Poder Judiciário

Conselho Nacional de Justiça

ANEXO V – Manual de referência – Prevenção e mitigação de ameaças cibernéticas e confiança digital

Manual de Referência

Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

Material de referência com os principais controles de segurança cibernética necessários para prevenção e mitigação de ameaças cibernéticas e confiança digital

Poder Judiciário

Conselho Nacional de Justiça

Sumário

Introdução

0.1. Visando responder aos recentes episódios de materialização de ameaças cibernéticas em entidades da Administração Pública, foi instituído o Comitê Gestor de Segurança Cibernética do Poder Judiciário (CGSCPJ), tendo como objetivo apoiar os órgãos do Judiciário estabelecendo padrões mínimos para proteção de sua infraestrutura tecnológica.

0.2. No que diz respeito à Prevenção e Mitigação de Ameaça Cibernéticas e Confiança Digital, foram organizadas, neste Manual, orientações para aplicação de melhores práticas reconhecidas no mercado e uma lista de controles mínimos exigidos para implantação pelos órgãos do Judiciário.

0.3. O documento está estruturado da seguinte forma.

- **Capítulo 1**: **Principais *frameworks* de referência utilizados**

  Em que são apresentados em uma visão macro os *frameworks* que foram utilizados para confecção do Manual.

- **Capítulo 2**: **Padrões mínimos de Gestão de Riscos de Segurança da Informação**

  Baseados nas normativas relacionadas e, em especial, na ABNT/NBR ISO/IEC 27005:2019, apresentam-se os requisitos mínimos para gestão de riscos de segurança da informação incluindo terminologia, princípios, diretrizes, objetivos, estrutura e competência e uma proposta de processo de gestão.

- **Capítulo 3**: **Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas**

  Com referência à norma ISO 27007:2018, são apresentados terminologia; princípios e diretrizes; objetivos e estruturas; e competências para contratação externa ou cooperação entre organizações do Poder Judiciário.

- **Capítulo 4**: **Confiança digital, prevenção e mitigação de ameaças cibernéticas**

  Considerando *framework* do MITTRE AT&CK e as cinco tecnologias-chave para habilitar uma estrutura de resiliência cibernética sugeridas pelo IDC,

apresenta metas, objetivos, princípios de *design*, *framework* sugerido e requisitos a serem observados para promoção de resiliência cibernética.

- **Capítulo 5 e Anexo I**: **Modelo de *checklist***

  Apresentam sugestões de controles para uso na organização que possibilitem acompanhar a maturidade no que diz respeito às iniciativas descritas no presente Manual.

1. Principais *frameworks* de referência utilizados

1.1 Quando se fala sobre "segurança digital", "segurança cibernética" ou até mesmo "segurança da informação", é muito importante identificar os principais modelos e referências utilizados no mercado, analisar e comparar os requisitos, implementar aquelas orientações que se adequam melhor ao cenário em que a empresa se encontra atualmente, e buscar melhorias que possibilitem alcançar a visão de futuro.

1.2 . Por isso, para os principais temas correlatos serão listados a seguir alguns padrões que podem auxiliar essa busca.

2. MITRE ATT&CK

2.1 A MITRE ATT&CK é uma base de conhecimento de táticas e técnicas adversárias com base em observações do mundo real[1]. A base de conhecimento da ATT&CK é aceita como base para o desenvolvimento de modelos e metodologias de ameaças específicas no setor privado, no governo e na comunidade de produtos e serviços de segurança cibernética. A publicação está disponível para uso gratuito por qualquer pessoa ou organização.

3. Norma ABNT NBR ISO/IEC 27000:2018

3.1 A norma ISO/IEC 27000:2018 fornece a visão geral dos sistemas de gerenciamento de segurança da informação e os termos e definições comumente usados na família de normas ISO/IEC 27001.

[1] https://attack.mitre.org/.

3.2 Projetada para ser aplicável a todos os tipos e tamanhos da organização de negócios, desde multinacionais até as pequenas e médias empresas, a nova versão é igualmente valiosa para agências governamentais ou organizações sem fins lucrativos[2].

4. Norma ABNT NBR ISO/IEC 27001:2013

4.1 Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Esta norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização[3].

5. Norma ABNT/NBR ISO/IEC 27005:2019

5.1 Fornece diretrizes para o processo de gestão de riscos de segurança da informação[4].

6. Norma ABNT NBR ISO/IEC 27007:2018

6.1 Fornece diretrizes sobre como gerenciar um programa de auditoria de sistemas de gestão da segurança da informação (SGSI), sobre como executar as auditorias e sobre a competência dos auditores de SGSI[5], em complemento às diretrizes descritas na ABNT NBR ISO 19011:2012.

7. Norma ABNT NBR ISO/IEC 19011:2018

7.1 Fornece orientação sobre a auditoria de sistemas de gestão, incluindo os princípios de auditoria, a gestão de um programa de auditoria e a condução de auditoria de sistemas de gestão, como também orientação sobre a avaliação de competência de pessoas envolvidas no processo de auditoria[6]. Essas atividades incluem a(s) pessoa(s) que gerencia(m) o programa de auditoria, os auditores e a equipe de auditoria.

---

[2] http://www.abnt.org.br/noticias/5777-iso-iec-27000-norma-internacional-de-seguranca-da-informacao-e-revisada.
[3] https://www.abntcatalogo.com.br/norma.aspx?ID=306580.
[4] https://www.abntcatalogo.com.br/norma.aspx?ID=429058.
[5] https://www.abntcatalogo.com.br/norma.aspx?ID=401077.
[6] http://www.abnt.org.br/noticias/6215-abnt-nbr-iso-19011-finalmente-publicada.

8. Norma Complementar n. 11/IN01/DSIC/GSIPR, de 2012

8.1 Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF[7].

9. NIST SP 800-160 v2

9.1 Esta publicação é usada em conjunto com a ISO/IEC/IEEE 15288: 2015 (Engenharia de sistemas e *software* – processos de ciclo de vida de sistemas), NIST *Special Publication* 800-160 volume 1 (Engenharia de segurança de sistemas – Considerações para uma abordagem multidisciplinar na engenharia de confiabilidade Sistemas Seguros) e NIST *Special Publication* 800-37 (Estrutura de Gerenciamento de Risco para Sistemas de Informação e Organizações – uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade)[8].

9.2 Ele pode ser visto como um manual para alcançar os resultados de resiliência cibernética identificados com base em uma perspectiva de engenharia de sistemas nos processos do ciclo de vida do sistema em conjunto com os processos de gerenciamento de risco, permitindo que a experiência e o conhecimento da organização ajudem a determinar o que é correto para seu propósito.

10. Resolução CNJ n. 309, 11 de março de 2020

10.1 Aprova as Diretrizes Técnicas das Atividades de Auditoria Interna Governamental do Poder Judiciário – DIRAUD-Jud e dá outras providências[9].

[7] https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/02/2012&jornal=1&pagina=2&totalArquivos=264.
[8] https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final.
[9] https://atos.cnj.jus.br/atos/detalhar/3289.

11. Padrões mínimos de Gestão de Riscos de Segurança da Informação

11.1 A gestão de riscos em âmbito corporativo é essencial para a boa governança, uma vez que fornece garantia razoável para que os objetivos organizacionais sejam alcançados. A integração da gestão de riscos à governança corporativa é apontada em diversos modelos de melhores práticas.

11.2 O Tribunal de Contas da União (TCU), por exemplo, define a gestão de riscos como uma das principais funções da governança em seu documento "Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública[10]".

11.3 Também compreendendo essa importância, o Conselho Nacional de Justiça (CNJ) instituiu, por meio da Portaria n. 277 de 10 de outubro de 2019, o "Manual de Gestão de Riscos[11]" no âmbito de sua Diretoria-Geral.

11.4 Considerando a importância da gestão de riscos também no que diz respeito à Segurança da Informação, a Associação Brasileira de Normas Técnicas (ABNT), baseando-se no modelo americano, publicou a NBR/ISO 27.005 (atualizada em 2019), que fornece diretrizes para o processo de gestão de riscos de segurança da informação.

11.5 Embora se assemelhe ao modelo de gestão de riscos corporativos (publicado por meio da norma NBR 31.000), a referida norma está focada na gestão de riscos relacionada à segurança da informação.

11.6 A seguir serão apresentadas a terminologia, os princípios, as diretrizes, os objetivos, a estrutura e as competências e o processo de gestão de riscos.

12. Princípios

12.1 Sugere-se que a política de gestão de riscos de segurança da informação observe os seguintes princípios:

a) Proteção dos valores organizacionais;
b) Melhoria contínua da organização;

[10] https://portal.tcu.gov.br/data/files/FA/B6/EA/85/1CD4671023455957E18818A8/Referencial_basico_governanca_2_edicao.PDF.
[11] https://atos.cnj.jus.br/atos/detalhar/3060.

c) Visão sistêmica;
d) Qualidade e tempestividade das informações;
e) Abordagem explícita da incerteza;
f) Transparência;
g) Dinamismo e interatividade;
h) Alinhamento à gestão de riscos corporativos;
i) Integração.

13. Diretrizes

13.1 Sugere-se que o processo de gestão de riscos de segurança da informação observe as seguintes diretrizes:

a) Ser parte integrante dos processos organizacionais de Tecnologia da Informação e Comunicação (TIC);
b) Ser parte da tomada de decisões;
c) Ser sistemático, estruturado e oportuno;
d) Ser baseado nas melhores informações disponíveis;
e) Considerar fatores humanos e culturais;
f) Ser transparente e inclusivo;
g) Ser dinâmico, iterativo e capaz de reagir às mudanças tempestivamente;
h) Contribuir para a melhoria contínua da organização.

14. Objetivos

14.1 Sugere-se que a política de gestão de riscos de segurança da informação tenha por objetivo:

a) Apoiar as unidades organizacionais no que tange aos riscos de segurança da informação em tecnologia da informação da organização;
b) Aprimorar o processo de tomada de decisão, com o propósito de incorporar a visão de riscos em conformidade com as melhores práticas;
c) Melhorar a alocação de recursos;
d) Aprimorar os controles internos;
e) Alinhar a tolerância a risco à estratégia adotada;

f) Resguardar a Administração Superior e os demais gestores da organização quanto à tomada de decisão e à prestação de contas;
g) Identificar, avaliar e reagir às oportunidades e ameaças;
h) Melhorar a eficiência operacional por meio do gerenciamento de riscos proativos.

15. Estrutura e Competências

15.1 Sugere-se que se estabeleça uma estrutura de gestão de riscos de segurança da informação identificando pelo menos:

a) O Comitê Gestor de Segurança da Informação (CGSI);
b) A unidade dirigente de TIC do órgão;
c) A unidade responsável pela Gestão de Segurança da Informação de TIC do órgão;
d) Os gestores de riscos;
e) Os gestores de processos, serviços e ativos de TIC.

15.2 São considerados gestores de riscos, em seus respectivos âmbitos e escopos de atuação, os titulares das unidades responsáveis pelos serviços.

15.3 São considerados gestores de processos, serviços e ativos de TIC os responsáveis pelos processos de trabalho, projetos e ações desenvolvidos nos níveis estratégico, tático e operacional do órgão.

15.4 Embora determinem-se papéis e responsabilidades específicas, espera-se que a gestão de riscos de segurança da informação seja de responsabilidade compartilhada de magistrados e magistradas, servidores e servidoras, estagiários e estagiárias, e prestadores e prestadoras de serviço.

16. Comitê Gestor de Segurança da Informação (CGSI)

16.1 Compete ao Comitê Gestor de Tecnologia da Informação:

I. Aprovar a política de gestão de riscos de segurança da informação;

II. Analisar os riscos não tratados bem como decidir sobre possíveis providências;

III. Decidir sobre prioridades de atuação.

17. Unidade dirigente de TIC do órgão

17.1 Compete à unidade dirigente de TIC do órgão:

I. Disseminar a política de gestão de riscos de segurança da informação em suas unidades subordinadas;

II. Monitorar, avaliar, revisar e propor alterações na política de gestão de riscos de segurança da informação;

III. Monitorar o tratamento dos riscos;

IV. Analisar e encaminhar o Relatório de Riscos de Segurança da Informação não tratados ao CGETI.

18. Unidade responsável pela Gestão de Segurança da Informação de TIC do Órgão

18.1 Compete à unidade responsável pela Gestão de Segurança da Informação de TIC do Órgão:

I. Propor as atualizações necessárias à presente política;

II. Monitorar o processo de gestão de riscos de segurança da informação;

III. Elaborar relatórios de riscos de segurança da informação.

19. Gestores de riscos

19.1 Compete aos gestores de riscos:

I. Realizar a escolha dos processos de trabalho que devam ter os riscos gerenciados e tratados, tendo em vista a dimensão dos prejuízos que possam causar;

II. Propor os níveis aceitáveis de exposição ao risco, de modo a consolidar a tolerância ao risco das unidades e dos serviços auxiliares do órgão;

III. Definir as ações de tratamento a serem implementadas, bem como o prazo de implementação e avaliação dos resultados obtidos.

20. Gestores de processos

20.1 Compete aos gestores de processos, serviços e ativos de TIC:

I. Contribuir para as atividades de identificação e avaliação dos riscos inerentes aos processos de trabalho, serviços e ativos de TIC sob sua responsabilidade;

II. Gerenciar os riscos inerentes aos processos de trabalho, serviços e ativos de TIC sob sua responsabilidade, de forma a mantê-los em nível de exposição aceitável;

III. Implementar os planos de ação definidos para tratamento dos riscos inerentes em processos de trabalho, serviços e ativos de TIC;

IV. Comunicar novos riscos inerentes aos seus processos e que não fazem parte da relação de riscos institucionais já identificados.

21. Processo de Gestão de Riscos de Segurança da Informação

21.1 Recomenda-se que o processo de gestão de riscos de segurança da informação contemple as seguintes fases.

I. Estabelecimento do contexto: os processos de trabalho, sistemas, serviços e ativos de Tecnologia da Informação e Comunicação do órgão de um contexto definido serão submetidos, periodicamente, à análise de segurança, buscando-se identificar vulnerabilidades técnicas que possam vir a comprometer os dados, os objetivos de negócio e/ou afetar a imagem institucional do órgão;

II. Identificação dos riscos: inventário e descrição dos eventos de risco que possam comprometer os dados, os objetivos de negócio e/ou afetar a imagem institucional do órgão;

III. Análise dos riscos: compreensão da natureza do risco e determinação do respectivo nível de risco mediante a combinação da probabilidade de sua ocorrência e dos impactos possíveis;

IV. Avaliação dos riscos: verificação dos resultados da análise de riscos pelas unidades responsáveis pelos processos de trabalho, sistemas, serviços ou ativos de TIC afetados, de modo a determinar se o risco é ou não aceitável;
V. Tratamento dos riscos: seleção e implementação, pelas unidades responsáveis pelos processos de trabalho, sistemas, serviços ou ativos de TIC afetados, de um ou mais controles em resposta aos riscos;
VI. Monitoramento: acompanhamento quanto à efetividade de todas as fases do processo de gestão de riscos de segurança da informação;
VII. Comunicação: manutenção de fluxo constante de informações entre as partes interessadas durante todas as fases do processo de gestão de riscos de segurança da informação.

21.2 As ações de tratamento deverão explicitar as iniciativas propostas, os responsáveis pela implementação, os recursos requeridos e o cronograma sugerido.

21.3 As fases, os procedimentos e os instrumentos necessários ao processo deverão ser formalizados em ferramenta corporativa adequada.

21.4 Os sistemas, serviços e ativos de TIC homologados devem ser submetidos à unidade responsável pela Gestão de Segurança da Informação de TIC do órgão para identificação de riscos, antes de sua primeira efetiva disponibilização em ambiente de produção, de modo a se evitar a exploração de vulnerabilidades em ambiente crítico.

21.5 A publicação de sítios eletrônicos, aplicações ou serviços no domínio oficial do órgão na internet e/ou em seus subdomínios deverá ser normatizada.

21.6 A política de gestão de riscos de segurança da informação deverá abranger categorias de impacto de risco, sugerindo-se os seguintes:

I. Muito baixo;

II. Baixo;
III. Médio;
IV. Alto;
V. Muito alto.

21.7 Além disso, também deverá prever categorias de probabilidade de risco, sugerindo-se os seguintes:

I. Muito baixo;
II. Baixo;
III. Médio;
IV. Alto;
V. Muito alto.

21.8 Deverão ser considerados, para fins de categorização e classificação, tanto os riscos internos quanto os riscos externos à organização.

22. Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas

22.1 A necessidade de garantia de melhoria contínua e adequação nas áreas de segurança da informação e gestão de segurança da informação abrem campo de alta relevância para as áreas de Controle Interno e Auditoria dos órgãos do Poder Judiciário.

22.2 Com base em boas práticas de referência e normativas vigentes no Judiciário, este Manual busca ampliar a capacidade de cooperação dos órgãos, bem como indicar requisitos que garantem qualidade das auditorias de segurança da informação.

23. Princípios e Diretrizes

23.1 Os princípios e diretrizes técnicas devem ser os observados na Resolução CNJ n. 309, de 11 de março de 2020, e em normas de referência que guiam atividades de

auditoria, como a ABNT ISO/IEC NBR 19011:2018 e a ABNT ISO/IEC NBR 19011:2018. As referências citadas devem ser consideradas no escopo das auditorias relacionadas à segurança da informação.

24. Objetivos

24.1 A aplicação dos controles deste Manual busca assegurar que as auditorias sobre segurança da informação cumpram pontos mais específicos desse tipo de auditoria, além de buscar caminhos para viabilizar auditorias cruzadas e terceirizadas. Auditorias serão executadas com mais independência, qualidade e, consequentemente, subsidiarão mais efetivamente a melhoria contínua da gestão de segurança da informação em cada órgão.

25. Estrutura e Competências

25.1 É imprescindível que esta norma seja compreendida e aplicada pela área de Controle Interno ou Auditoria de cada órgão. A internalização dessa necessidade deve elevar a maturidade da gestão de segurança da informação no Poder Judiciário como um todo, principalmente se viabilizadas as auditorias cruzadas e eventuais auditorias terceirizadas.

25.2 Cada órgão tem autonomia para definir o posicionamento das suas unidades na estrutura organizacional, o que garante a acomodação de novas funções organizacionais que considera as peculiaridades de cada órgão. Entretanto, é imprescindível que cada órgão considere a inclusão da gestão de segurança da informação em sua estrutura, buscando conciliar as boas práticas e suas peculiaridades na escolha da posição dessas funções na estrutura organizacional.

26. Confiança digital, prevenção e mitigação de ameaças cibernéticas

26.1 Resiliência, segundo Hausken[12], é a capacidade de uma entidade resistir, responder e se recuperar de um incidente cibernético, mantendo os seus serviços operacionais.

[12] Hausken, Kjell (9/2020). "Cyber resilience in firms, organizations and societies".

27. Metas

27.1 Para a garantia de um nível de segurança cibernética adequado deve-se estabelecer, no mínimo, 4 (quatro) metas[13]:

a) Antecipar: manter o estado informado e preparado para adversidade;
b) Resistir: manter as atividades essenciais ao negócio apesar da adversidade;
c) Recuperar: restaurar a missão ou as funções de negócios durante e após a adversidade; e
d) Adaptar: modificar a missão ou as funções de negócios e/ou recursos de suporte para mudanças previstas nos ambientes técnicos, operacionais ou de ameaças.

28. Objetivos

28.1 Para implementar uma estratégia de resiliência cibernética devem ser previstos, no mínimo, 4 (quatro) objetivos específicos[14]:

a) Prevenir: impedir a execução bem-sucedida de um ataque ou a imposição de condições adversas;
b) Preparar: manter um conjunto de ações realistas que abordem adversidades previstas;
c) Continuar: maximizar a duração e a viabilidade da missão ou funções de negócios essenciais durante adversidades;
d) Conter: limitar a extensão de dados em uma adversidade.

29. Princípios de *design* da resiliência cibernética

29.1 Para alcançar os objetivos a estratégia de resiliência cibernética deve estar baseada em 5 (cinco) princípios fundamentais[15]:

a) Focalizar em ativos comuns e críticos

É fundamental a identificação de ativos usados em funções essenciais do negócio ou usados em múltiplos serviços de negócio para o desenvolvimento de planos de continuidade, recuperação e resposta aos ataques cibernéticos.

[13] NIST SP 800-160 v2 (11/2019) https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final.
[14] NIST SP 800-160 v2 (11/2019) https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final.
[15] NIST SP 800-160 v2 (11/2019) https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final

São comumente utilizadas nessa identificação metodologias como a MIA (*Mission Impact Analysis*) e BIA (*Business Impact Analysis*).

b) Ter suporte ágil e arquitetura para adaptabilidade

A agilidade, na resiliência cibernética, é definida pela capacidade dos componentes e os sistemas permitem reconfigurações para responder às adversidades ou serem reutilizados ou realocados de outras formas para a defesa em relação ao ataque.

A adaptabilidade deve estar inserida na arquitetura das soluções de maneira a permitir mudanças quer pelas ameaças apresentadas, quer pelas restrições tecnológicas ou operacionais.

Ou seja, esse princípio se refere à busca no *design* de soluções de pontos de fragilidades (pontos únicos de falha, canais de comunicação únicos, tecnologias proprietárias, entre outros).

c) Reduzir a superfície de ataque

A superfície de ataque se refere ao conjunto de pontos na fronteira de um sistema em que um atacante pode realizar uma tentativa de acesso.

São pontos que podem propiciar a exploração de vulnerabilidade por parte dos adversários, como um *hardware*, um *software*, uma conexão, uma mídia removível ou mesmo um serviço. Busca-se a redução tanto em extensão como na imposição de camadas de controle para acesso a um recurso, a redução de duração (como na implementação de *tokens* de conexão temporários) e a redução de abertura (como na implantação de estratégia de privilégio mínimo).

Esse princípio, aplicado aos ativos críticos e comuns, permite traçar estratégias para proteção do acesso aos recursos essenciais da empresa.

d) Assumir que recursos serão comprometidos

Entre os diversos componentes de *hardware*, *software*, processos, serviços é razoável estabelecer como premissa, durante um período, que alguma parte será comprometida.

Esse princípio define a necessidade de avaliação constante dos recursos para medição da extensão e da velocidade dos prejuízos a que esse comprometimento pode alcançar.

São utilizadas técnicas de modelagem e simulação de impacto para aplicação desse princípio da estratégia de segurança cibernética.

e) Esperar que os adversários evoluam

Atacantes têm investido recursos em desenvolver novas técnicas, táticas e procedimentos. As organizações também devem fazer o mesmo para conhecer a perspectiva do atacante a fim de melhorar as suas defesas.

Para implementação desse princípio, deve-se buscar o conhecimento de *frameworks* de ataque como o MITRE ATT&CK[16] e a implementação de times de ataque (*red team*) e jogos de guerra (*war gaming*).

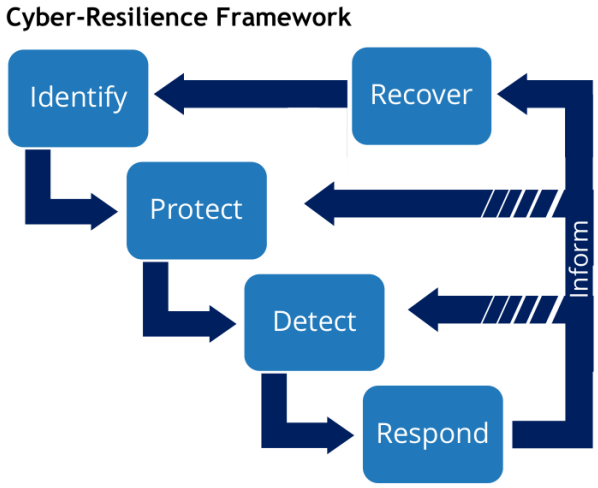
30. *Framework* de resiliência cibernética

30.1 Um *framework* de resiliência cibernética possui os seguintes componentes[17].

a) Identificar: ativo crítico e comuns, mapeamento de processo, avaliação de risco e prontidão para resposta;
b) Proteger: mecanismos de segurança de primeira linha de defesa;
c) Detectar: análise de segurança; verificação de integridade de dados de configuração/reconfiguração de ativos em tempo real;
d) Responder: resposta a violações ou falhas de segurança; e
e) Recuperar: mecanismos coordenados de recuperação.

Figura 1 – *Cyber resilience framework*[18]

[16] https://attack.mitre.org
[17] IDC (10/2020). Five Key Technologies for Enabling a Cyber-Resilience Framework.
[18] IDC (10/2020). Five Key Technologies for Enabling a Cyber-Resilience Framework (https://www.ibm.com/downloads/cas/YBDGKDXO).



Fonte: *International Data Corporation* (IDC) em 2020.

31. Requisitos de resiliência cibernética

31.1 Com base nas metas, nos objetivos, nos princípios e no *framework* apresentados, estabelecem-se requisitos para um ambiente de segurança cibernética resiliente (IDC, 2020).

32. Da identificação

32.1 Espera-se que na organização:

a) Exista inventário e base de configuração de todos os itens de TIC, cujos atributos dos itens de configuração evidenciem quais ativos são considerados críticos ou de múltiplo uso pela organização;
b) Exista uma base centralizada de processos da organização, de forma que os processos essenciais possam ser evidenciados e priorizados;
c) Exista um processo de gerenciamento de risco cibernético, com a precificação desse risco, que demonstre o impacto para a organização da exploração das vulnerabilidades, considerando também seus fornecedores;
d) Declare-se o nível de exposição ao risco, também com base no risco cibernético;
e) Exista mapeamento das comunicações e dos fluxos de dados da organização;

f) Existam papéis e políticas de segurança cibernética estabelecidas e comunicadas para o quadro próprio e de fornecedores;

g) Exista processo de identificação e documentação das vulnerabilidades dos seus ativos;

h) Exista processo de buscas e compartilhamento de informações sobre inteligência de ameaças.

33. Da proteção

33.1 Espera-se que na organização:

a) Identidades e credenciais sejam emitidas, gerenciadas, verificadas, revogadas e auditadas para dispositivos, usuários e processos;

b) Usuários, dispositivos e outros ativos sejam autenticados de acordo com o risco da transação (por exemplo, riscos de privacidade e segurança dos indivíduos e outros riscos organizacionais) e que, sempre que possível, se possuam múltiplos fatores de autenticação habilitados para acesso de usuários aos sistemas de informações;

c) Identidades sejam verificadas e vinculadas a credenciais e afirmadas nas interações. Esse processo deve apresentar soluções de validações de *tokens* em período regulares de tempo de acordo com a criticidade das transações;

d) O acesso físico aos ativos seja gerenciado e protegido, possuindo-se mecanismos de segurança de perímetro, como *firewalls*, *Intrusion Prevention Systems* (IPS) e *Web Application Firewall* (WAF) para restrição de acessos não autorizados;

e) Existam gerenciamento de acessos remotos e tecnologia de implementações de rede privada, se possível com certificados pessoais e por dispositivos, para garantia de controle legítimo;

f) Permissões de acesso e autorizações sejam gerenciadas, incorporando os princípios de privilégio mínimo e separação de funções. Que acessos administrativos sejam ofertados somente quando necessário e por tempo limitado;

g) A integridade da rede seja protegida por meio da segmentação e segregação de ambientes, de maneira a estabelecer barreiras de contenção de danos em caso de comprometimento (sub-redes distintas por serviços) e para garantia de recursos para serviços prioritários (missão crítica, em detrimento de ambientes de laboratório/desenvolvimento/homologação);

h) Existam programas de conscientização e treinamento dos funcionários, inclusive da alta administração, demonstrando os papéis e a responsabilidade de cada colaborador e colaboradora da organização quanto aos aspectos de segurança cibernética;

i) Sejam conhecidos pela alta administração os procedimentos a serem adotados em cenários de crise cibernética;

j) Existam processos que busquem a garantia de capacidade, disponibilidade e desempenho. Os dados devem estar protegidos tanto em repouso quanto em trânsito. Deve existir solução de proteção contra vazamento de dados;

k) *Backups* de dados e informações de configuração sejam realizados, mantidos e testados, e exista política para destruição adequada dos dados e das mídias que os suportem;

l) Exista processo de gerenciamento de mudanças para todos os ativos de TIC;

m) Mecanismos de verificação de integridade sejam implementados para verificar a integridade de *hardware*, *software*, *firmware* e informação;

n) Seja mantida uma linha de base de configuração dos ativos de tecnologia da informação, incorporando-se princípios de segurança;

o) Exista um processo de gerenciamento de ciclo de vida das aplicações; que o processo de desenvolvimento de aplicações possua características de segurança desde o desenho e a esteira de desenvolvimento; haja homologação e implementação possuam análise de ferramentas de segurança;

p) Exista um processo de melhoria contínua das soluções de proteção;

q) Sejam implementados, testados e gerenciados os planos de resposta (Resposta a Incidentes e Continuidade de Negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Desastres);

r) Manutenção e reparo de ativos, presenciais ou remotas, sejam registrados em *log*, se possível, utilizando-se ferramentas para aprovação e controle das atuações;

s) Existam registros de auditoria (*log*), devidamente documentados e revisados de acordo com a política específica;

t) As mídias removíveis sejam protegidas e seu uso seja restrito de acordo com a política específica; e

u) A comunicação de rede deve ser protegida e controlada.

34. Da detecção

34.1 Espera-se que na organização:

a) Sejam implementados mecanismos (alta disponibilidade, balanceamento de carga, *hot swap*) para atingir os requisitos de resiliência em situações adversas;

b) Sejam estabelecidas linhas de base de operações de rede e fluxos de dados esperados para usuários e sistemas. Se possível, implementando sistemas do tipo *Endpoint Detection and Response* (EDR) e *User and Entity Behavioral Analysis* (UEBA) para avaliação do comportamento de usuários e sistemas;

c) Os eventos detectados sejam analisados a fim de se compreender os alvos e métodos dos ataques;

d) Os dados de eventos sejam coletados e correlacionados a partir de várias fontes e sensores. Sugere-se utilizar solução de *Security Information and Event Management* (SIEM) para auxiliar no correlacionamento de eventos;

e) Existam *thresholds* e regras para geração de incidentes a partir dos eventos coletados;

f) Exista monitoramento específico de segurança cibernética para o ambiente físico, a rede e as atividades pessoais a fim de se detectar eventos;
g) Exista processo de detecção de códigos maliciosos;
h) Sejam realizados escaneamentos de vulnerabilidades frequentemente;
i) Seja realizado monitoramento de pessoal, conexões, dispositivos e *softwares* não autorizados;
j) A atividade do provedor de serviço externo seja monitorada para detectar potenciais eventos de segurança cibernética;
k) Exista processo de comunicação dos eventos detectados;
l) Os processos de detecção de eventos devem ser testados frequentemente;
m) Os processos de detecção sejam melhorados continuamente.

35. Da resposta

35.1 Espera-se que na organização:

a) Exista um plano de resposta a ser executado durante e após um incidente, e que a comunicação de incidentes ocorra de acordo com a política estabelecida, envolvendo a alta administração quando houver comprometimento de imagem;
b) Todas as notificações de detecção de ameaças sejam investigadas;
c) Os incidentes sejam classificados de forma consistente de acordo com política específica;
d) Os incidentes devem ser contidos ou mitigados no menor tempo possível;
e) Realize-se investigação forense dos incidentes de segurança cibernética;
f) Existam processos estabelecidos para receber, analisar e responder às vulnerabilidades divulgadas à organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança ou pesquisadores de segurança);
g) O plano de resposta incorpore as lições aprendidas e que as estratégias de resposta sejam constantemente atualizadas.

36. Da recuperação

36.1 Espera-se que na organização:

a) Exista um plano de recuperação a ser executado durante ou após um incidente de segurança cibernética;
b) Exista gerenciamento de comunicação com o público e um plano de recuperação de reputação após incidentes;
c) O plano de recuperação incorpore as lições aprendidas e seja constantemente testado e atualizado.

37. *Checklist*

37.1 Após definida a estratégia de segurança cibernética da organização, espera-se que sejam estipuladas metas de atendimento/implantação desses recursos, com acompanhamento pela alta administração.

37.2 No caso de adequação de dependências descentralizadas ou distribuídas geograficamente pelo país, o ideal é definir o tempo de adequação que cada uma terá que atender, possibilitando o apoio centralizado da área de segurança da empresa.
Considerando que as tecnologias mudam rapidamente e que as ameaças cibernéticas crescem exponencialmente não haverá momento de "relaxamento" no atendimento desses requisitos mínimos num futuro próximo.

Recomenda-se que a aplicação dos *checklists* ou das listas de autoverificação implementadas pela organização seja periódica (sugere-se no mínimo periodicidade anual) e que sejam estabelecidos níveis de maturidade nessa avaliação. O objetivo é possibilitar a melhoria contínua dos normativos, dos processos e das iniciativas em segurança cibernética da organização.

O quadro a seguir apresenta uma sugestão de níveis de maturidades a serem empregados.

Definição	Descrição
1 – Não observado ou inicial	Fator não foi demonstrado claramente
2 – Maturidade baixa ou em desenvolvimento	Fator demonstrado claramente, mas não integrado
3 – Maturidade média ou definida	Fator suficientemente demonstrado, integrado, mas não está medido
4 – Maturidade alta ou gerenciada	Fator constantemente demonstrado, integrado, gerenciado, mas não possui melhoria contínua
5 – Melhoria contínua ou otimizada	Fator complemente demonstrado, integrado, gerenciado e continuamente melhorado.

No Anexo I serão apresentados controles sugeridos para o presente Manual.

38. Anexo I – modelo de *checklist*

Checklist de controles para prevenção e mitigação de ameaças cibernéticas e confiança digital

N.	Item	Referencial	Maturidade				
			1	2	3	4	5
1.	Padrões mínimos de Gestão de Riscos de Segurança da Informação						
1.1.	Existe um Processo de Gestão de Riscos de Segurança Cibernética estabelecido.	NBR 27.005:2019					
1.2.	O Processo de Gestão de Riscos de Segurança Cibernética é chancelado pela administração superior.	NBR 27.005:2019					
1.3.	O Processo de Gestão de Riscos de Segurança Cibernética está associado ao Sistema de Gestão de Segurança da Informação.	NBR 27.005:2019					
1.4.	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Estabelecimento de Contexto definida.	NBR 27.005:2019					
1.5.	O Processo de Gestão de Riscos de Segurança Cibernética possui um subprocesso de Avaliação de Riscos definido.	NBR 27.005:2019					
1.5.1.	O subprocesso de Avaliação de Riscos contempla atividade de Identificação de Riscos.	NBR 27.005:2019					
1.5.2.	O subprocesso de Avaliação de Riscos contempla atividade de Análise de Riscos.	NBR 27.005:2019					
1.5.3.	O subprocesso de Avaliação de Riscos contempla atividade de Avaliação de Riscos.	NBR 27.005:2019					
1.5.4.	Critérios para determinação do impacto/criticidade e probabilidade dos riscos de segurança cibernética estão definidos.	NBR 27.005:2019					
1.5.5	Critérios para aceitação de riscos de segurança cibernética estão definidos.	NBR 27.005:2019					
1.6.	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Tratamento de Riscos definida.	NBR 27.005:2019					
1.7.	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Monitoramento e Análise Crítica definida.	NBR 27.005:2019					
1.8.	O Processo de Gestão de Riscos de Segurança Cibernética possui atividade de Comunicação e Consulta definida.	NBR 27.005:2019					
1.9.	O Processo de Gestão de Riscos de Segurança Cibernética é periodicamente revisado e atualizado.	NBR 27.005:2019					
2.	Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas						
2.1.	Considerar para, determinação de objetivos, no planejamento anual do programa interno de auditorias do órgão: requisitos de segurança da informação legais, normativos e contratuais, riscos de segurança da informação para as áreas auditadas e clientes da auditoria e, quando aplicável, riscos e oportunidades determinados no fase de planejamento do sistema de gestão de segurança da informação.	ISO 27007:2018					

2.2.	Para determinar a abrangência e as prioridades das auditorias sobre requisitos de segurança, considerar: complexidade dos sistemas a serem auditados, número de localidades similares, importância da preservação da confidencialidade, integridade e disponibilidade das informações e riscos para o negócio. Quando aplicável, considerar tamanho, complexidade e riscos para o sistema de gestão de segurança da informação.	ISO 27007:2018					
2.3.	Considerar na avaliação de riscos de execução das auditorias requisitos legais, normativos e contratuais de confidencialidade e outros tipos, se relevantes.	ISO 27007:2018					
2.4.	Utilizar termos de confidencialidade, técnicas de anonimização e cláusulas contratuais específicas quando requerido por auditados e outras partes pertinentes.	ISO 27007:2018					
2.5.	Estabelecer um cronograma de trabalho das auditorias que permitam uma análise crítica dos auditores sobre a eficácia das ações de abordagem de riscos de segurança da informação e, quando aplicável, ao sistema de gestão de segurança da informação.	ISO 27007:2018					
2.6.	Considerar como possíveis objetivos de uma auditoria individual, quando aplicável, considerando o escopo de um sistema de gestão de segurança da informação: avaliar se o órgão identifica e aborda os requisitos de segurança da informação, avaliar processos que suportam os requisitos de segurança da informação e determinar a abrangência da conformidade controles de segurança da informação com os requisitos e procedimentos determinados.	ISO 27007:2018					
2.7.	Considerar os riscos de segurança da informação na determinação do escopo de uma auditoria individual e, quando aplicável, os riscos para o sistema de gestão de segurança da informação.	ISO 27007:2018					
2.8.	Considerar como critérios de uma auditoria individual para determinar a conformidade com requisitos de segurança, quando aplicáveis: política de segurança da informação; objetivos da segurança da informação; políticas e procedimentos adotados pelo auditado; requisitos legais normativos, contratuais e outros relevantes para o auditado; critérios de riscos de segurança da informação do auditado e os processos de avaliação e tratamento de riscos; justificativas para inclusão e exclusão de controles para atendimentos de requisitos ou ao estabelecimento de um sistema de gestão de segurança da informação; definição de controles para tratamento apropriado de riscos de segurança da informação; método e critérios usados para monitoramento, medição, análise e avaliação de desempenho da gestão de segurança da informação ou do sistema de gestão de segurança da informação; requisitos de segurança da informação de clientes, fornecedores ou terceirizados.	ISO 27007:2018					
2.9.	No caso de auditorias integradas/compartilhadas, conjuntas, contratadas ou cruzadas providenciar, necessariamente, contrato, termos de cooperação técnica, convênios ou instrumento que formalize a prestação da auditoria nos moldes especificados e, obrigatoriamente, acompanhados dos devidos acordos de confidencialidade assinados pelas partes envolvidas.	ISO 27007:2018					
2.10.	Incluir no conhecimento global da equipe de auditoria conhecimentos sobre gestão de riscos de segurança da informação, suficiente para avaliar métodos usados, e gestão de segurança da informação, suficiente para avaliar a implementação de requisitos de segurança da informação, ou, quando aplicável, o funcionamento de um sistema de gestão de segurança da informação.	ISO 27007:2018					

2.11.	No contato inicial com o auditado comprovar, por instrumento apropriado, que os auditores obtiveram autorização para acessos às informações necessárias para a auditoria.	ISO 27007:2018					
2.12.	Determinar e formalizar a inviabilidade ou comprometimento de algum aspecto da auditoria no caso de negação de acesso pelo auditado às evidências que contemplem informações sensíveis ou sigilosas.	ISO 27007:2018					
2.13.	Conscientizar a equipe de auditoria, especialmente o auditor líder, que a atividade de auditoria implica ampliação de riscos das informações do auditado (vazamento, exclusão acidental, alteração intencional, indisponibilidade de serviço etc.).	ISO 27007:2018					
2.14.	Acordar, com as áreas envolvidas e impactadas, por meio do auditor líder, melhor cronograma para interrupções e perda de desempenho de serviços, quando imprescindíveis para as atividades de auditoria.	ISO 27007:2018					
2.15.	Equipe de auditoria classificar e tratar documentos de trabalho de acordo com suas classificações originais quanto a sigilo ou à sensibilidade.	ISO 27007:2018					
2.16.	Equipe de auditoria validar documentação de trabalho de acordo com escopo e critérios da auditoria, confirmando se os controles estão relacionados com os processos de análise e tratamento de riscos e se são rastreáveis em relação aos objetivos e política de segurança da informação.	ISO 27007:2018					
2.17.	Basear a coleta e validação de informações e técnicas de auditoria de TIC, que incluem: análise crítica de informação documentada (*logs*, trilhas, arquivos, massas de dados, configurações etc.), visitas às instalações de processamento de informações para inspeção visual, observação de processo e controles relacionados aos requisitos de segurança da informação e, quando aplicável, ao sistema de gestão de segurança da informação e uso de ferramentas automatizadas de auditoria.	ISO 27007:2018					
2.18.	Não comprometer a classificação ou sensibilidade de uma evidência em razão da indisponibilidade desta para avaliação da auditoria. O auditor líder deve tratar o assunto no relatório de auditoria, incluindo o impacto nos resultados causado pela ausência da evidência.	ISO 27007:2018					
2.19.	Adotar medidas para garantir a confidencialidade do relatório, incluindo a encriptação dele quando em meio eletrônico.	ISO 27007:2018					
2.20.	Selecionar auditores para auditorias tomando como base inclusive: quando aplicável, tipos de negócios suportados, complexidade, abrangência, diversidade tecnológica e avaliações anteriores do sistema de gestão de segurança da informação ou relacionados aos requisitos de segurança auditados; abrangência de acordos e contratos com terceiros relacionados aos requisitos de segurança ou, quando aplicável, ao escopo do sistema de gestão de segurança da informação; normas, requisitos legais e outros requisitos do programa de auditoria.	ISO 27007:2018					
2.21.	Incluir no plano de capacitação de auditores conhecimentos sobre tecnologia da informação, segurança da informação e conhecimentos inerentes aos requisitos de negócio da organização, inclusive legais, normativos e contratuais.	ISO 27007:2018					

2.22.	Avaliar a conformidade de requisitos de segurança da informação por meio de auditorias de forma contínua e planejada com o objetivo de apoiar o aperfeiçoamento da gestão de segurança da informação no órgão, garantir a conformidade legal, normativa e contratual sobre segurança da informação e com requisitos de referência sobre boas práticas de segurança da informação e gestão de segurança da informação.	NC 11 IN01/DSIC/GSIPR					
2.23.	No que diz respeito às auditorias de segurança da informação, basear o planejamento do programa de auditorias na análise e avaliação de riscos.	NC 11 IN01/DSIC/GSIPR					
2.24.	No que diz respeito ao planejamento da auditoria individual de segurança da informação, considerar a análise e avaliação de riscos na determinação de escopo e objetivos da auditoria.	NC 11 IN01/DSIC/GSIPR					
2.25.	Entregar o relatório da auditoria individual para a alta administração do órgão e, quando existente, para o gestor de segurança da informação do órgão.	NC 11 IN01/DSIC/GSIPR					
2.26.	Adequar, de forma geral ou específica para segurança da informação, normativos internos dos órgãos para admitir as formas de auditoria: terceirizada (executada por terceirizado contratado), integrada/compartilhada (área de auditoria de um órgão audita o outro órgão com a participação da área de auditoria do auditado) e, quando previsto em normativo próprio do Poder Judiciário, cruzada (área de auditoria de um órgão audita o outro órgão sem a participação da área de auditoria do auditado).	Res. 309 de 11/03/2020 do CNJ					
2.27.	Em relação aos requisitos de segurança da informação, considerar nos planejamentos dos programas de auditoria e das auditorias individuais as auditorias nas formas: terceirizada (executada por terceirizado contratado), integrada/compartilhada (área de auditoria de um órgão audita o outro órgão com a participação da área de auditoria do auditado) ou, quando previsto em normativo próprio do Poder Judiciário, cruzada (área de auditoria de um órgão audita o outro órgão sem a participação da área de auditoria do auditado).	Res. 309 de 11/03/2020 do CNJ					
3.	Confiança digital, prevenção e mitigação de ameaças cibernéticas						
3.1.	A organização possui mecanismos de resiliência cibernética que implementam uma fase de identificação de ameaças.	*Framework* de resiliência cibernética. IDC, 2020.					
3.2.	A organização possui mecanismos de resiliência cibernética que implementam uma fase de proteção de ativos.	*Framework* de resiliência cibernética. IDC, 2020.					
3.3.	A organização possui mecanismos de resiliência cibernética que implementam uma fase de detecção de ameaças.	*Framework* de resiliência					

		cibernética. IDC, 2020.					
3.4.	A organização possui mecanismos de resiliência cibernética que implementam uma fase de respostas a ameaças.	*Framework* de resiliência cibernética. IDC, 2020.					
3.5.	A organização possui mecanismos de resiliência cibernética que implementam uma fase de recuperação.	*Framework* de resiliência cibernética. IDC, 2020.					