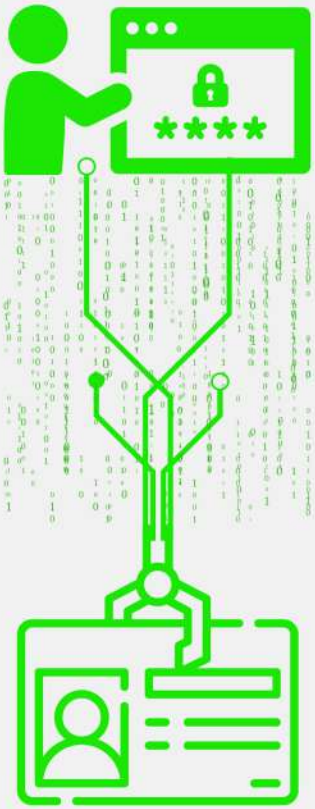


Segurança do funcionário - aborda como os funcionários precisam ser informados sobre segurança cibernética quando iniciam um emprego, deixam um emprego ou mudam de emprego dentro de uma organização. Para garantir a conformidade, os procedimentos de segurança para informações breves durante o embarque e descomissionamento precisam ser registrados pela organização.

Gerenciamento de ativos - descreve as etapas necessárias para gerenciar ativos de dados e como eles precisam ser protegidos. No caso de uma auditoria de certificação, o processo de sua organização para rastrear o *hardware*, *software* e bancos de dados de sua organização será testado, portanto, você pode ser solicitado a demonstrar seus métodos para proteger a integridade de seus ativos de dados.

Controle de acesso - orienta como uma organização deve controlar o acesso dos funcionários aos dados, dependendo do cargo e da situação. Para estar em conformidade, a organização deve definir claramente como os direitos de acesso são definidos e quem é o responsável.

4. Controles de Segurança



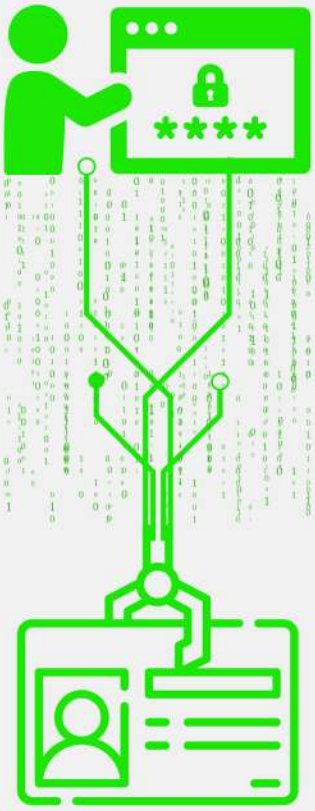
Criptografia - Este *site* abrange as práticas recomendadas em torno da criptografia. No estudo de caso, será analisado como cada sistema que transporta dados sensíveis é criptografado, incluindo o tipo de criptografia utilizado.

Segurança Ambiental e Ambiental - aborda como uma organização deve proteger edifícios e ativos internos. Para garantir que sua organização esteja em conformidade, os riscos de segurança em seu ambiente de negócios devem ser eliminados.

Segurança Operacional - Descreve as melhores práticas para coleta e armazenamento de dados. Para conformidade, certifique-se de que os fluxos de dados e onde os dados são armazenados possam ser comprovados durante uma auditoria.

Segurança das Comunicações - cobre a segurança das informações transmitidas dentro da rede de uma organização. Para garantir que sua organização seja compatível com esse domínio, a segurança dos sistemas de comunicação, como *e-mail* e videoconferência, precisa ser testada.

4. Controles de Segurança



Aquisição e Manutenção do Sistema - detalhes de como os sistemas novos e existentes introduzidos nas operações da organização serão gerenciados. Para garantir a conformidade, todos os sistemas precisam ser mantidos no mais alto nível de segurança da informação.

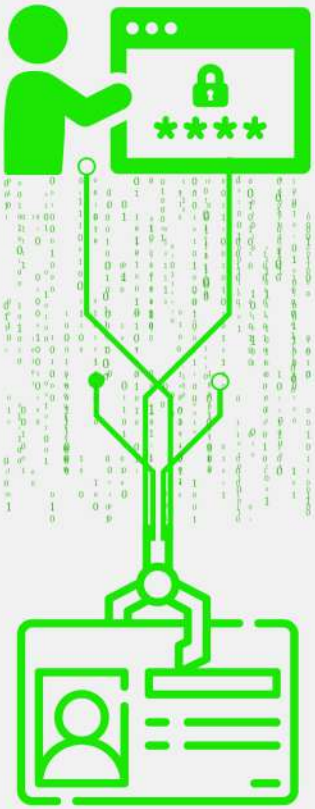
Relacionamento com o Fornecedor - analisa como uma organização deve garantir a segurança de informações/dados confidenciais ao trabalhar com um fornecedor terceirizado. Em caso de auditoria, os contratos e quaisquer terceiros com acesso a esses dados serão auditados.

Gerenciamento de Incidentes de Segurança - este domínio abrange como uma organização deve lidar com questões de segurança. No caso de uma auditoria, a resposta e o gerenciamento de incidentes serão revisados.

Gerenciamento de Continuidade de Negócios - trata de como as interrupções nos negócios e as principais mudanças devem ser tratadas. Os auditores apresentam uma série de etapas de consideração para avaliar se o SGSI inclui as etapas a seguir.

Conformidade - Identifica as regulamentações governamentais ou do setor relevantes que se aplicam à sua organização.

4. Controles de Segurança



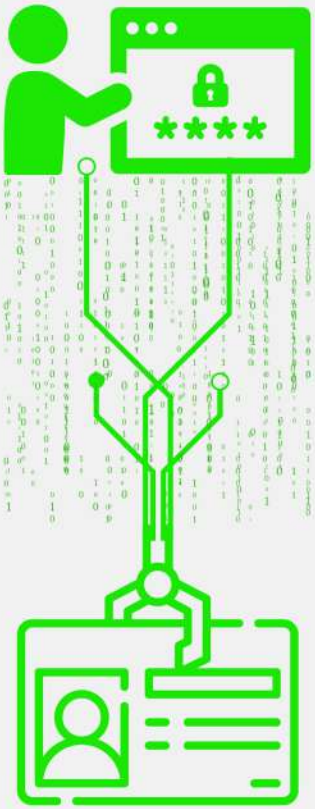
4.3 Como a ISO 27001 resolve os desafios organizacionais?

Dada a ampla gama de domínios cobertos pela norma ISO 27001, o processo de certificação resolve alguns dos maiores desafios que seu negócio enfrenta:

1. Sua organização não conhece seus ativos de informação - Um problema comum entre as organizações é que elas não veem quais informações e dados estão atualmente armazenados em seus sistemas. A ISO 27001 pode ajudar a identificar ativos de informação e protegê-los, o que pode levar ao aumento de seu valor de mercado potencial.

2. Os sistemas de informação de sua organização podem ser desorganizados ou subdesenvolvidos - O objetivo da ISO 27001 é manter seu Sistema de Gestão de Informação atualizado. O gerenciamento eficaz de informações pode aumentar a facilidade de uso e ajudar os funcionários a trabalhar com eficiência, obter sua certificação ISO ISMS é um passo para conseguir isso.

4. Controles de Segurança

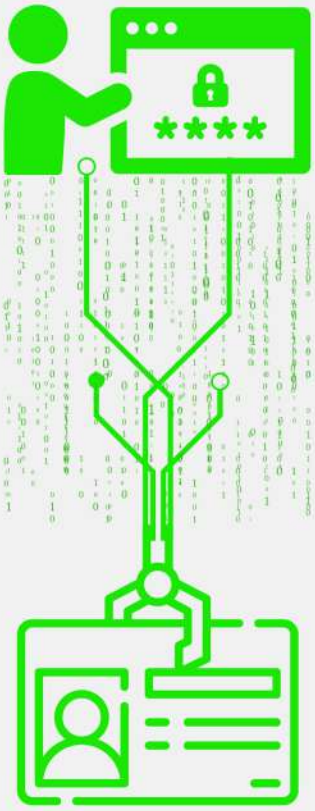


3. Sua organização pode não estar ciente dos riscos que enfrenta - Existem 3 (três) tipos de organizações, organizações que sabem que foram violadas, aquelas que não sabem de uma violação de segurança e aquelas que sabem que não foram violadas. Arriscada se sua organização se enquadra na segunda categoria, a ISO 27001 pode capacitar sua organização a identificar riscos conhecidos e desconhecidos e evitá-los antes que causem danos à sua reputação ou finanças.

4. Sua organização pode perder clientes e receita adicional - Obter e manter a certificação ISO 27001 para seu SGSI pode ajudar não apenas a atrair clientes, mas também a tranquilizar seus clientes atuais quanto ao seu compromisso com a proteção de informações e dados confidenciais. Ao garantir seus clientes, você também garante que sua organização não perca receita adicional.

5. Sua organização pode estar perdendo tempo com auditorias repetidas - Obtendo seu ISMS aprovado, a certificação ISO 27001 ajuda sua organização a ser reconhecida globalmente como segura, eliminando a necessidade de seus clientes auditarem sua organização.

4. Controles de Segurança



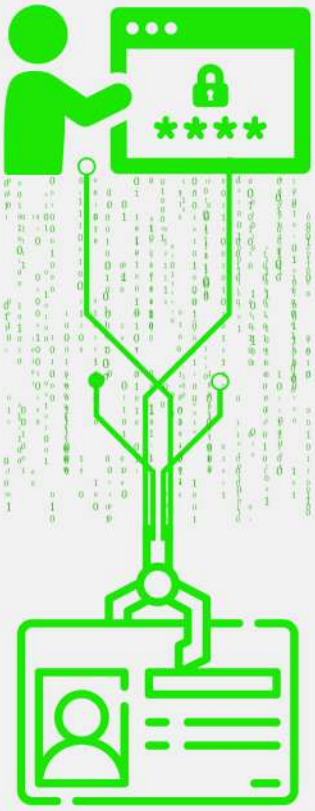
6. Preenchendo um Questionário de Segurança do Cliente - Uma vez que você esteja em conformidade com a ISO e/ou certificado, a capacidade de preencher um questionário de segurança é muito mais fácil.

Sumário

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

5. Governança da Segurança da Informação

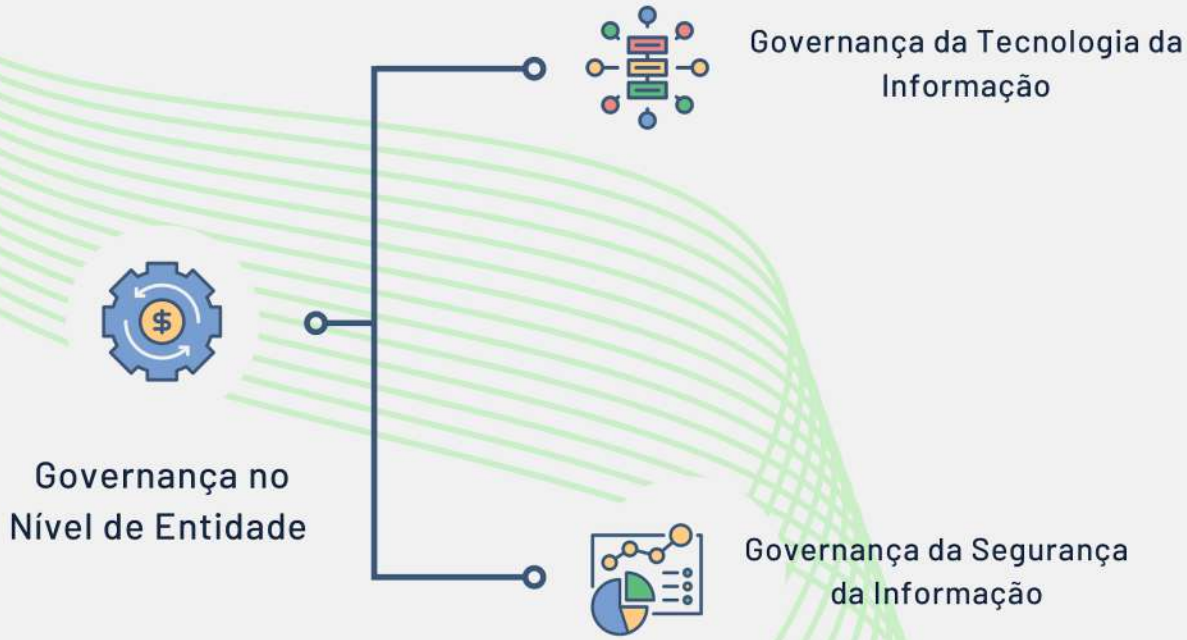
5.1 Conceito de Governança da Segurança da Informação



A governança da segurança da informação, apresentada na ABNT NBR ISO/IEC 27014 de 2013 e atualizada em 2021, funciona como um sistema de controle, sendo o conjunto de ações, políticas e regras que espelham o comportamento de uma organização quanto à segurança das informações.

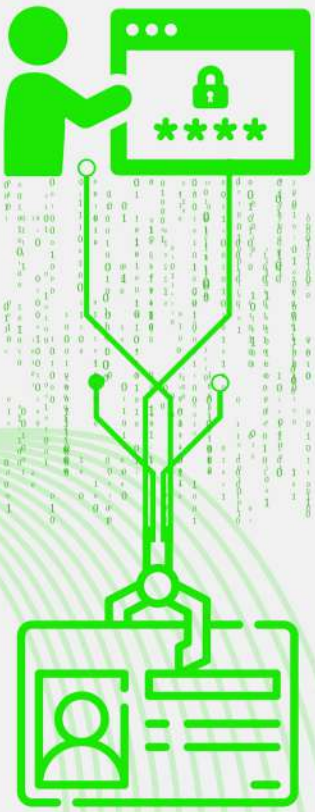
Nesse sentido, a governança, conforme preceitua a norma mencionada "é o meio pelo qual o órgão diretivo de uma organização fornece orientação geral e controle das atividades que afetam a segurança das informações de uma organização." (ABNT, 2021, p. 3). Importante destacar, a diferença entre governança da tecnologia da informação e segurança da informação, enquanto a primeira busca os recursos necessários para adquirir, processar, guardar e disseminar informação, a segunda abrange confidencialidade, integridade e disponibilidade da informação.

5. Governança da Segurança da Informação



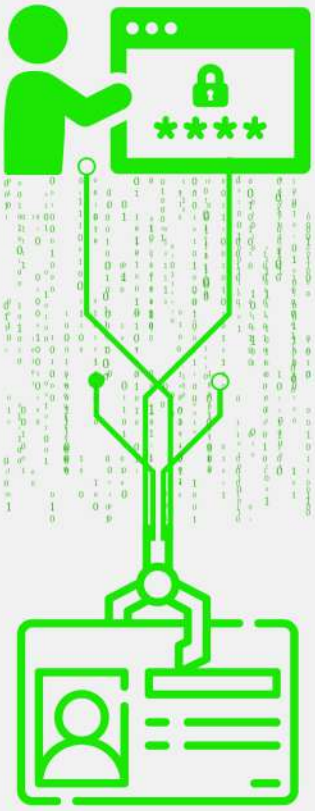
Representação de Figura Ilustrativa ISO/IEC 27014 (ABNT, 2021, p. 14)

As diretivas utilizadas são fundamentadas no fato de que riscos à segurança podem prejudicar a organização quanto às metas, finalidades e objetivos, considerando as possibilidades de uma ameaça explorar vulnerabilidades, comprometendo a confidencialidade, integridade e disponibilidade das informações. Desta forma, a governança tem por finalidade definir as ações para a validação da segurança da informação e verificar se as normas e políticas estão sendo seguidas corretamente.



5. Governança da Segurança da Informação

5.2 Termos e Definições



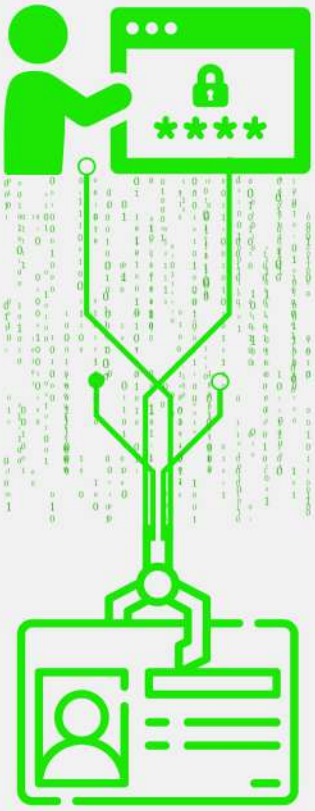
A ISO/IEC 27014:2021, destaca os seguintes termos: entidade, organização, órgão diretivo e alta direção.

Entidade e organização são por vezes utilizadas como sinônimos, quando se trata de empresas menores, a definição pela norma daquela é “organização e outros órgãos ou partes”, enquanto essa “parte de uma entidade que executa e gerencia um Sistema de Segurança de Informação (SGSI)”. Nota-se que enquanto a entidade retrata a instituição como um todo, organização se restringe aos responsáveis pelo SGSI.

Enquanto Alta Direção é a “pessoa ou grupo de pessoas que dirige e controla uma organização no mais alto nível”, órgão diretivo é a “pessoa ou grupo de pessoas responsáveis pelo desempenho e pela conformidade da entidade”.

5.3 Objetivos da Governança da Segurança da Informação

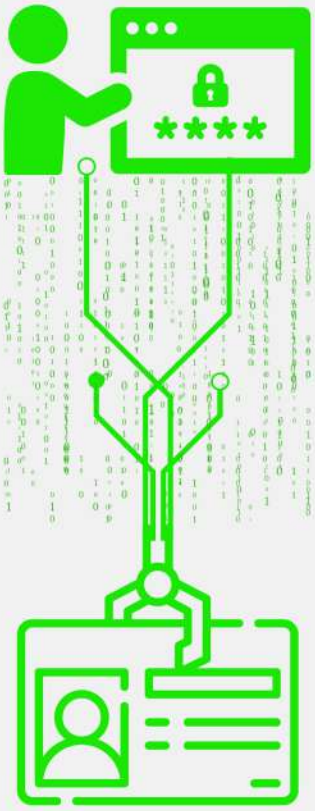
5. Governança da Segurança da Informação



Sempre que se fala no conceito de governança, busca-se integrar a conformidade pretendida em todas as camadas da entidade. Desta forma, o primeiro objetivo a ser destacado é o da necessidade de se estabelecer uma segurança da informação abrangente e integrada em toda a entidade. Com isso a segurança da informação precisa ser tratada conforme as prioridades da organização e de acordo com as medidas do (s) Sistema de Segurança de Informação (SGSI)s da organização e com acompanhamento de ponta a ponta.

Outro objetivo é tomar decisões usando uma abordagem baseada em risco, isso porque a governança em segurança da informação deve unificar o *Compliance* face aos riscos da não conformidade, já que os recursos alocados para esse mecanismo de controle, com políticas e regras, serão pautados considerando a necessidade tecnológica, o grau de maturidade e o apetite de risco da entidade, face às obrigações legais, critérios operacionais, de reputação e de imagem, risco financeiro, dentre outros.

5. Governança da Segurança da Informação

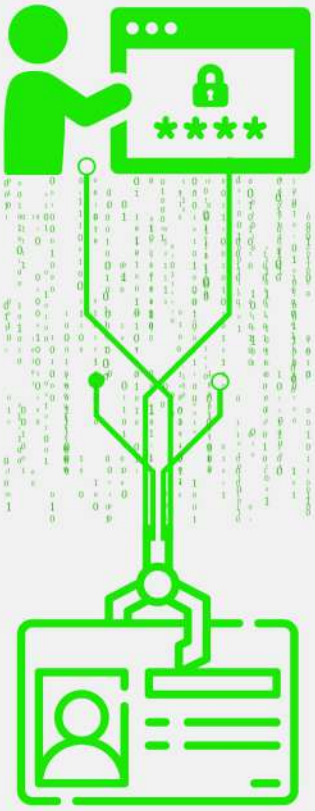


Observa-se então, a necessidade de se definir o direcionamento de aquisições, para que os investimentos estejam alinhados com a abordagem definida. Faz-se necessário que a Alta Direção de cada SGSI possua uma estratégia de segurança da informação fundamentada nos objetivos organizacionais, para possibilitar integração entre os requisitos da entidade e os requisitos de segurança da informação.

No mais, a governança da segurança da informação deve assegurar a conformidade com os requisitos internos e externos, quanto à legislação e regulamentação vigente, bem como requisitos contratuais e compromissos internos. Indica-se a prática de auditorias independentes para validação contínua dos processos implementados.

Como próximo objetivo, destaca-se a necessidade de se promover uma cultura positiva de segurança, trazendo correta orientação sobre as políticas e regras, com treinamentos e *workshops*, já que o comportamento humano é fator fundamental parasse alcançar um nível adequado de segurança da informação.

5. Governança da Segurança da Informação

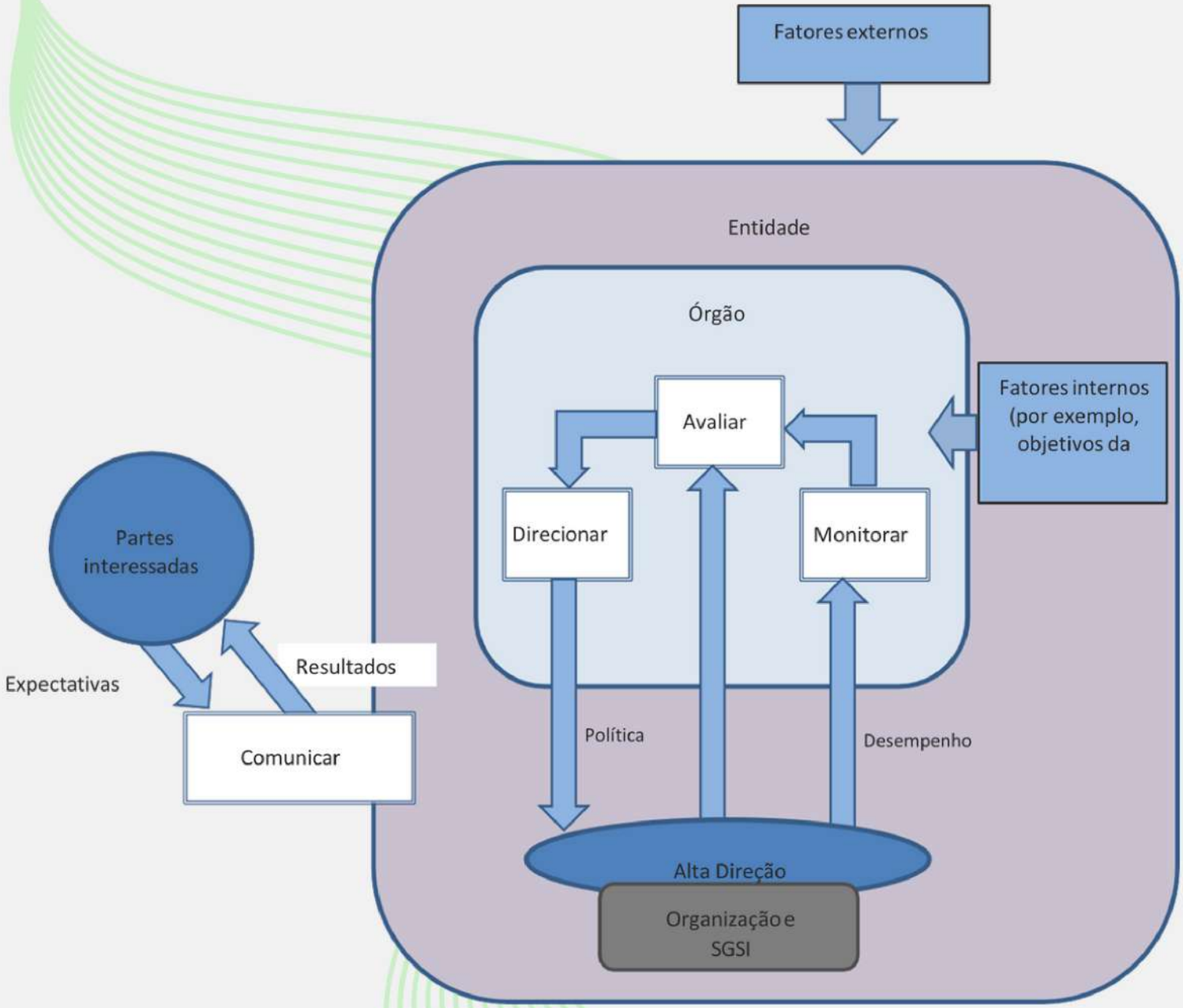


Por último, assegurar que o desempenho da segurança atenda aos requisitos atuais e futuros da entidade é fundamental, uma vez que a governança da segurança da informação funciona como mecanismo de controle, convém que esta se certifique que as condutas adotadas no contexto de segurança estejam de acordo com os objetivos da instituição, para tanto, orienta-se à Alta Direção, para que possua programa de medição de desempenho para cada SGSI, com a finalidade de monitorar, auditar e identificar oportunidades de melhoria.

5.4 Dos Processos

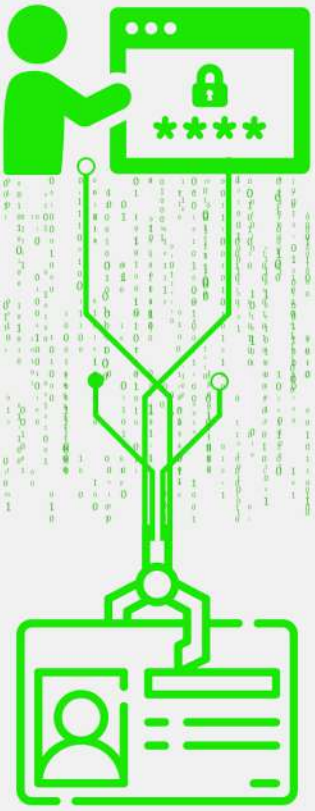
Os processos realizados pelo órgão diretivo dentro de uma entidade são os detalhados na figura em que se destacam o contexto de “avaliar”, “direcionar”, “monitorar” e “comunicar”, (ABNT, 2021, p. 8):

5. Governança da Segurança da Informação



"Avaliar" consiste na análise atual do cenário e previsão de mudanças e melhorias, buscando alcançar os objetivos estratégicos, considerando: os riscos e as oportunidades pertinentes, as medições verificadas em relatórios da informação e do SGSI, apoio e sustação dos objetivos da entidade e correta aprovação do órgão diretivo dos projetos juntamente com a verificação do impacto de cada projeto.

5. Governança da Segurança da Informação

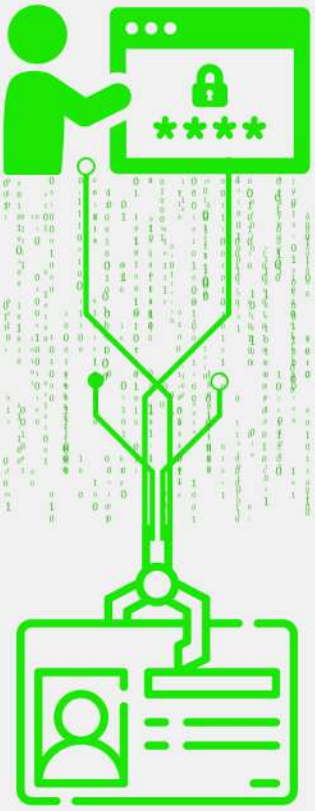


Já, “Direcionar” está para orientação, em que tanto o órgão diretivo, como a Alta Direção possuem papéis fundamentais. Enquanto o primeiro deve estabelecer a direção estratégica geral e os objetivos da entidade juntamente com a definição do apetite de risco e a estratégia de segurança, esse último deve se comprometer em alocar recursos, funções, responsabilidades e prover políticas que sustentem o órgão diretivo.

De outro lado “Monitorar” destaca a avaliação do cumprimento dos objetivos estratégicos, quando o órgão diretivo recebe relatórios sobre a operação de cada SGSI, e os avalia no contexto das prioridades da entidade, assim como repassa informações à Alta Direção sobre o tema. No mais a Alta Direção deve verificar a execução das tarefas da gestão da segurança da informação quanto à eficácia para que os processos estejam alinhados com as necessidades da entidade.

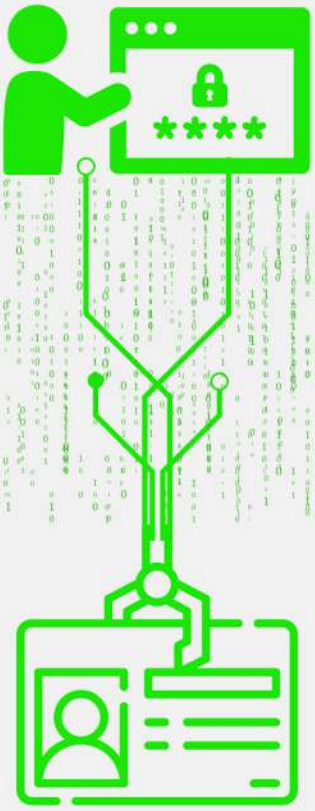
5. Governança da Segurança da Informação

Como último pilar processual, o estágio de “Comunicar”, em que há troca de informações entre o órgão diretivo e as partes interessadas no intuito de validar as necessidades entre eles. Processo extremamente importante e vinculado ao cumprimento dos objetivos da governança da segurança da informação, isso porque é por meio desse estágio que o órgão diretivo relata aos demais setores sobre as políticas de segurança da entidade, nível de maturidade e compatibilidade com a natureza de sua atividade, assim como detalha as obrigações que identificou dentro do escopo regulatório e normativo, para fins de priorização e conformidade dentro do contexto de segurança da informação, em especial para atenção da Alta Direção, destaca questões referente à cultura positiva quanto à segurança da informação, tais como palestras, eventos e treinamentos.



5. Governança da Segurança da Informação

5.5 Do órgão diretivo e do SGSI



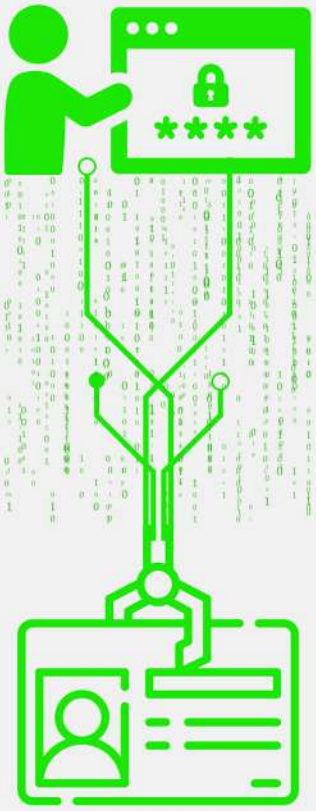
O órgão diretivo deve requerer a elaboração do planejamento de um ou mais SGSI para apoiar a entidade, de acordo com as políticas e os processos gerais da entidade, incluindo a gestão de riscos.

Um SGSI pode adotar o mesmo processo de avaliação de riscos que o órgão diretivo, seguindo, preferencialmente, o padrão ABNT NBR ISO/IEC 27001.

Caso sejam adotados padrões diferentes, a abordagem de avaliação, para fins de conformidade, deverá ser ajustada para viabilizar a análise.

É de responsabilidade do órgão diretivo aprovar a criação de cada SGSI, juntamente com o escopo, certificações objetivos, requisitos, funções e recursos, além de manifestar-se referente à matriz de riscos e quanto aos canais de comunicação, para que o SGSI pode entregar para a entidade os riscos e a eficácia de cada sistema.

5. Governança da Segurança da Informação

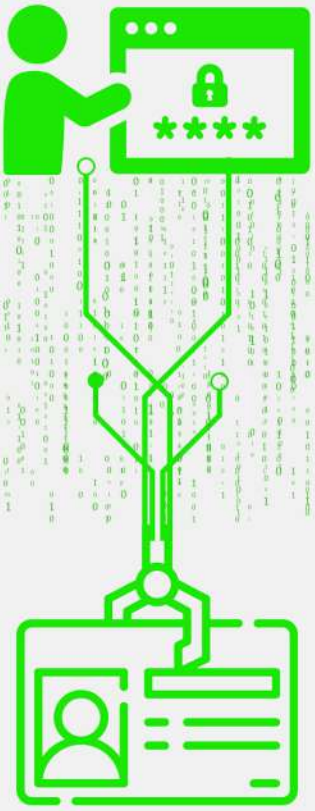


A relação entre SGSI e a entidade fica estruturada em 03 (três) possíveis cenários: Tipo A: A organização do SGSI é toda a entidade, Tipo B: A organização do SGSI faz parte de uma entidade maior, e, Tipo C: A organização do SGSI inclui partes de algumas entidades.

No cenário Tipo A, existe um sistema de gestão de acordo com a ABNT NBR ISO/IEC 27001 para fornecer informações referente a segurança da informação, nesse sentido, o direcionamento quanto aos objetivos da segurança da informação com os objetivos gerais da entidade se demonstra mais simples, já que a Alta Direção será a responsável pela determinação de todo conteúdo.

Outrossim, há manutenção dos quatro processos apresentados e vale destacar a necessidade de regras bem definidas para assegurar que as responsabilizações pelas tarefas de governança e direção sejam adequadamente separadas uma da outra, uma vez que é comum a mesma função assumir ambas as responsabilidades.

5. Governança da Segurança da Informação

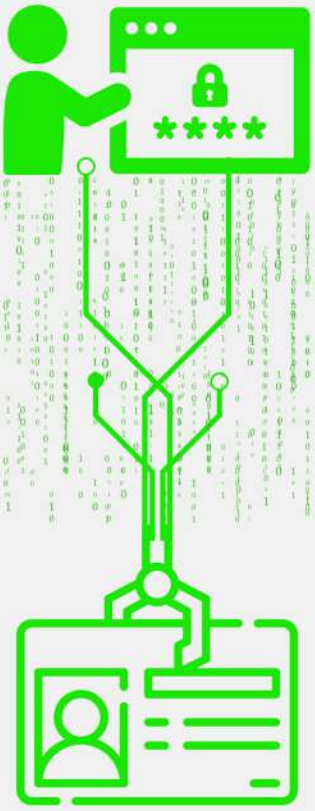


No cenário Tipo B, em que algumas organizações do SGSI são partes de uma entidade maior, verifica-se que uma organização pode ter múltiplos SGSI e o órgão diretivo também pode orientar diversos SGSI e a Alta Direção de cada organização do SGSI e o órgão diretivo da entidade controladora estão relacionados, em que o(s) integrante(s) da Alta Direção e do órgão diretivo podem ser os mesmos, ter integrantes em comum ou não. Nessa formação, os quatro processos de governança são aplicáveis, em que para a relação entre a(s) organização(ões) do SGSI e a entidade controladora, verifica-se uma das opções abaixo:

- Cada organização do SGSI atua como parte autônoma da organização controladora com objetivos próprios e específicos de negócio;
- Cada organização do SGSI tem por finalidade alcançar um ou mais dos objetivos de negócio da entidade controladora;

5. Governança da Segurança da Informação

- Cada organização do SGSI gerencia um aspecto dos riscos de segurança da informação em nome da entidade controladora;



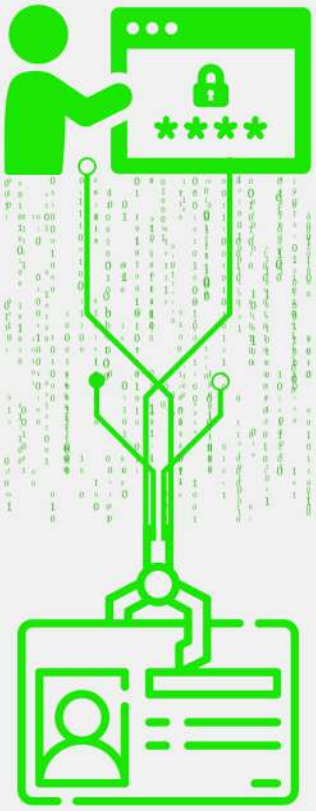
No cenário Tipo C, quando a organização do SGSI inclui partes de algumas entidades, a estrutura do SGSI é direcionada e controlada pela Alta Direção, mas abrange diversas entidades. A situação é comum quando várias entidades buscam alcançar os mesmos objetivos e segurança da informação, considerando os requisitos para um subconjunto de suas atividades.

Os quatro processos de governança são aplicáveis e se torna imprescindível que os objetivos de segurança da informação da organização do SGSI estejam de acordo com os objetivos de negócio mútuos que das entidades-membro.

Sumário

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

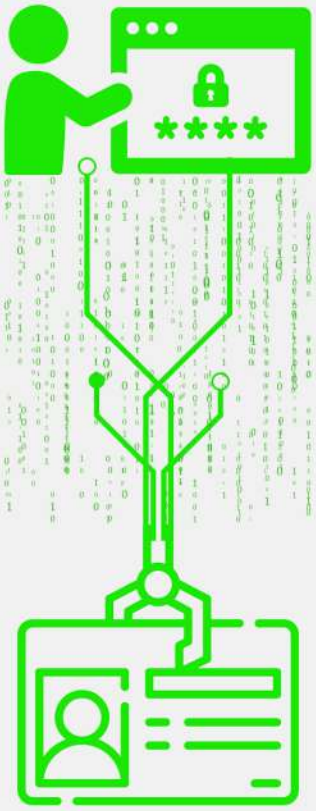
6. Gestão de Riscos em Segurança da Informação



A gestão de riscos em segurança da informação requer atenção especial e olhar crítico. Isso porque quando o assunto é segurança da informação os riscos nem sempre conseguem ser elevados a níveis aceitáveis, pois geralmente os custos podem ser elevadíssimos ou inalcançáveis para algumas organizações, ou, ainda depender de fatores externos alheios as organizações. Como é sabido as organizações de pequeno e médio porte mal conseguem fechar o exercício anual positivo, quiçá fechar com lucros, poucas empresas hoje podem destinar ou destinam recursos para a segurança da informação.

Nesse sentido, a Lei 13.709/2018 Lei Geral de Proteção de Dados Pessoais favoreceu a matéria “segurança da informação” em seus artigos 46 e seguintes passando a exigir medidas mínimas de segurança, técnicas e administrativas. E aqui cabe ressaltar que não será possível analisar os riscos em segurança da informação somente sobre o viés dos dados pessoais, mas, dados e consequente informações como um todo.

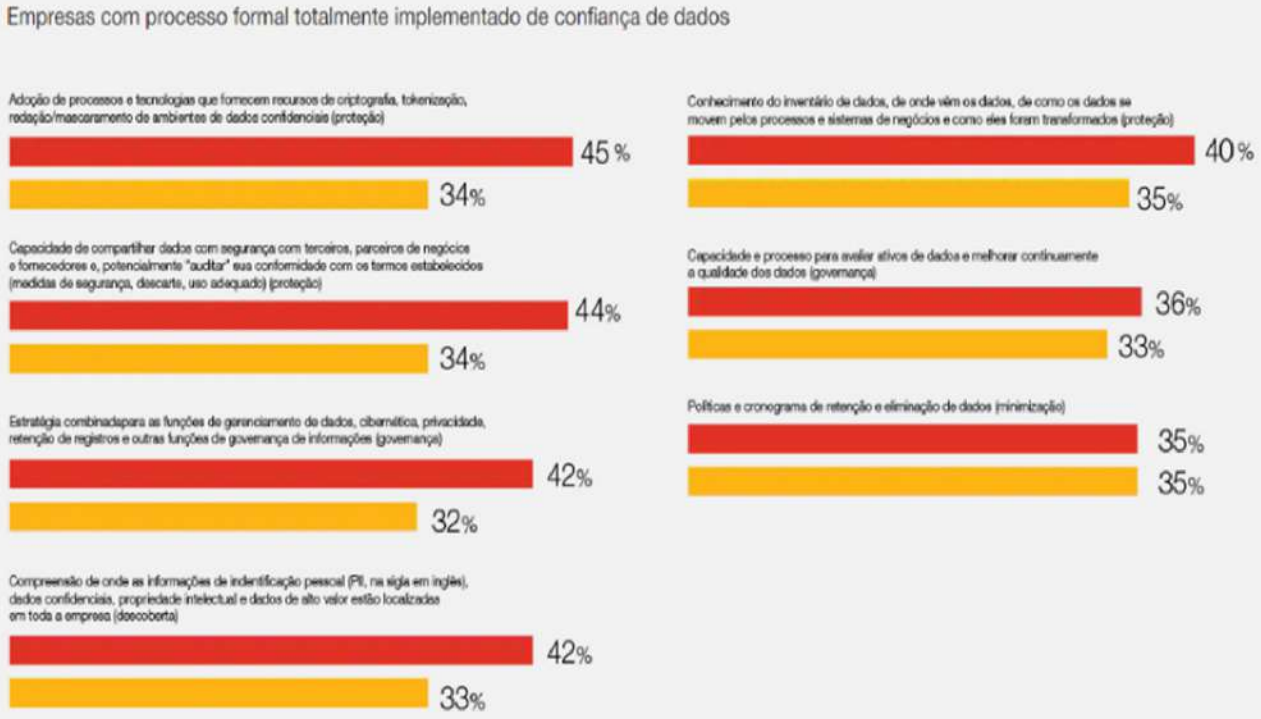
6. Gestão de Riscos em Segurança da Informação



Em pesquisa realizada pela *Global Digital Trust Insights Survey* 2022 apurou que no Brasil 83% organizações preveem um aumento nos gastos cibernéticos em 2022, em comparação com 69% no mundo. Em 2020, esses mesmos índices eram de 55% e 57%, respectivamente, e, 45% dos brasileiros (26% no mundo) preveem aumento de gastos cibernéticos acima de 10%. Disponível em: https://www.pwc.com.br/pt/estudos/servicos/consultoria-negocios/2021/global-digital-trust-insights-survey-2022.html).

Essa mesma pesquisa pergunta qual é a maturidade das práticas de confiança de dados da sua organização, o Brasil está representado pela cor vermelha e o amarelo representa o percentual global, vejamos.

6. Gestão de Riscos em Segurança da Informação



Fonte: *Global Digital Trust Insights Survey* 2022 (pwc.com.br)

O risco é a probabilidade de um agente de ameaça tirar proveito de uma vulnerabilidade e do impacto no negócio correspondente (*Foudations os Information Security*). O risco é o efeito da incerteza, em segurança da informação representa ameaça.

De outra sorte, a vulnerabilidade representa a ausência ou fraqueza de garantia passível de ser explorada como por exemplo, *desktop* sem senha, *e-mails* sem criptografia, portas de *firewall* abertas, antivírus gratuito ou desatualizado, dentre outros.

6. Gestão de Riscos em Segurança da Informação

Portanto, notadamente no Brasil a maturidade diante dos índices são um pouco melhores em alguns pontos em relação aos demais países, seguindo com mesmo percentual, ou seja, único quesito de empate, apenas quanto a “política de minimização e descarte dos dados”.

Em verdade, a temática não só Brasil mas a nível global, tem ganhado novos contornos, seja por imposição legal, seja por exigências de mercado, seja pela cultura da empresa, fato é que o assunto está cada dia mais evidente e preocupante e não há como não fazer nada.

6. Gestão de Riscos em Segurança da Informação

Avaliar riscos diante da aceleração digital e das evoluções mercadológicas não é tarefa fácil e deve ser constante, nesse sentido, órgãos e instituições tem realizado grandes esforços para amenizar os impactos financeiros sofridos pelas organizações e trabalhar de forma mais efetiva na gestão de riscos em segurança da informação.

Riscos podem surgir da incerteza do mercado financeiro, de falhas de projeto, de responsabilidades legais, de riscos de crédito, de acidentes, de causas naturais e desastres, bem como de ataques deliberados de adversários. Diversos padrões de gerenciamento de riscos foram desenvolvidos, incluindo os do *Project Management Institute* (PMI), *National Institute of Science and Tecnology* (NIST) e padões ISO. Métodos, definições e objetivos variam muito - por exemplo, se o método de gerência de riscos se encontra no contexto da gerência de projetos, segurança, engenharia, processos industriais, carteiras financeiras, avaliações atuariais ou segurança e saúde pública.

6. Gestão de Riscos em Segurança da Informação

A estratégia de risco pode incluir transferir risco para outra parte, evitar o risco, reduzir o efeito negativo do risco e aceitar algumas ou todas as consequências de um risco em particular" (*HINTZBERGEN, Jule*. Fundamentos de segurança da informação: com base na ISO 27001 e na 27002).

Isto posto, os riscos são inúmeros e dependem de vários fatores internos e externos além do olhar crítico e da base de conhecimento técnico de quem o realiza. Com base nisso, a norma ISO/IEC 27005:2011 traz recomendações para a gestão de riscos em segurança da informação, dispondo sobre a abordagem da gestão de riscos, os critérios para a avaliação de riscos, critérios de impactos, critérios para aceitação de riscos, escopo e limites etc.

O risco se configura como uma probabilidade e isto pode resultar em impactos positivos e negativos. No entanto, quando se refere à Segurança da Informação, o foco reside nos impactos negativos, principalmente.

6. Gestão de Riscos em Segurança da Informação

Isto porque a identificação dos riscos, assim como sua análise e avaliação são fundamentais para a continuidade de negócio satisfatória. Por essa razão, é recomendável realizar uma gestão de risco em segurança da informação de forma habitual e efetiva.

Para este tipo de gestão, a sistematização e a organização são essenciais para o controle dos riscos, pois não existem sistemas totalmente seguros.

Normas técnicas internacionais podem ajudar nessa tarefa, a exemplo da ISO 27005. Há, igualmente, outras normas que podem auxiliar nesta atividade, como o *NIST Risk Management Framework* (RMF) ou a metodologia OCTAVE. O objetivo, porém, é comum a todas elas: alcançar um grau elevado e adequado de confiabilidade em seus processos e sistemas.

6. Gestão de Riscos em Segurança da Informação

Figura: Risk Management Framework (RMF). Nist.

O *framework* do *NIST* possui uma estrutura de gerenciamento estruturada em sete etapas, podendo ser aplicada em qualquer sistema, novos ou em funcionamento, independentemente do tipo de tecnologia utilizada e em qualquer tipo de entidade, sendo irrelevante o tamanho, dado o nível de abstração que foi desenhado.

Segue as etapas dessa estrutura:

6. Gestão de Riscos em Segurança da Informação

1. PREPARAÇÃO: consiste na preparação da entidade para o gerenciamento de risco. Nesta etapa, é definido o escopo e o contexto da gestão, as responsabilidades e o nível de tolerância a riscos, assim como os critérios pra as demais etapas.

2. CATEGORIZAÇÃO: consiste na classificação e rotulação dos dados e informações em seus três estados: processamento, repouso e em trânsito. Essa classificação deve ser realizada com base na avaliação de impacto.

3. SELEÇÃO: consiste na seleção dos controles de segurança dispostos no *NIST* SP 800-53 com base na avaliação de risco.

4. IMPLEMENTAÇÃO: consiste na implementação dos controles de segurança selecionados, assim como sua documentação.

5. AVALIAÇÃO: consiste em avaliar se tais controles implementados estão em funcionamento e produzindo os efeitos desejados.

6. Gestão de Riscos em Segurança da Informação

6. AUTORIZAÇÃO: consiste na devida autorização a operação do sistema com base em uma decisão fundamentada no risco analisado.

7. MONITORAMENTO: consiste no devido monitoramento dos controles de segurança implementados, assim como nos riscos para todo o sistema.

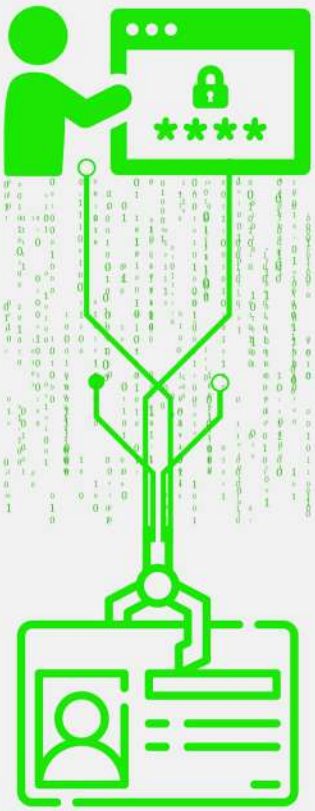
Além do *NIST Risk Management Framework*, o *NIST* também mantém o *CyberSecurity Framework*, que pode auxiliar no aprimoramento da postura de segurança das entidades que fazem seu uso.
O *CyberSecurity Framework* é formado por um conjunto de padrões e diretrizes e está dividido em 5 (cinco) funções principais a seguir:

6. Gestão de Riscos em Segurança da Informação

Figura: *CyberSecurity Framework* - Fonte: *NIST* (S/D)

1. <u>IDENTIFICAÇÃO</u>: o principal objetivo desta função reside no desenvolvimento da compreensão da entidade quanto aos aspectos referentes aos sistemas, ativos, os dados e recursos dela pertencentes. Neste sentido, identificar processos e ativos críticos, documentar fluxos de informação, manter inventário de hardware e software, estabelecer políticas de segurança e identificar as ameaças, vulnerabilidades e riscos que são de vital importância para esta compreensão.

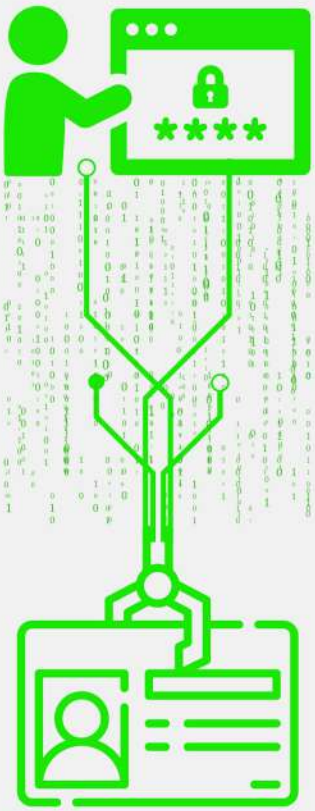
6. Gestão de Riscos em Segurança da Informação



2. PROTEÇÃO: o principal objetivo desta função está no desenvolvimento e implementação das medidas de segurança adequadas para a entidade. Assim, o gerenciamento do acesso a ativos e informação, a proteção de dados confidenciais, a realização de backups, o gerenciamento de vulnerabilidades e o treinamento de usuários formam as atividades basilares para a proteção do sistema.

3. DETECÇÃO: o principal objetivo desta função aponta para o desenvolvimento e a implementação de meios eficientes e adequados para a detecção de ocorrência de eventos de segurança da informação. Para tanto, a implementação-testes-atualização dos processos de detecção, o conhecimento dos fluxos de dados esperados e transitados pela entidade e a manutenção-monitoramento dos registos são essenciais para prover um sistema de detecção funcional e suficiente para uso dentro da entidade.

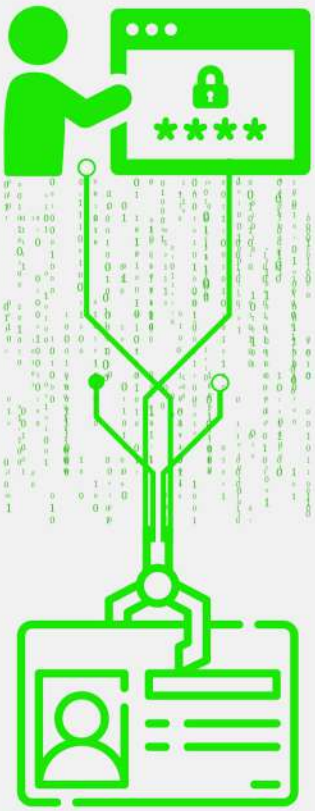
6. Gestão de Riscos em Segurança da Informação



4. RESPOSTA: o principal objetivo desta função direciona para o desenvolvimento e para a implementação de atividades oportunas para agir e reagir durante a detecção de um evento de segurança da informação. Neste ponto, a formulação e garantia que os planos de resposta sejam testados e atualizados e a coordenação das partes interessas (internas e externas) são fundamentais para o sucesso desta função.

5. RECUPERAÇÃO: por fim, o principal objetivo desta função está no desenvolvimento e na implementação de planos de continuidade e restauração de recursos e serviços afetados por evento ou incidente de segurança da informação. Assim, a comunicação entre as partes interessadas, a garantia que os planos de recuperação estejam atualizados e o gerenciamento de relações públicas e de reputação da entidade podem fazer a diferença para a concretização desta função.

6. Gestão de Riscos em Segurança da Informação

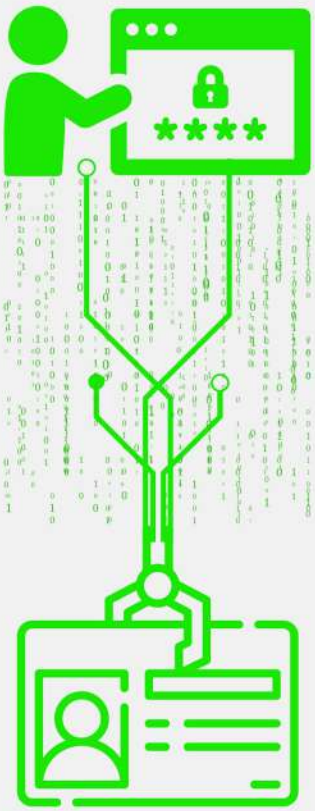


No *CyberSecurity Framework*, é possível observar que o gerenciamento de risco integra o gerenciamento de eventos e incidentes de segurança da informação, trazendo uma estrutura sólida e robusta utilizada em ciclo para funcionamento contínuo. Esses dois *frameworks* representam alternativas viáveis para controle de gestão de risco em segurança da informação.

Já o gerenciamento de riscos com base no padrão *Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE)* tem como foco o aproveitamento da experiência e da expertise dos recursos humanos na organização da gestão de riscos.

Esse método pode ajudar as entidades na minimização das vulnerabilidades e, por consequência, na exposição às ameaças. Igualmente, pode ajudar a estimar e determinar as consequências advindas de ataques cibernéticos e fornecer diretrizes para o enfrentamento destes incidentes de segurança caso se concretizem (CARALLI, 2007). Para isso, o OCTAVE possui três fases *in verbis*:

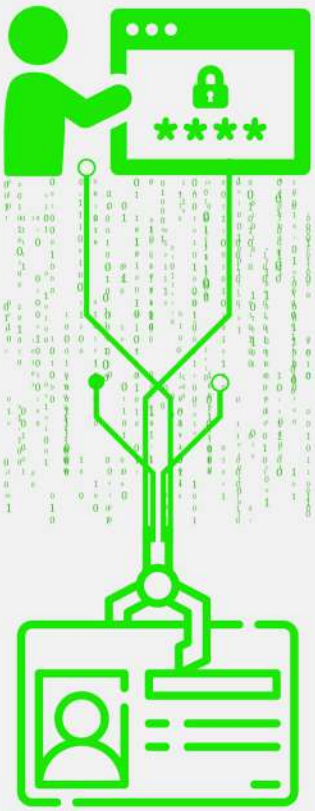
6. Gestão de Riscos em Segurança da Informação



1. A criação de perfis de ameaças, levando-se em consideração a priorização dos ativos apontados pela entidade; **2**. A identificação de todas as vulnerabilidades voltadas à infraestrutura; e, **3**. O desenvolvimento dos planos de segurança adequados com base nas fases anteriores.

Característica peculiar desta metodologia está na existência de duas categorias: uma para pequenas entidades (*OCTAVE-S*) e; uma versão mais abrangente, que pode ser utilizada até por entidades de grande porte (*OCTAVE Allegro*). A complexidade na implementação desta metodologia pode ser fator determinante para a escolha de sua utilização para a gestão de risco. Todavia, ela pode ser aplicada em conjunto com outras metodologias de gestão de risco, como a trazida pela ISO 27005.

6. Gestão de Riscos em Segurança da Informação



Na ISO/IEC 27005 é possível visualizar um sistema cíclico de gestão de risco em segurança da informação. Essa gestão é estabelecida em etapas que ajudam a entidade na definição de contexto, na identificação, análise e avaliação dos riscos, assim como em seu tratamento. Todas as etapas integram a comunicação e o monitoramento em suas atividades, permitindo que o controle da gestão seja eficiente e eficaz.

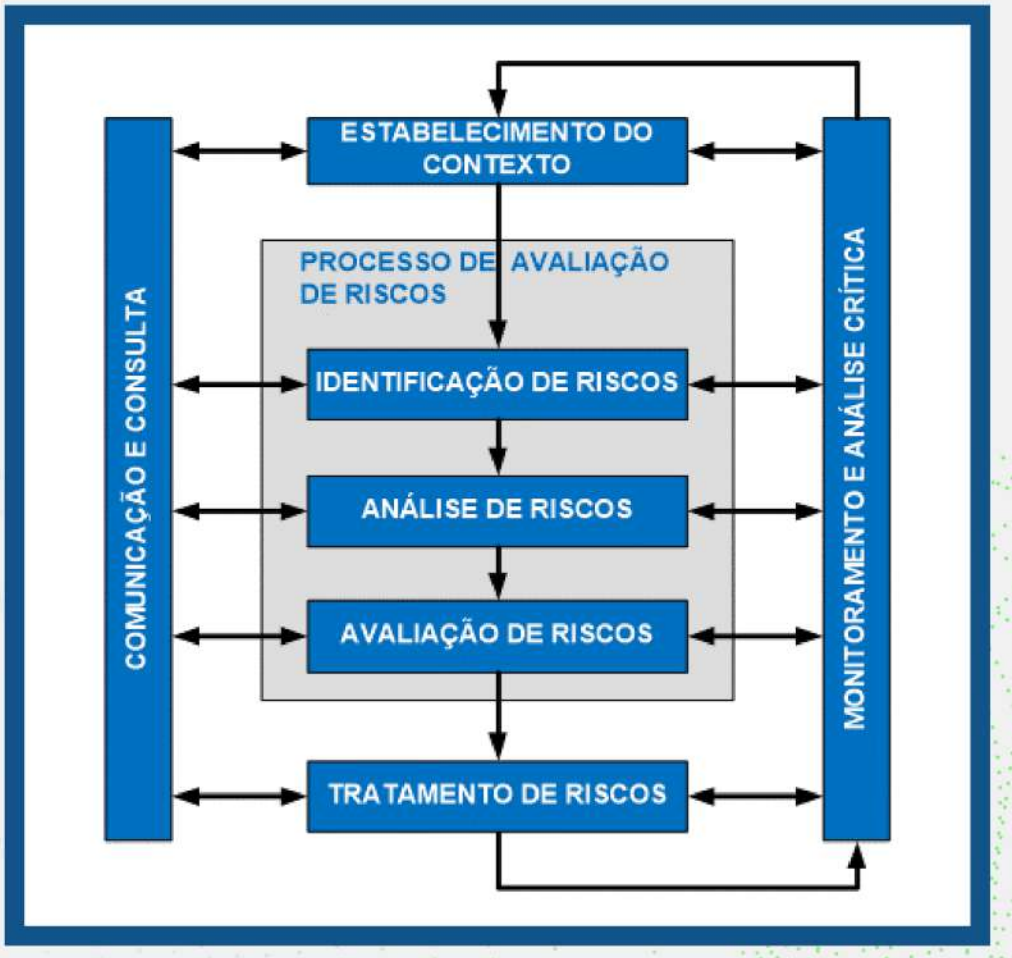
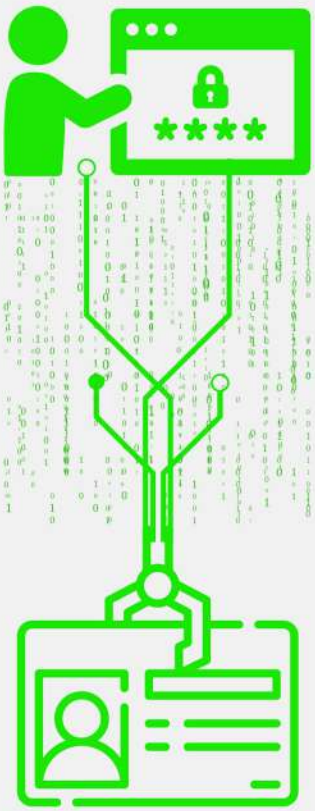


Figura: Gestão de risco em segurança da informação – ISO 27005

6. Gestão de Riscos em Segurança da Informação

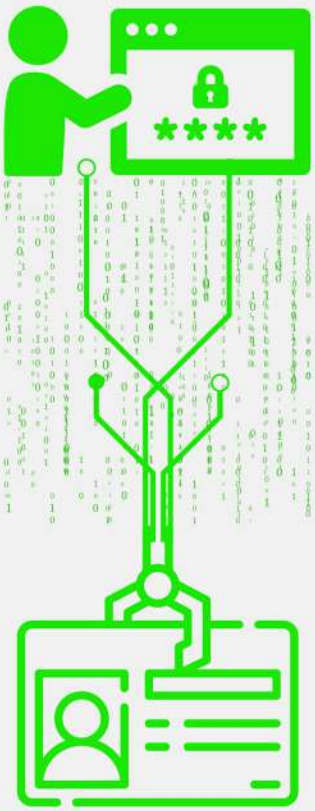


A ilustração evidencia o processo de gestão de risco proposto pela ISO 27005. Nela, observa-se as etapas mencionadas no parágrafo anterior. Segue breve descrição delas, conforme LÓPEZ (2014):

ESTABELECIMENTO DO CONTEXTO: nesta etapa, o contexto da gestão de risco deve ser estabelecido. Desta forma, os critérios para gestão e para a aceitação de riscos, as métricas para análise quantitativa e qualitativa devem ser apontadas, a abrangência da gestão e as responsabilidades precisam de definição. A partir deste passo que os demais se nortearão.

IDENTIFICAÇÃO DE RISCOS: nesta etapa, a identificação e mapeamento dos ativos de interesse da entidade, assim como os controles existentes, vulnerabilidades e possíveis consequências de sua explicação devem ser apontados.

6. Gestão de Riscos em Segurança da Informação

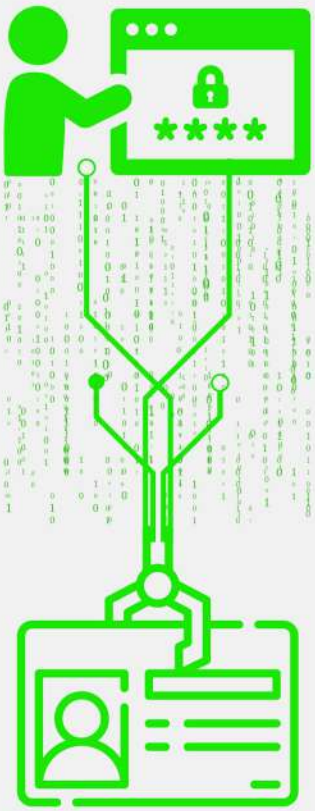


ANÁLISE DE RISCOS: nesta etapa, há uma estimativa das consequências e da probabilidade dos riscos identificados se concretizarem. Esta análise usualmente é realizada através de uma metodologia qualitativa ou quantitativa. Porém, nada impede que seja realizada através de uma metodologia quali quantitativa, integrando ambas as metodologias.

AVALIAÇÃO DE RISCOS: nesta etapa, ocorrerá um confronto com os resultados da análise dos riscos com os critérios de avaliação definidos na etapa de contexto, resultando na ordenação de prioridades de tratamento de riscos.

TRATAMENTO DE RISCOS: nesta etapa, o risco será tratado com base em estratégias bem definidas: modificação do risco, consiste na redução do risco encontro; retenção do risco, suportar as consequências do risco caso ele se concretize; evitar o risco, deixar de utilizar os ativos que representam um risco, o eliminando completamente e; compartilhamento do risco, estratégias que agrega terceiros para lidar com risco caso aconteça.

6. Gestão de Riscos em Segurança da Informação

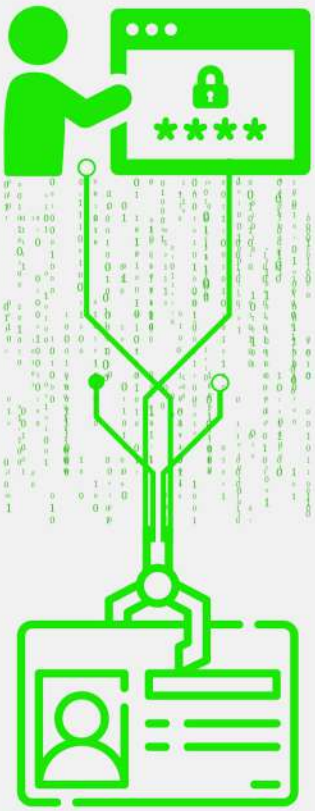


COMUNICAÇÃO: nesta etapa, o compartilhamento de dados e informação entre as partes interessadas sobre os riscos identificados, avaliados e tratados são essenciais para a gestão. Esta etapa é permanente e ocorre durante todo o ciclo de gestão do risco.

MONITORAMENTO: nesta etapa, todas as atividades e dados/informação da gestão de risco são controlados, proporcionando um alinhamento contínuo para a gestão.

ACEITAÇÃO DO RISCO: a aceitação do risco consiste em uma etapa em que os riscos que não puderam ser tratados são registrados e formalizados para que os responsáveis possam assumir as consequências pelo não tratamento. Isso mostra um retrato dos riscos que não foram tratados e as razões que resultado nisto.

6. Gestão de Riscos em Segurança da Informação



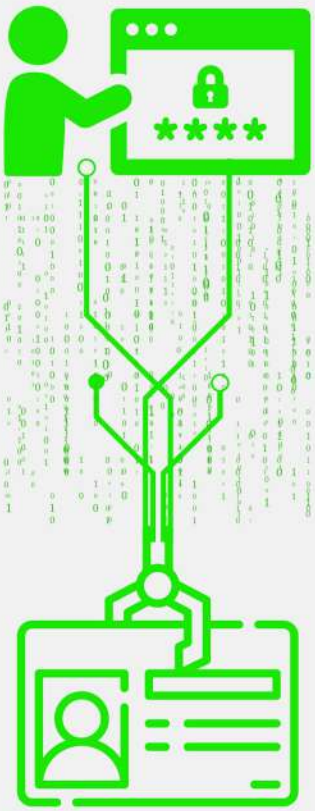
Por fim, o melhor método de gestão de risco em segurança da informação será aquele que melhor se adaptar às necessidades da entidade que a usará.

Cumpre destacar que todas as normas e padrões apresentados aqui são apenas de caráter orientativo, portanto, há abertura e margem para que a própria entidade possa utilizar o que lhe convier, inclusive usando-as em conjunto, se necessário.

Sumário

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

7. Gestão de Incidentes de Segurança da Informação



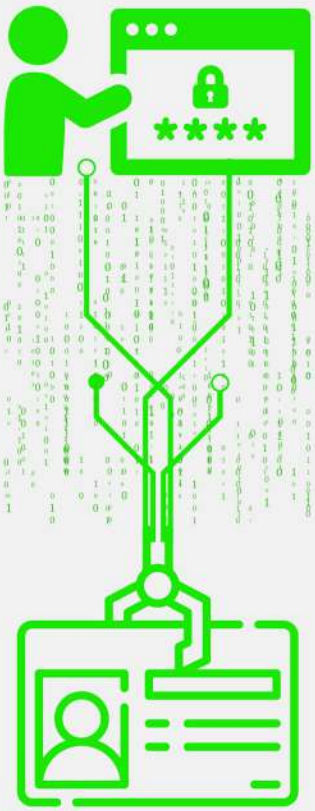
De início, cabe ressaltar que a existência de quaisquer controles de segurança tem como objetivo alcançar e manter os pilares da segurança da informação, são eles: a confidencialidade, a integridade e a disponibilidade.

Com este propósito estabelecido, uma gestão de risco em segurança da informação fornecerá uma ampla visualização do contexto que deverá ser resguardado.

O resultado de uma avaliação de risco bem-sucedida indicará quais estratégias de tratamento de risco e, por consequência os controles de segurança, poderão ser utilizados para atingir um nível de segurança adequado e específico para cada entidade.

Existem vários tipos de controles de segurança, dentre eles, os controles de segurança preventivos geralmente possuem protagonismo, ao passo que os investimentos direcionados a eles são consideráveis. No entanto, nenhum sistema está totalmente seguro, significando dizer que em algum momento eventos danosos ao sistema podem ocorrer.

7. Gestão de Incidentes de Segurança da Informação



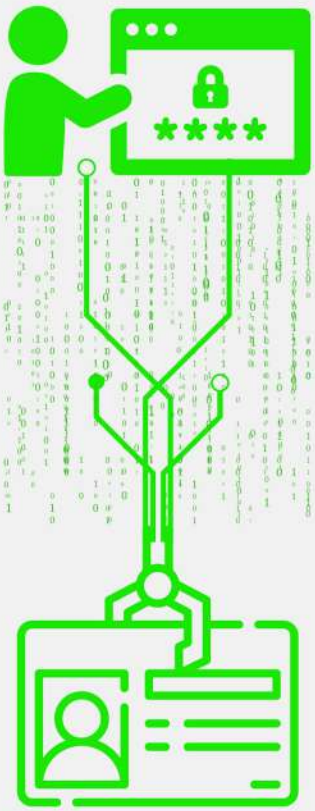
Neste ponto, lidar com estes tipos de eventos definirá se a entidade conseguirá continuar com suas atividades ou sofrerá com a possibilidade de paralisação de seus processos, projetos e serviços, resultando em prejuízos significativos.

7.1 Incidentes de segurança da informação

Para compreender a gestão de incidentes de segurança da informação, primeiramente, deve-se entender o que é um incidente de segurança da informação.

A literatura especializada usualmente o define como um evento ou série de eventos – indesejáveis ou inesperados - de segurança da informação com potencial para interromper as atividades de negócio da entidade ou que resultem em ameaça à segurança da informação (*HINTZBERGEN et al*, 2018).

7. Gestão de Incidentes de Segurança da Informação



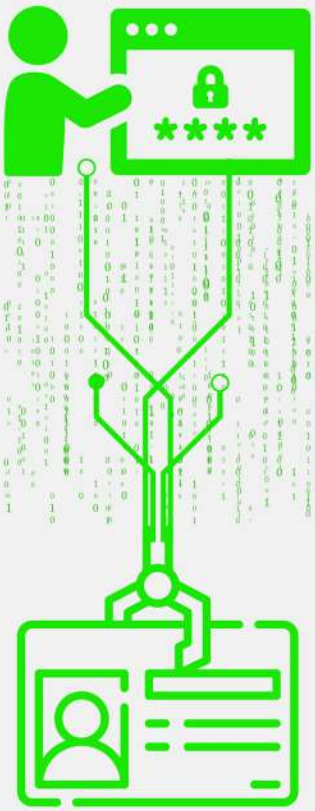
Por sua vez, um evento de segurança da informação pode ser conceituado como uma ocorrência identificada de um estado do sistema (*software*, infraestrutura, serviço) que aponte para uma possível violação da política de segurança da informação da entidade ou para uma falha em sua proteção (*HINTZBERGEN et a*l, 2018). Desta forma, é possível afirmar que todo incidente de segurança da informação é, em sua natureza, um evento de segurança a informação, porém, não se pode afirmar que todo evento de segurança da informação é um incidente de segurança.

O evento de segurança da informação, portanto, pode representar a concretização de um risco, que antes restava apenas em uma probabilidade. Diante deste cenário, cada evento de segurança deverá ser analisado e avaliado a fim de convertê-lo ou não em um incidente.

Consoante, esta decisão detém significativa relevância, pois desencadeará uma série de protocolos para eliminá-lo com o mínimo de prejuízos para a entidade.

7. Gestão de Incidentes de Segurança da Informação

7.2 O ciclo de vida de um incidente de segurança da informação



No incidente de segurança da informação é possível visualizar estágios que compõe um ciclo de vida, são eles: ameaça, o incidente, o dano e a recuperação.

A ameaça consiste na causa em potencial do incidente, onde um agente de ameaça é aquele que pode agir direta ou indiretamente para a concretização de um evento danoso para a entidade. No incidente, já existe toda a mobilização de recursos para combatê-lo.

Nesse passo, o dano é a consequência do incidente. Esse dano em si pode extrapolar facilmente a esfera patrimonial da entidade e saber como diminuí-lo é de vital importância. Por fim, a recuperação visa reestabelecer o estado anterior das atividades da entidade. Na Figura 1 expõe esse ciclo em sua sequência.

7. Gestão de Incidentes de Segurança da Informação

Figura: Ciclo de vida do incidente de segurança da informação

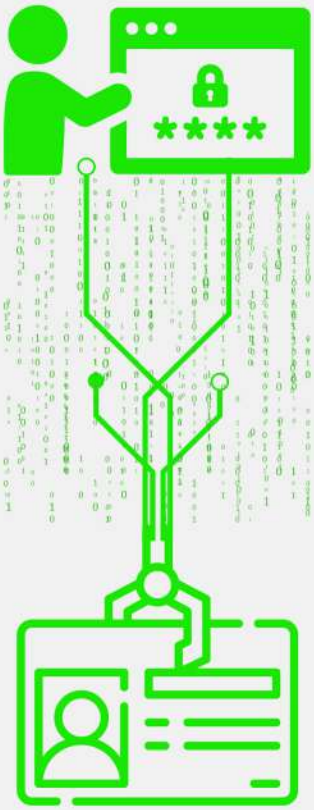
Fonte: Adaptada de HINTZBERGEN et al (2018).

Com base neste ciclo, os controles de segurança podem ser posicionados para evitar, detectar, reduzir, corrigir e avaliar o incidente. Segue breve descrição destas medidas e sua finalidade:

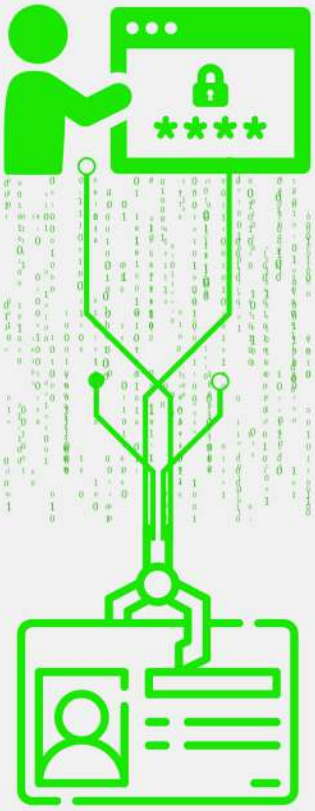
Medidas preventivas: tem como objetivo evitar que o incidente ocorra. Essa medida está presente entre a ameaça e o incidente.

Medidas detectivas: tem como finalidade a percepção do incidente, seja através de notificação de usuário ou de sistema. Essa medida está no incidente.

Medidas repressivas: tem como objetivo restringir os efeitos do incidente sobre o contexto da entidade. Essa medida está entre o incidente e o dano.



7. Gestão de Incidentes de Segurança da Informação



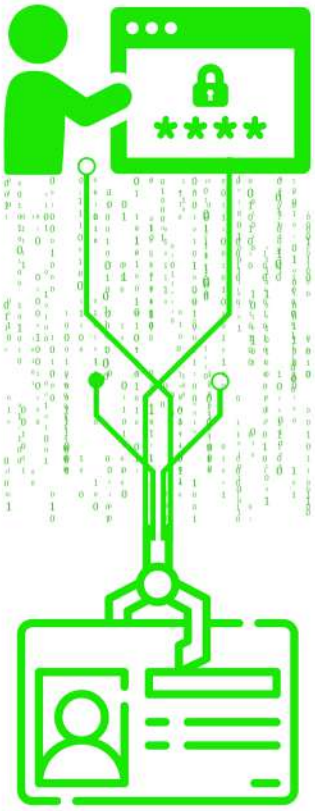
Medidas corretivas: tem como fim o reestabelecimento das atividades de negócio da entidade, devolvendo a capacidade de execução dos processos e serviços. Essa medida está na recuperação.

Medidas avaliativas: o objetivo destas medidas está na possibilidade de aprendizado, pois servirá como base para criação de novos protocolos contra incidentes. Essas medidas estão após a recuperação.

Todas os controles/medidas de segurança associadas ao modelo de ciclo de vida trazido nesta exposição funcionam em conjunto para lidar com incidentes de segurança. É preciso, no entanto, agrupar recursos humanos especializados e capacitados para utilizá-los da melhor forma.

7. Gestão de Incidentes de Segurança da Informação

7.3 Estrutura de gestão de incidentes de segurança da informação



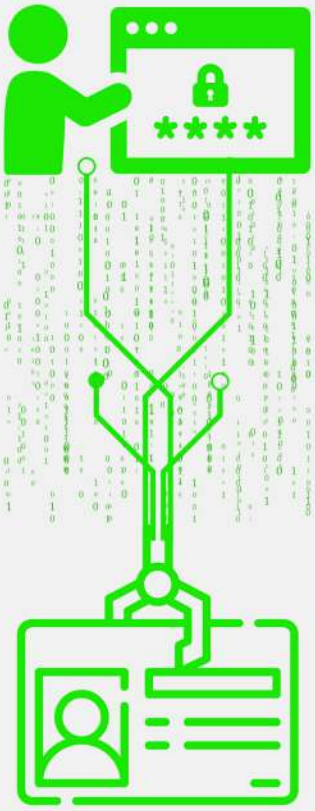
A estruturação de um sistema de gestão de incidentes de segurança da informação é fundamental para o sucesso da continuidade do negócio após um incidente ocorrer.

Essa estrutura tem por objetivo sistematizar a gestão do incidente, atribuindo responsabilidades, estabelecendo parâmetros para avaliação de eventos de segurança da informação, criando procedimentos para erradicação do incidente e planos para recuperação das atividades.

A ISO 27035 pode ajudar neste sentido. A Figura a seguir mostra como essa estrutura pode funcionar.

Fonte: Adaptada de BRITISH STANDARDS INSTITUTION (2011).

7. Gestão de Incidentes de Segurança da Informação



Na figura o primeiro ponto a ser observado está no estabelecimento de responsabilidade e procedimentos.

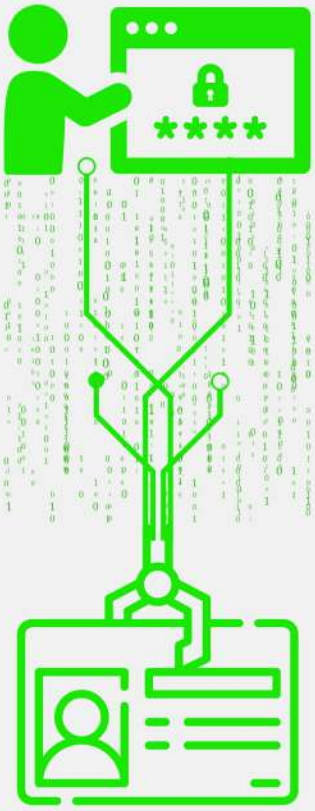
Nesta etapa, se faz necessária a criação de procedimentos para reverter cenários prováveis e conhecidos, a exemplo da contaminação dos sistemas por *malware*, invasão de dispositivo computacionais e infraestrutura, vazamento de dados e diversos outros. Além disso, as responsabilidades serão indicadas e distribuídas entre os recursos humanos disponíveis.

Questões primordiais precisam de resposta, são elas: Quem deverá receber as notificações de eventos de segurança? Quem será responsável pela avaliação desses eventos para determinar a conversão em incidente? Quem deverá declarar o incidente e mobilizar recurso? Quem deverá realizar os procedimentos de contenção, erradicação e recuperação dos sistemas? Quem deverá realizar as ações de suporte? Quem deve declarar o término do incidente?

Em seguida, as notificações de eventos e de fragilidade devem ser, igualmente, estruturadas ao ponto de essas tais atividades eficientes.

A notificações de eventos possibilitará que o usuário, interno e externo, e o sistema possam notificar um ou mais eventos para a ciência da entidade.

7. Gestão de Incidentes de Segurança da Informação



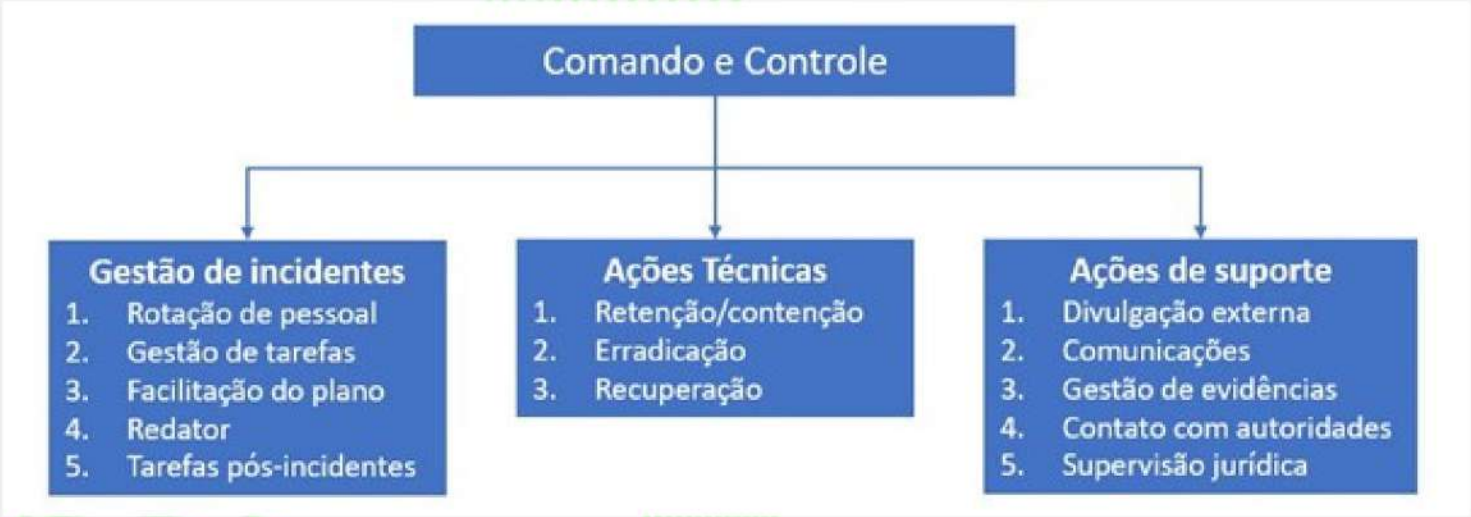
As notificações de fragilidade destinam-se à comunicação externa com parceiros e fornecedores que compartilham sistemas, pois uma entidade fragilizada pode servir de ponto de acesso à entidade alvo.

Após o evento de segurança ser detectado e reportado, segue para uma avaliação mais detalhada com base em parâmetros definidos na primeira etapa. Nesta fase, será decidido se existirá a conversão do evento para incidente de segurança. Diante desta decisão, dois caminhos podem ser percorridos: **1**) em caso de incidente de segurança, os protocolos adequados serão acionados e executados e; **2**) em caso de não configuração de incidente de segurança, o evento será representado como conhecimento para que em um próximo ciclo não seja estranho à entidade.

No fim do ciclo estrutural está a coleta de evidências. A preocupação com esta fase reside no fato, se robusta e bem feita, em substanciar procedimentos oficiais como auxílio ao trabalho policial ou provas em processos judiciais, por exemplo. Esta fase, mais do que nas demais, se faz necessária a presença de um perito capacitado, pois o erro na coleta ou a forma errada de preservação pode comprometer todas as evidências inutilizando-as.

7. Gestão de Incidentes de Segurança da Informação

Figura: Topologia de ações em planos de resposta à incidentes de segurança

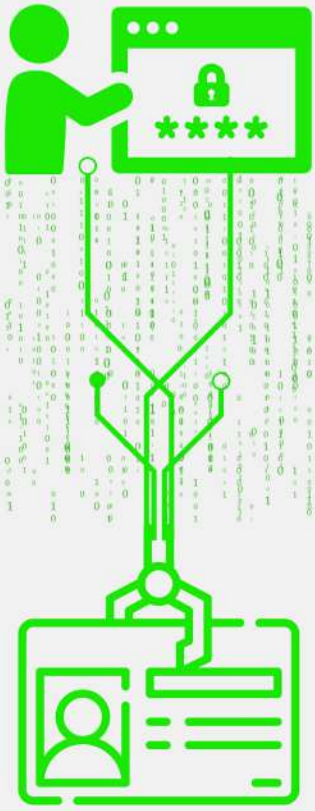


Fonte: Adaptada de MCCARTHY (2014).

Na Figura acima, três grupos de ações são expostas: gestão de incidentes, ações técnicas e ações de suporte.

A primeira diz respeito às ações de gerência do incidente, cujas tarefas e pessoas serão direcionadas, a documentação das ações estará concentrada e o pós-incidente será direcionado. Nas ações técnicas, a equipe de reposta se concentrará em reter os efeitos do incidente para que não se espalhe em proporções. Além disto, realizarão ações para erradicar a ameaça, seguindo para ações de recuperação do sistema.

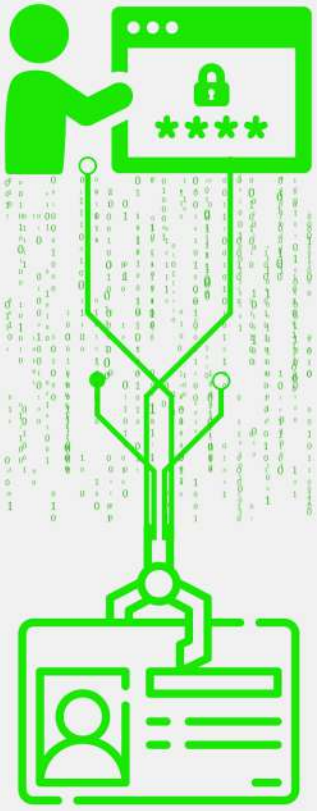
Nas ações de suporte, atividades complementares serão executadas com o propósito de dar sustentação efetiva às ações técnicas. Na divulgação externa, o incidente será reportado aos terceiros interessados, aqueles que são afetados.



7. Gestão de Incidentes de Segurança da Informação

As comunicações internas são importantes para que todos saibam o que fazer e quando.

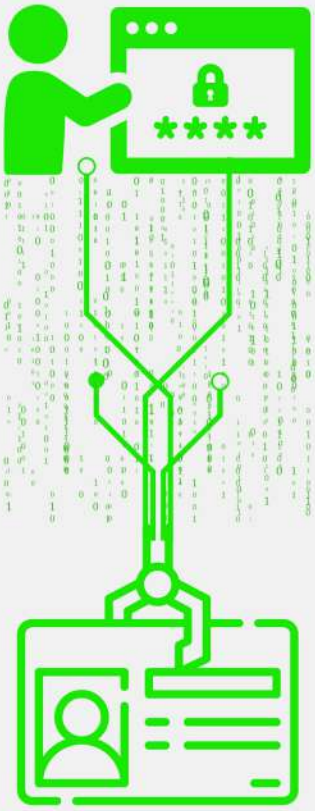
A gestão de evidências se destina a preservação da cadeia de evidências. Já o contato com autoridades poderá ser necessário para uma possível investigação policial ou para cumprimento de dever legal, como a comunicação com a Autoridade Nacional de Proteção de Dados (ANPD), em casos de incidentes com dados pessoais. Ao final, o acompanhamento jurídico durante todo o processo ajudará com questões legais, tanto de forma preventiva quanto reativa.



Sumário

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

Considerações Finais



A conclusão é que quando o assunto é segurança da informação é necessário para alcançar um mínimo desejável, que haja pessoas comprometidas e treinadas, uso de tecnologia para facilitar e monitorar, e que somando pessoas e tecnologias haja processos bem definidos pois será esse conjunto que fará a segurança da informação acontecer de forma efetiva e eficaz nas organizações.

Segurança da informação não é assunto exclusivo da área de TI/segurança da informação envolve a organização como um todo, é um assunto que tem início mas não tem fim, um programa que, portanto deve ser atualizado e revisado constantemente pelas pessoas envolvidas nos processos.

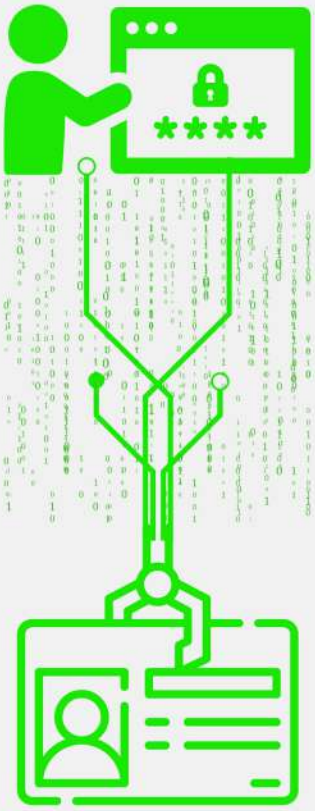
Há diversas boas práticas que podem e devem ser adotadas mesmo quando não haja recursos financeiros, pois conforme discorrido neste *e-book* há diversas orientações normativas, *frameworks*, legislações e doutrinas que permitem ações independentemente de investimentos financeiros.

Sendo assim, para o presente e o futuro, enquanto profissionais de TI, área jurídica (advogados), consultores e demais interessados é essencial a união de esforços e parcerias desses profissionais que atuam nas diversas áreas da proteção e privacidade de dados, segurança da informação, tecnologia da informação, gestão de continuidade de negócios, compliance digital, inovação e areas

Considerações Finais

correlatas, pois segurança da informação é apenas um tema dentre tantos da atualidade no direito digital, inovação e tecnologia.

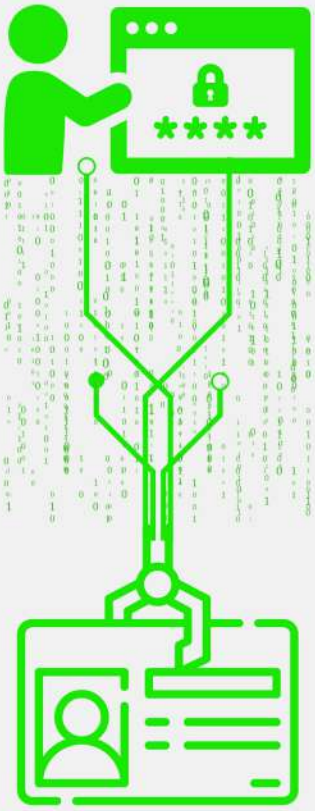
Na atualidade o profissional deve ter conhecimentos interdisciplinares e multidisciplinares para atender as demandas de mercado, e mais, é necessário buscar parcerias para oferecer as melhores soluções integradas para o ecossistema das organizações, gerando desta forma mais credibilidade e confiabilidade.



Sumário

ANADD
Associação Nacional de Advogadas e Advogados de Direito Digital

Referências bibliográficas



ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27014: Segurança da informação, segurança cibernética e proteção da privacidade — Governança da segurança da informação. Rio de Janeiro, 2ª Ed. 2021.

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 – Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005.

AGRAWAL, Vivek. Towards the Ontology of ISO/IEC 27005: 2011 Risk Management Standard. In: HAISA. 2016.

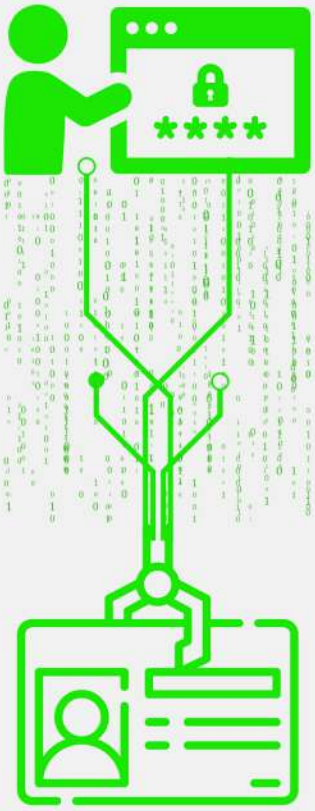
ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO 27002:2013: Tecnologia da Informação - Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

BRITISH STANDARDS INSTITUTION. BS ISO/IEC 27035: 2011: Information Technology-Security Techniques-Information Security Incident Management. BSI, 2011.

CARALLI, Richard A. et al. Introducing octave allegro: Improving the information security risk assessment process. Carnegie-Mellon Univ Pittsburgh PA Software Engineering Inst, 2007.

HINTZBERGEN, Jule et al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. Brasport, 2018.

Referências bibliográficas



https://radarlegislativo.org/projeto/1/
https://www.27001.pt/iso27001_2.html
https://www.abnt.org.br/
https://www.abntcatalogo.com.br/normagrid.aspx
https://www.gov.br
https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/legislacao-federal
https://www.iso.org/home.html
https://www25.senado.leg.br/web/atividade/materias/-/materia/113947
https://www.estrategiaconcursos.com.br/blog/principios-seguranca-informacao.

ISO. ISO 27005:2011 - Information security risk management. [S.l.]: ISO/IEC, 2011.

LÓPEZ, Víctor Leonel Orozco et al. Análise/avaliação de riscos de segurança de informação: quantificação de confiança como um parâmetro de redução de desvios de resultados por causas humanas. 2014.

MCCARTHY, N. K. Resposta a Incidentes de Segurança em Computadores: planos para proteção de informação em risco. Bookman Editora, 2014.

NIST. CyberSecurity Framework. 2018. Disponível em: https://www.nist.gov/cyberframework/framework, acesso em: 31 out 2022.

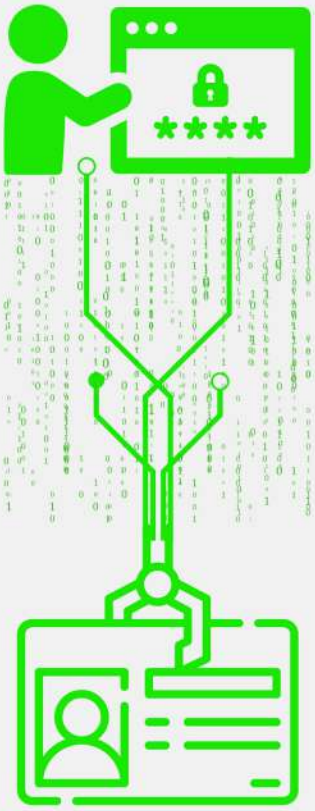
Risk Management Framework. 2022. Disponível em: https://csrc.nist.gov/Projects/risk-management, acesso em: 31 out 2022.

Referências bibliográficas

SEGURANÇA E SUA IMPORTÂNCIA NAS OPERAÇÕES DE TECNOLOGIA DA INFORMAÇÃO DAS ORGANIZAÇÕES - Monografia Renato Amabile Novembro 2015 rev2.

SOBRAL ROCHA, K. H. Conheça os Princípios da Segurança da Informação para a SEFAZ AL. [S. l.], 2021.

TEXEIRA FILHO, S. A. Segurança da Informação segundo a ISO 27002/2005: Conceitos de Segurança da Informação. In: SEGURANÇA da Informação Descomplicada. 1. ed. Brasília: [s. n.], 2015.



COMITÊ DE CIBERSEGURANÇA

ANADD

Associação Nacional de
Advogadas e Advogados de Direito Digital

GT Cibersegurança

Coautores:

Andreza Sobreira
Crystine Joranhezon
Eduardo Dias
Everton Lopes
Izaac Alencar
Maria Santos

Coordenação:

Andreza Sobreira e Izaac Alencar

Arte e Design:

Ricardo Castro Cajazeira

Revisão:

Andreza Sobreira, Fábio Uema e Ricardo Castro Cajazeira

ISBN registrado sob nº: 978-65-999397-0-9
Título: Introdução à Cibersegurança
Subtítulo: Principais Aspectos da Segurança da Informação
Formato: Livro Digital
Veiculação: Digital

ANADD.ORG