Poder Judiciário

Conselho Nacional de Justiça

ANEXO I DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

Protocolo – Prevenção de Incidentes Cibernéticos do Poder Judiciário

Protocolo

Prevenção de Incidentes Cibernéticos do Poder Judiciário

Material de referência com as principais diretrizes necessárias para implantação do protocolo de prevenção de incidentes cibernéticos do Poder Judiciário

Sumário

1. Escopo 7
2. Funções básicas 7
3. Princípios críticos 8
4. Gestão de Incidentes de Segurança da Informação 9
5. Competência de atuação 9
6. Funcionamento da ETIR 10
7. Boas Práticas de Segurança Cibernéticas 10

Protocolo de Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ)

1. Escopo

1.1 O PPINC-PJ contemplará um conjunto de diretrizes para a prevenção a incidentes cibernéticos em seu mais alto nível.

1.2 As diretrizes serão divididas em funções que expressem a gestão do risco organizacional e que permitam as decisões adequadas para o enfrentamento de ameaças e a melhor gestão de práticas e de metodologias existentes.

1.3 As diretrizes poderão ser adaptadas, incrementadas ou ajustadas, considerando-se a realidade de cada órgão do Poder Judiciário.

2. Funções básicas

2.1 São funções básicas do PPINC-PJ: identificar, proteger, detectar, responder e recuperar, nos seguintes termos:

2.1.1 **identificar:** entendimento organizacional para gerenciar o risco direto e/ou indireto de ataques cibernéticos a sistemas, pessoas, ativos, dados e recursos. Permite ao órgão avaliar os recursos que suportam funções críticas e os riscos relacionados. São medidas de concentração e priorização dos esforços na gestão de ativos, ambiente de negócios, governança, avaliação de riscos e estratégia de gestão de riscos.

2.1.2 **proteger:** desenvolvimento e implementação de salvaguardas que assegurem a proteção de dados, inclusive pessoais, e de ativos de informação, bem como a prestação de serviços críticos.

2.1.3 **detectar:** desenvolvimento e implementação de atividades adequadas à descoberta oportuna de eventos ou à detecção de incidentes de segurança cibernética. Estão contempladas ações de monitoramento contínuo de segurança, processos de detecção de anomalias e eventos.

2.1.4 **responder:** desenvolvimento e implementação de atividades apropriadas à adoção de medidas em incidentes cibernéticos detectados. Nessa categoria, são

incluídos os planos de resposta, de comunicações, de análise, de mitigação e de melhorias.

2.1.5 recuperar: desenvolvimento, implementação e manutenção dos planos de resiliência e de restauração de quaisquer capacidades ou serviços que foram prejudicados em razão de incidentes de segurança cibernética.

3. Princípios críticos

3.1 O protocolo de prevenção a incidentes cibernéticos criado no âmbito de cada tribunal contemplará um conjunto de princípios críticos que assegurem a construção de sistema de segurança cibernética eficaz.

3.2 São princípios críticos que podem ser adaptados, incrementados ou ajustados, considerada a realidade de cada órgão do Poder Judiciário:

3.2.1 base de conhecimento de defesa: consiste no uso de informações e conhecimento de ataques reais que comprometeram sistemas. Informações conseguidas por meio de interação e de cooperação com outras equipes de tratamento a incidentes e respostas. Tem por propósito fornecer bases fundamentais ao aprendizado contínuo com apoio em eventos ocorridos. Apoia a construção de defesas eficazes e práticas.

3.2.2 priorização: foco prioritário na formação, na revisão de controles/acessos, nos processos e na disseminação da cultura de segurança cibernética. Contribui para a redução de riscos e para a proteção contra as ameaças mais sensíveis e que encontram viabilidade em sua célere implementação.

3.2.3 instrumentos de medição e métricas: definição e estabelecimento de métricas comuns que fornecem linguagem compartilhada e de compreensão abrangente para magistrados, servidores, colaboradores, prestadores de serviços, especialistas em tecnologia da informação, auditores e demais atores do sistema de segurança. Permite a medição da eficácia das medidas de segurança dentro da organização. Fornece insumos para que os ajustes necessários, quando identificados, possam ser implementados de forma célere.

3.2.4 **diagnóstico contínuo:** processo de trabalho que realiza continuamente medição para testar e validar a eficácia das medidas de segurança atuais e contribui para a definição de prioridades e para os próximos passos a serem tomados.

3.2.5 **formação, capacitação e conscientização:** processos formais de educação continuada com a inclusão em planos de capacitação que contemplem a disseminação, a formação, a conscientização e a instrução para todos os atores envolvidos em atividades diretas ou indiretas que contribuam para a cultura de segurança cibernética dentro da organização. Tais instrumentos deverão ser revisados periodicamente.

3.2.6 **automação:** incentivo à busca de soluções automatizadas de segurança cibernética para que as organizações obtenham medições confiáveis, escaláveis e contínuas. Tal processo está correlacionado com os resultados almejados por meio dos instrumentos de controle e de métricas**.**

3.2.7 **resiliência:** poder de recuperação ou capacidade de a organização resistir aos efeitos de um incidente, bem como impedir a reincidência secundária do incidente identificado.

4. Gestão de Incidentes de Segurança Cibernética

4.1 A gestão de incidentes de segurança cibernética é realizada por meio de processo definido e constituída formalmente, contendo as fases de detecção, triagem, análise e resposta aos incidentes de segurança.

5. Competência de atuação

5.1 Deverá ser formalmente instituída Equipe de Tratamento e Resposta a Incidentes de Segurança Cibernética (ETIR), em todos os órgãos do Poder Judiciário, à exceção do STF.

5.2 A ETIR poderá solicitar apoio multidisciplinar para responder aos incidentes de segurança de maneira adequada e tempestiva, em áreas como: tecnologia da informação, segurança da informação, jurídica, pesquisas judiciárias, comunicação, controle interno, segurança institucional, entre outras.

5.3 Caberá a cada órgão do Poder Judiciário avaliar o adequado posicionamento da ETIR em seu organograma institucional, considerando-se seu desenho organizacional e suas peculiaridades.

5.4 A ETIR terá autonomia compartilhada, ou seja, participará do resultado da decisão recomendando os procedimentos a serem executados ou as medidas de recuperação durante a identificação de uma ameaça e debaterá sobre as ações a serem tomadas, seus impactos e a repercussão, caso as recomendações não sejam seguidas.

6. Funcionamento da ETIR

6.1 O funcionamento da ETIR é regulado por documento formal de constituição, publicado no sítio eletrônico do respectivo órgão, devendo constar, no mínimo, os seguintes pontos:

a) definição da missão;
b) público-alvo;
c) modelo de implementação;
d) nível de autonomia;
e) designação de integrantes;
f) canal de comunicação de incidentes de segurança; e
g) serviços que serão prestados.

7. Boas Práticas de Segurança Cibernéticas

7.1 A segurança cibernética é um empreendimento coletivo.

7.2 Para melhor detectar, conter e eliminar ataques cibernéticos e minimizar eventuais impactos na operação, assegurando o funcionamento dos sistemas críticos do Poder Judiciário, sobretudo em ambiente de constante ameaça, é necessário que todos os seus órgãos possuam mecanismos de respostas e prevenção.

7.3 A prevenção a incidentes contempla funções de preparação, identificação, contenção, erradicação, recuperação e lições aprendidas.

7.4 As dimensões e práticas poderão ser adaptadas, incrementadas ou ajustadas conforme a realidade de cada órgão.

7.5 São assim definidas as dimensões e práticas da segurança cibernética:

7.5.1 **preparação:** processo que envolve as equipes de tratamento a incidentes e respostas. Trata-se de resposta metódica, contemplando ferramentas forenses de análise e custódia, planejamento sobre como responder e notificar cada incidente de segurança, identificação de cadeia de comando em situação de crise, processos de educação e de formação.

7.5.2 **identificação:** capacidade de identificar que um ataque cibernético está em andamento, por meio da percepção de sinais de anomalias ou de comportamentos inesperados. Trata-se da aptidão dos entes para diferenciar as irregularidades em redes de dados e identificar o mau funcionamento dos sistemas críticos, em razão de ataques cibernéticos em curso. Para essa atividade, podem ser elaboradas listas de verificação investigativas para apoiar o processo de diagnóstico, triagem e acionamento das equipes de resposta, permitindo a avaliação do impacto e a determinação dos próximos passos a serem tomados.

7.5.3 **contenção:** visa a garantir que o incidente não cause mais danos. Nessa dimensão, a prioridade geral é isolar o que foi afetado, manter a produção e, acima de tudo, garantir que as ações não comprometam, ainda mais, a segurança ou as operações críticas. Tal atividade tende a ser complexa incluindo, dentre outros, a imediata comunicação prevista na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSECPJ) e seus anexos, o isolamento da fonte do ataque, a aplicação de ferramentas forenses para remoção de *malware* das redes de produção, a limitação de transferências de dados desnecessárias e a adoção dos mecanismos de comunicação previstos no Protocolo de Gerenciamento de Crises Cibernéticas.

7.5.4 **erradicação:** remoção da ameaça, garantindo que as operações essenciais sejam apoiadas, caso surjam desafios no processo de restauração. Os métodos possíveis para essa função podem variar desde patches ou reconstruções do sistema até redesenho completo da arquitetura, devendo, sempre que possível, preservar evidências que apoiarão o processo de investigação do crime cibernético.

7.5.5 **recuperação:** promulgação de plano de recuperação em fases para restauração de operações, com foco prioritário nos sistemas críticos ou na execução da operação em modo analógico até que haja confiança no desempenho do sistema. Nessa atividade, são necessárias verificações ambientais e de segurança paralelas ao controle dos impactos de desempenho não intencionais da restauração.

7.5.6 **lições aprendidas:** atividade contínua que não só deve capturar os impactos imediatos de um incidente, mas também as melhorias em longo prazo da segurança cibernética do órgão. Tal função pode variar de um sistema de controle de processos melhor projetado até a evolução e preparação de centros de identificação e resposta a ataques cibernéticos do Poder Judiciário.

ANEXO II DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

Protocolo – Gerenciamento de Crises Cibernéticas do Poder Judiciário

Protocolo

Gerenciamento de Crises Cibernéticas do Poder Judiciário

Material de referência com as principais diretrizes para implantação do protocolo de gerenciamento de Crises Cibernéticas do Poder Judiciário

Sumário

1. Escopo 15
2. Identificação de Crise Cibernética 15
3. Fases do Gerenciamento de Crises 15
4. Planejamento da Crise (pré-crise) 15
5. Execução (durante a crise) 17
6. Melhoria contínua (lições aprendidas no pós-crise) 19
7. Exemplo de Plano de Gestão de Incidentes Cibernéticos 19

Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ)

1. Escopo

1.1. O Protocolo de Gerenciamento de Crises Cibernéticas do Poder Judiciário é complementar ao Protocolo de Prevenção de Incidentes Cibernéticos e prevê as ações responsivas a serem colocadas em prática quando ficar evidente que um incidente de segurança cibernética não será mitigado rapidamente e poderá durar dias, semanas ou meses.

2. Identificação de Crise Cibernética

2.1. O gerenciamento de incidentes se refere às atividades que devem ser executadas para avaliar o problema e determinar a resposta inicial diante da ocorrência de um evento adverso de segurança da informação.

2.2. O gerenciamento de crise se inicia quando:

a) ficar caracterizado grave dano material ou de imagem;

b) restar evidente que as ações de resposta ao incidente cibernético provavelmente persistirão por longo período, podendo se estender por dias, semanas ou meses;

c) o incidente impactar a atividade finalística ou o serviço crítico mantido pela organização; ou

d) o incidente atrair grande atenção da mídia e da população em geral.

3. Fases do Gerenciamento de Crises

3.1 O Gerenciamento de Crises pode ser dividido em 3 (três) fases:

a) planejamento (pré-crise);

b) execução (durante a crise); e

c) melhoria Contínua (pós-crise).

4. Planejamento da Crise (pré-crise)

4.1 Para melhor lidar com uma crise cibernética, é necessário prévia e adequada preparação, sendo fundamental que os órgãos do Poder Judiciário estabeleçam um Programa de Gestão da Continuidade de Serviços que contemple as seguintes atividades:

a) observar o Protocolo de Prevenção a Incidentes Cibernéticos do Poder Judiciário;
b) definir as atividades críticas que são fundamentais para a atividade finalística do órgão;
c) identificar os ativos de informação críticos, ou seja, aqueles que suportam as atividades primordiais, incluindo as pessoas, os processos, a infraestrutura e os recursos de tecnologia da informação;
d) avaliar continuamente os riscos a que as atividades críticas estão expostas e que possam impactar diretamente na continuidade do negócio;
e) categorizar os incidentes e estabelecer procedimentos de resposta específicos (*playbooks*) para cada tipo de incidente, de forma a apoiar equipes técnicas e de liderança em casos de incidentes cibernéticos;
f) priorizar o monitoramento, acompanhamento e tratamento dos riscos de maior criticidade. Tais atividades deverão ser detalhadas e consolidadas em um plano de contingência que contemple diversos setores, em razão de possíveis cenários de crise, a fim de se contrapor à escalada de uma eventual crise e com o objetivo de manter os serviços prestados pela organização; e
g) realizar simulações e testes para validação dos planos e procedimentos.

4.2 Deve-se definir a sala de situação e criar um Comitê de Crises Cibernéticas, composto por representantes da alta administração e por representantes executivos, com suporte da ETIR e de especialistas:

a) da área Jurídica;
b) da área de Comunicação Institucional;
c) da área de Tecnologia da Informação e Comunicação;
d) da área de Privacidade de Dados Pessoais;
e) da área de Segurança da Informação;
f) das unidades administrativas de apoio à contratação; e
g) da área de Segurança Institucional.

4.3 O Plano de Gestão de Incidentes Cibernéticos deve possuir, no mínimo, as categorias de incidentes a que os ativos críticos estão sujeitos; a indicação do procedimento de resposta específico a ser aplicado em caso de ocorrência do incidente; e a severidade do incidente.

5. Execução (durante a crise)

5.1 A comunicação entre as áreas envolvidas é fator fundamental para uma organização reagir a uma crise cibernética de longa duração ou de grande impacto.

5.2 Assim que a ETIR identificar que um incidente constitui uma crise cibernética, o Comitê de Crise deverá se reunir imediatamente na sala de situação previamente definida.

5.3 Os planos de contingência existentes, caso aplicáveis, devem ser efetivados imediatamente, visando à continuidade dos serviços prestados.

5.4 A chefia do Comitê de Crise deve ficar a cargo de profissional, indicado pelo Presidente do respectivo órgão do Poder Judiciário, com autoridade e autonomia para tomar decisões sobre conteúdo de comunicação a serem divulgados, bem como delegar atribuições, estabelecer metas e prazos de ações.

5.5 A sala de situação é o local a partir do qual serão geridas as situações de crise, devendo dispor dos meios necessários (ex.: sistemas de áudio, vídeo, chamadas telefônicas) e estar preferencialmente próxima a um local onde se possa fazer declarações públicas à imprensa e com acesso restrito ao Comitê de Crise e a outros entes eventualmente convidados a participar das reuniões.

5.6 A sala de situação deve ser um ambiente que permita ao Comitê deliberar com tranquilidade e que possua uma equipe dedicada à execução de atividades administrativas para o período da crise.

5.7 Para eficácia do trabalho, é necessário o Comitê de Crise:

a) entender claramente o incidente que gerou a crise, sua gravidade e os impactos negativos;
b) levantar todas as informações relevantes, verificando fatos e descartando boatos;
c) levantar soluções alternativas para a crise, avaliando sua viabilidade e consequências;

d) avaliar a necessidade de suspender serviços e/ou sistemas informatizados;
e) centralizar a comunicação na figura de um porta-voz para evitar informações equivocadas ou imprecisas;
f) realizar comunicação tempestiva e eficiente, de forma a evidenciar o trabalho diligente das equipes e a enfraquecer boatos ou investigações paralelas que alimentem notícias falsas;
g) definir estratégias de comunicação com a imprensa e/ou redes sociais e estabelecer qual a mídia mais adequada para se utilizar em cada caso;
h) aplicar o Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário;
i) solicitar a colaboração de especialistas ou de centros de resposta a incidentes de segurança;
j) apoiar equipes de resposta e de recuperação com gerentes de crise experientes;
k) avaliar a necessidade de recursos adicionais extraordinários a fim de apoiar as equipes de resposta;
l) orientar sobre as prioridades e estratégias da organização para recuperação rápida e eficaz;
m) definir os procedimentos de compartilhamento de informações relevantes para a proteção de outras organizações com base nas informações colhidas sobre o incidente; e
n) elaborar plano de retorno à normalidade.

5.8 As etapas e os procedimentos de resposta são diferentes a depender do tipo de crise. Dessa forma, são necessárias reuniões regulares para avaliar o progresso até que seja possível retornar à condição de normalidade.

5.9 Todos os incidentes graves deverão ser comunicados ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ), órgão superior vinculado ao Conselho Nacional de Justiça.

6. Melhoria contínua (lições aprendidas no pós-crise)

6.1 Após o retorno das operações à normalidade, o Comitê de Crises Cibernéticas deverá realizar a análise criteriosa das ações tomadas, observando as que foram bem-sucedidas e as que ocorreram de forma inadequada.

6.2 Para a identificação das lições aprendidas e a elaboração de relatório final, devem ser objeto de avaliação:

a) a identificação e análise da causa-raiz do incidente;
b) a linha do tempo das ações realizadas;
c) a escala do impacto nos dados, sistemas e operações de negócios importantes durante a crise;
d) os mecanismos e processos de detecção e proteção existentes e as necessidades de melhoria identificadas;
e) o escalonamento da crise;
f) a investigação e preservação de evidências;
g) a efetividade das ações de contenção;
h) a coordenação da crise, liderança das equipes e gerenciamento de informações; e
i) a tomada de decisão e as estratégias de recuperação.

6.3 As lições aprendidas devem ser utilizadas para a elaboração ou revisão dos procedimentos específicos de resposta (*playbooks*) e para a melhoria do processo de preparação para crises cibernéticas.

6.4 Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, bem como o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados. Deve ser elaborado Relatório de Comunicação de Incidente de Segurança Cibernética, que contenha a descrição e o detalhamento da crise, e o plano de ação tomado para evitar que incidentes similares ocorram novamente ou para que, em caso de ocorrência, se reduzam os danos causados.

7. Exemplo de Plano de Gestão de Incidentes Cibernéticos

Item	Indicação do incidente cibernético	Descrição	Procedimento	Severidade
1	Campanha de *phishing*	O órgão é alvo de uma campanha de *phishing*.	Identificação do documento de procedimento de resposta específico.	Média
2	Degradação de serviços	Degradação ou interrupção de serviços ou sistemas por ataque de negação de serviço (DoS).	Identificação do documento de procedimento de resposta específico.	Alta
3	Comprometimento de credenciais	Comprometimento de credenciais com acesso a informações sensíveis.	Identificação do documento de procedimento de resposta específico.	Alta
4	Impossibilidade de acesso à informação	Importantes informações organizacionais inacessíveis por encriptação (*ransomware*).	Identificação do documento de procedimento de resposta específico.	Crítica
5	Vazamento de informação e dados pessoais	Informações críticas encontradas fora da organização.	Identificação do documento de procedimento de resposta específico.	Crítica

ANEXO III DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

Protocolo – Investigação para Ilícitos Cibernéticos do Poder Judiciário

Protocolo

Investigação para Ilícitos Cibernéticos do Poder Judiciário

Material de referência com as principais diretrizes necessárias para implantação do protocolo de investigação para Ilícitos Cibernéticos do Poder Judiciário

Sumário

1. Objetivo 2
2. Requisitos para Adequação dos Ativos de Informação 2
3. Procedimento para Coleta e Preservação das Evidências 4
4. Comunicação do Incidente de Segurança 5

Protocolo de Investigação para Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ)

1. Objetivo

1.1. O Protocolo de Investigação para Ilícitos Cibernéticos (PIILC-PJ) tem por finalidade estabelecer os procedimentos básicos para coleta e preservação de evidências e para comunicação obrigatória dos fatos penalmente relevantes ao Ministério Público e ao órgão de polícia judiciária com atribuição para o início da persecução penal.

2. Requisitos para Adequação dos Ativos de Tecnologia da Informação

2.1. O horário dos ativos de tecnologia da informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a Hora Legal Brasileira (HLB), de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

2.2. Os ativos de tecnologia da informação devem ser configurados de forma a registrar todos os eventos relevantes de Segurança da Informação e Comunicações (SIC), tais como:

a) autenticação, tanto as bem-sucedidas quanto as malsucedidas;
b) acesso a recursos e dados privilegiados; e
c) acesso e alteração nos registros de auditoria.

2.3. Os registros dos eventos previstos no item 2.2 devem incluir as seguintes informações:

a) identificação inequívoca do usuário que acessou o recurso;
b) natureza do evento, como, por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha etc.;
c) data, hora e fuso horário, observando-se a HLB; e

d) endereço IP (*Internet Protocol*), porta de origem da conexão, identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

2.4. Os ativos de informação que não propiciem os registros dos eventos listados no item 2.3. devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria permitidos e armazenados.

2.5. Os sistemas e as redes de comunicação de dados devem ser monitorados, registrando-se, minimamente, os seguintes eventos de segurança, sem prejuízo de outros considerados relevantes:

a) utilização de usuários, perfis e grupos privilegiados;
b) inicialização, suspensão e reinicialização de serviços;
c) acoplamento e desacoplamento de dispositivos de *hardware*, com especial atenção para mídias removíveis;
d) modificações da lista de membros de grupos privilegiados;
e) modificações de política de senhas, como, por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico etc.;
f) acesso ou modificação de arquivos ou sistemas considerados críticos; e
g) eventos obtidos por meio de quaisquer mecanismos de segurança existentes.

2.6. Os servidores de hospedagem de página eletrônica, bem como todo e qualquer outro ativo de informação que assim o permita, devem ser configurados para armazenar registros históricos de eventos (*logs*) em formato que possibilite a completa identificação dos fluxos de dados.

2.7. Os registros devem ser armazenados pelo período mínimo de 6 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

2.8. Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas localmente, mas também remotamente, por meio do uso de tecnologia aplicável.

3. Procedimento para Coleta e Preservação das Evidências

3.1. A ETIR, sob a supervisão de seu responsável, durante o processo de tratamento do incidente penalmente relevante, deverá, sem prejuízo de outras ações, coletar e preservar:

a) as mídias de armazenamento dos dispositivos afetados ou as suas respectivas imagens forenses;
b) os dados voláteis armazenados nos dispositivos computacionais, como a memória principal (memória RAM); e
c) todos os registros de eventos citados neste documento.

3.2. Nos casos de inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados ou das suas respectivas imagens forenses, em razão da necessidade de pronto restabelecimento do serviço afetado, a ETIR, sob a supervisão do seu responsável, deverá coletar e armazenar cópia dos arquivos afetados pelo incidente, tais como: *logs*, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original e os "metadados" desses arquivos, como data, hora de criação e permissões.

3.3. O agente responsável pela ETIR deverá fazer constar em relatório a eventual impossibilidade de preservação das mídias afetadas e listar todos os procedimentos adotados.

3.4. As ações de restabelecimento do serviço não devem comprometer a coleta e a preservação da integridade das evidências.

3.5. Para a preservação dos arquivos coletados, deve-se:

a) gerar arquivo que contenha a lista dos resumos criptográficos de todos os arquivos coletados;

b) gravar os arquivos coletados, acompanhados do arquivo com a lista dos resumos criptográficos descritos na alínea *a* deste subitem; e
c) gerar resumo criptográfico do arquivo a que se refere *a* deste subitem.

3.6. Todo material coletado deverá ser lacrado e custodiado pelo agente responsável pela ETIR, o qual deverá preencher Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança penalmente relevante.
3.7. O material coletado ficará à disposição da autoridade responsável pelo órgão do Poder Judiciário competente.

4.Comunicação do Incidente de Segurança

4.1. Assim que tomar conhecimento de Incidente de Segurança Cibernética penalmente relevante, deverá o responsável pelo órgão do Poder Judiciário afetado comunicá-lo de imediato ao órgão de polícia judiciária com atribuição para apurar os fatos e ao Ministério Público.
4.2. Considerado o incidente Crise Cibernética, o Comitê de Crise deverá ser acionado, nos termos do Protocolo de Gerenciamento de Crises Cibernéticas.
4.3. Após a conclusão do processo de coleta e preservação das evidências do incidente penalmente relevante, o responsável pela ETIR deverá elaborar Relatório de Comunicação de Incidente de Segurança Cibernética, descrevendo detalhadamente os eventos verificados.
4.4. O Relatório de Comunicação de Incidente de Segurança Cibernética deverá conter as seguintes informações, sem prejuízo de outras julgadas relevantes:
a) nome do responsável pela preservação dos dados do incidente, com informações de contato;
b) nome do agente responsável pela ETIR e informações de contato;
c) órgão comunicante com sua localização e informações de contato;
d) número de controle da ocorrência;

e) relato sobre o incidente que descreva o que ocorreu, como foi detectado e quais dados foram coletados e preservados;

f) descrição das atividades de tratamento e resposta ao incidente e todas as providências tomadas pela ETIR, incluindo as ações de preservação e coleta, a metodologia e as ferramentas utilizadas e o local de armazenamento das informações preservadas;

g) resumo criptográfico dos arquivos coletados;

h) Termo de Custódia dos Ativos de Informação Relacionados ao Incidente de Segurança;

i) número de lacre de material físico preservado, se houver; e

j) justificativa sobre a eventual inviabilidade de preservação das mídias de armazenamento dos dispositivos afetados, diante da impossibilidade de mantê-las.

4.5. O Relatório de Comunicação de Incidente de Segurança em Redes Computacionais deverá ser acondicionado em envelope lacrado e rubricado pelo agente responsável pela ETIR, protocolado e encaminhado formalmente à autoridade responsável pelo órgão do Poder Judiciário afetado.

4.6. Deverá constar no documento formal de encaminhamento a que se refere o item 4.5, apenas a informação de que se trata de comunicação de evento relacionado à segurança da informação, sem a descrição dos fatos.

4.7. Recebida a Comunicação de Incidente de Segurança em Redes Computacionais, a autoridade responsável pelo órgão do Poder Judiciário deverá encaminhá-la formalmente ao Ministério Público e ao órgão de polícia judiciária com atribuição para apurar os fatos, juntamente com o todo o material previsto neste protocolo, para fins de instrução da notícia crime.

Poder Judiciário

Conselho Nacional de Justiça

ANEXO IV DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

Manual de Referência – Proteção de Infraestruturas Críticas de TIC

Manual de Referência

Proteção de Infraestruturas Críticas de TIC

Material de Referência com os Principais Controles de Segurança Cibernética necessários para proteção estratégica de infraestruturas de TIC

Sumário

1. Motivação e Origem 9
2. Estrutura do Documento 9
3. Referência Normativa 10
4. Campo de Aplicação 11
5. Finalidade e Escopo 11
6. Princípios 12
7. Controles Mínimos Recomendados 13
8. *Checklist* para utilização dos Controles Mínimos Recomendados: 15

1. Motivação e Origem

1.1. O cenário tecnológico atual propicia avanços em todos os setores da sociedade, inclusive nos serviços prestados pelo Poder Judiciário. Nos últimos anos o Judiciário vem passando por grandes avanços tecnológicos, conferindo-lhe mais agilidade e ampliando o acesso à Justiça. De forma quase natural os ambientes tecnológicos tornaram-se maiores, mais complexos, bem como os processos de negócio se tornaram mais dependentes da tecnologia. Nesse contexto os riscos relacionados à segurança da informação tendem a amplificar-se e, em muitos casos, materializar-se.

1.2. Esse cenário tecnológico é reforçado pela Resolução CNJ nº 345/2020, que autoriza os tribunais a adotarem o Juízo 100% Digital para viabilizarem a execução de todos os atos processuais exclusivamente por meio eletrônico e remoto. A medida segue um dos principais eixos definidos pelo CNJ, voltada para o incentivo à inovação tecnológica, eficiência na prestação do serviço jurisdicional e a redução de custos do Judiciário.

1.3. Os fatores citados somados às novas exigências legais, como, por exemplo, a LGPD, motivam o CNJ, por meio do Comitê Gestor de Segurança Cibernética do Poder Judiciário (CGSCPJ), a apoiar os órgãos do Judiciário, estabelecendo padrões mínimos para proteção de sua infraestrutura tecnológica. Esses padrões foram organizados neste Manual, que conta com orientações organizacionais sobre sua aplicação e uma lista de controles mínimos exigidos para implantação pelos órgãos do Judiciário.

2 Estrutura do Documento

2.1 Este documento foi organizado no intuito de facilitar sua leitura e entendimento, incrementando sua aplicabilidade em ambientes reais e está dividido nas seguintes seções:

a) **Motivação e Origem:** descreve a motivação e a autoria do documento;

b) **Estrutura do Documento**: trata-se desta seção;

c) **Referência Normativa**: lista as referências relevantes utilizadas na elaboração do documento;

d) **Campo de Aplicação**: descreve quais órgãos estão submetidos aos requisitos mínimos descritos;

e) **Finalidade e Escopo**: descreve de forma geral a finalidade e os limites de aplicabilidade deste documento;

f) **Termos e Definições**: lista termos e suas definições aplicáveis no âmbito deste documento e das discussões acerca dele;

g) **Princípios**: lista os princípios que devem nortear a leitura e as atividades baseadas neste documento;

h) **Diretrizes Gerais**: descreve as diretrizes gerais norteadoras da construção deste documento;

i) **Competências e Responsabilidades**: descreve de maneira geral as responsabilidades envolvidas no processo de implantação;

j) **Controles Mínimos Exigidos**: lista informações sobre os controles que cada órgão do Judiciário deve implementar em seu ambiente; e

k) **Atualização**: descreve a expectativa de atualização deste Manual.

3 Referência Normativa

a) Resolução CNJ nº 370/2021, que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

b) Portaria CNJ nº 242/2020, que institui o Comitê de Segurança Cibernética do Poder Judiciário;

c) Portaria CNJ nº 249/2020, que designa os integrantes do Comitê de Segurança Cibernética do Poder Judiciário (CSCPJ);

d) Recomendações constantes da norma técnica ABNT NBR ISO/IEC 27005:2019 – Gestão de Riscos de Segurança da Informação;

e) *CIS Controls Framework* – Versão 7.1, Center for Internet Security (CIS), https://www.cisecurity.org/controls/”

f) *NIST Cybersecurity Framework* – Versão 1.1, National Institute of Standards and Technology (NIST), *https://www.nist.gov/cyberframework/framework"*

4 Campo de Aplicação

4.1. Este Manual é de aplicação mandatória no âmbito do Poder Judiciário, com exceção do Supremo Tribunal Federal. Portanto, todo órgão do Judiciário que conte com infraestrutura tecnológica, inclusive mantida ou administrada por terceiros, deve seguir as orientações e implantar os controles mínimos aqui recomendados.

5 Finalidade e Escopo

5.1. Este Manual tem por finalidade estabelecer as diretrizes estratégicas para a implementação dos controles de segurança cibernética necessários para proteção de infraestruturas de TIC de forma a preservar a disponibilidade, integridade, confidencialidade e autenticidade das informações.

5.2. As orientações e os controles recomendados neste Manual aplicam-se a todos os membros do órgão, sejam eles magistrados ou magistradas, servidores ou servidoras, colaboradores ou colaboradoras, fornecedores, prestadores ou prestadoras de serviços, estagiários ou estagiárias que, oficialmente, executem atividades relacionadas ao órgão.

5.3. Cabe ainda ressaltar que as orientações e os controles aqui expostos consistem em base mínima para a proteção de infraestruturas críticas de TI, não limitando a evolução do modelo de segurança da informação de cada órgão, bem como a adoção de outros controles, processos e *frameworks* que possam contribuir nesse contexto.

5.4. Ainda, considerando que os controles foram selecionados a partir do conjunto de boas práticas denominado *CIS Controls*, versão 7.1, recomenda-se que a instituição avalie a pertinência e a oportunidade de aplicar os demais controles por ele preconizados ou eventual versão posterior.

6. Princípios

6.1. Está disposta a seguir uma lista com os princípios que devem nortear a leitura e as atividades baseadas neste documento.

6.1.1 Eficiência: propriedade de que a Política de Segurança da Informação e das Comunicações (POSIC) e suas Normas busquem o melhor resultado possível, por meio das suas diretrizes e normatizações, visando a auxiliar para que a atividade administrativa seja exercida com presteza, perfeição e rendimento funcional.

6.1.2 Ética: propriedade de que a POSIC e suas Normas devem seguir os valores morais de conduta. São todos os direitos e interesses legítimos de usuários.

6.1.3 Impessoalidade: propriedade de que a POSIC e suas Normas devem servir para todos, sem preferências ou aversões pessoais ou partidárias.

6.1.4 Legalidade: propriedade de que a POSIC e suas Normas devem atuar no âmbito das leis.

6.1.5 Moralidade: propriedade de que as diretrizes estabelecidas nesta POSIC e suas Normas preservarão a moral dos princípios éticos, da boa-fé e da lealdade.

6.1.6 Publicidade: propriedade de que a POSIC e suas Normas terão publicidade e serão levadas ao conhecimento de toda a Entidade, buscando garantir atuação transparente do Poder Público.

7 Controles Mínimos Recomendados

7.1. O Poder Judiciário conta com um cenário heterogêneo em relação à diversidade de características entre seus órgãos integrantes, embora existam similaridades reconhecidas pelo fato de todos comporem um mesmo Poder. As variações entre eles estão presentes em vários aspectos, tais como finalidade para a qual cada um existe, distribuição geográfica, dimensão de recursos disponíveis, peculiaridades do seu ambiente tecnológico, características de competências do corpo funcional, entre outros. Tomando como base as similaridades, diversidades e boas práticas de segurança da informação corporativa reconhecidas na atualidade, este Manual baseia-se em um conjunto de controles mínimos exigidos compreendidos como pertinentes e condizentes com a realidade do Judiciário.

7.2. Os controles selecionados como linha base (recomendações iniciais mínimas) para a versão inicial deste Manual foram selecionados a partir do *framework* denominado *CIS Controls*, versão 7.1. Considerando a visão de adequação a médio prazo na busca de linha base mínima de controles para os diferentes órgãos do Judiciário, considerou-se para este momento os controles do agrupamento *Basic* do *CIS Control 7.1* e, adicionalmente, os seguintes controles desse *framework*: *E-mail* e Proteções de Navegador *web*; Defesas contra *malware*; Capacidade de Recuperação de Dados; e Proteção de Dados. Dentro desses destaques ainda houve uma segunda seleção e eventuais ajustes de texto em alguns controles para adequação ao contexto e a normativos já existentes.

7.3. Dessa maneira, segundo o *framework*, por meio da adoção desses controles, estima-se que cerca de 85% (oitenta e cinco por cento) dos principais ataques praticados quando do lançamento do *CIS* versão 7.1 poderiam ser evitados.

Optou-se também por se manter a escala de aplicabilidade de cada controle em relação ao porte da organização, categorizado por Grupo 1, Grupo 2 e Grupo 3, esses grupos fornecem uma forma simples e acessível de ajudar as organizações de diferentes portes a direcionar seus recursos com o melhor custo × benefício, alcançando os melhores resultados na busca pela mitigação do risco. Os critérios aplicáveis para a classificação do órgão quanto ao porte estão detalhados no quadro seguinte.

Grupo	Sugestão de ordem de implantação
Grupo 1	Organizações com nível limitado de recursos disponíveis e pouca experiência em segurança cibernética
Grupo 2	Organizações com nível moderado de recursos disponíveis e experiência média em segurança cibernética
Grupo 3	Organizações com nível elevado de recursos disponíveis e alta experiência em segurança cibernética

7.4. Cabe ressaltar que a classificação por grupos é uma sugestão para direcionamento e priorização dos esforços de segurança da informação a serem operacionalizados, e que tal abordagem deve ter sua aplicabilidade e aderência sempre validadas\adequadas para o contexto de cada organização.

7.5. A categorização pelo *NIST CSF* também foi incluída para apoiar o entendimento sobre em que fase de um incidente o controle se enquadra.

7.6. Os controles disponíveis para trabalho a partir deste Manual são essencialmente técnicos. Entretanto, para alcançar sua implementação, os órgãos precisam de medidas organizacionais que apoiem a efetivação de cada um deles. A descrição dessas medidas não faz parte do escopo deste Manual, mas é importante considerar o patrocínio e o acompanhamento pela alta administração, que deve entender a aplicação desses controles como estratégica para o órgão.

7.7. Considerando que as tecnologias mudam rapidamente e as ameaças cibernéticas crescem exponencialmente, a busca pela adequação dos órgãos ao atendimento dos requisitos mínimos deve ser contínua. Portanto, é imprescindível que a aplicação dos *checklists* pela organização seja periódica (anualmente, pelo menos), e que esses *checklists* tenham níveis de atendimento/maturidade, possibilitando a melhoria contínua da segurança digital de cada dependência.

8 Checklist para utilização dos Controles Mínimos Recomendados

ID	Requisito	Controle	NIST CSF	Maturidade de SI		
				Grupo 1	Grupo 2	Grupo 3
Inventário e controle de ativos de hardware						
1.1	Utilizar uma ferramenta de descoberta ativa para identificar dispositivos conectados à rede da organização, e atualizar o inventário de *hardware*.		Identificar		X	X
1.2	Utilizar os registros (*logs*) do *Dynamic Host Configuration Protocol* (DHCP) em todos os servidores ou utilizar ferramentas de gerenciamento de endereços IP para atualizar o inventário de ativos de *hardware*.		Identificar		X	X
1.3	Manter inventário atualizado e preciso de todos os ativos de tecnologia que detenham o potencial de armazenamento ou processamento de informações. Esse inventário deve incluir ativos de *hardware*, conectados ou não à rede da organização.		Identificar	X	X	X

1.4	Garantir que o inventário de ativos de *hardware* armazene o endereço de rede, endereço de *hardware*, nome do equipamento, proprietário do ativo e departamento para cada ativo, registrando ainda se foi aprovada ou não a conexão do ativo à rede.	Identificar		X	X
1.5	Garantir que ativos não autorizados sejam removidos da rede ou colocados em quarentena, ou que o inventário seja atualizado em tempo hábil.	Responder	X	X	X
Inventário e controle de ativos de *software*					
2.1	Manter uma lista atualizada de todos os *softwares* autorizados que sejam necessários à organização para qualquer propósito ou sistema de negócios.	Identificar	X	X	X
2.2	Garantir que apenas aplicações ou sistemas operacionais atualmente suportados pelo fabricante sejam adicionados ao inventário de *softwares* autorizados. *Softwares* sem suporte devem ser indicados no sistema de inventário.	Identificar	X	X	X
2.3	Utilizar ferramentas de inventário de *software* em toda a organização de forma a automatizar a documentação de todos os *softwares* que componham sistemas de negócio.	Identificar		X	X
2.4	O sistema de inventário de *software* deve registrar nome, versão, fabricante e data de instalação para todos os *softwares*, incluindo sistemas operacionais autorizados pela organização.	Identificar		X	X
2.5	O sistema de inventário de *software* deve ser vinculado ao inventário de ativos de *hardware*, de forma que todos os dispositivos e *softwares* associados possam ser rastreados a partir de uma única localidade.	Identificar			X
2.6	Garantir que qualquer *software* não autorizado seja removido, ou que o inventário seja atualizado em tempo hábil.	Identificar	X	X	X

2.7	Sistemas segregados física ou logicamente devem ser utilizados para isolar e executar *softwares* que sejam necessários às operações do negócio, mas que não tragam maior risco à organização.	Proteger			X
Gerenciamento Contínuo de Vulnerabilidade					
3.1	Utilizar uma ferramenta atualizada e compatível com o SCAP para efetuar varreduras automatizadas em todos os ativos conectados à rede com frequência semanal ou inferior. para identificar todas as vulnerabilidades potenciais nos sistemas da organização.	Detectar		X	X
3.2	Realizar varreduras por vulnerabilidades com contas autenticadas em agentes executados localmente em cada sistema, ou varreduras por *scanners* remotos que sejam configurados com privilégios elevados nos sistemas que estejam sendo testados.	Detectar		X	X
3.3	Utilizar uma conta dedicada para as varreduras por vulnerabilidades autenticadas, que não deve ser utilizada para quaisquer outras atividades administrativas e que deve ser vinculada a equipamentos específicos, em endereços IP específicos.	Detectar		X	X
3.4	Implantar ferramentas de atualização automatizada de *software*, de forma a garantir que os sistemas operacionais sejam executados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	Proteger	X	X	X
3.5	Implantar ferramentas de atualização automatizada de *software* de forma a garantir que os *softwares* de terceiros em todos os equipamentos sejam utilizados com as atualizações de segurança mais recentes disponibilizadas pelo fabricante.	Proteger	X	X	X
3.6	Utilizar um processo de classificação de riscos para priorizar a remediação de vulnerabilidades descobertas.	Responder		X	X

Uso controlado de privilégios administrativo					
4.1	Utilizar ferramentas automatizadas para inventariar todas as contas administrativas, incluindo contas de domínio e contas locais, para garantir que apenas indivíduos autorizados tenham privilégios elevados.	Detectar		X	X
4.2	Antes de ativar qualquer novo ativo, modificar todas as senhas padrão de forma consistente com contas de nível administrativo.	Proteger	X	X	X
4.3	Garantir que todos os usuários com contas administrativas utilizem uma conta secundária para atividades de privilégio elevado. Essa conta deve ser utilizada somente para atividades administrativas e não para navegação na internet, correio eletrônico ou atividades similares.	Proteger	X	X	X
4.4	Utilizar autenticação multifator e canais criptografados para todos os acessos de contas administrativas.	Proteger		X	X
4.5	Garantir que administradores utilizem um equipamento dedicado para todas as tarefas administrativas ou tarefas que requeiram acesso administrativo. Tal equipamento deve estar em rede segregada da rede principal da organização e não deve ter permitido o acesso à internet. Esse equipamento não deverá ser utilizado para a leitura de *e-mails*, elaboração de documentos, ou navegação na internet.	Proteger		X	X
4.6	Limitar o acesso a ferramentas de *scripting* (tais como *Microsoft PowerShell and Python*) exclusivamente a usuários administrativos ou de desenvolvimento que necessitem acessar tais funcionalidades.	Proteger		X	X
4.7	Configurar os sistemas para efetuarem um registro no *log* e um alerta quando uma conta for adicionada ou removida de qualquer grupo com privilégios administrativos.	Detectar		X	X

4.8	Configurar os sistemas para efetuarem um registro no *log* e um alerta no caso de *logins* sem sucesso de uma conta administrativa.	Detectar		X	X
Configuração segura para *hardware* e *software* em dispositivos móveis, *laptops*, estações de trabalho e servidores					
5.1	Manter padrões documentados de configuração segura para todos os sistemas operacionais e *softwares* autorizados.	Proteger	X	X	X
5.2	Manter imagens ou *templates* seguros para todos os sistemas na organização com base nos padrões de configuração aprovados. Todos os novos sistemas implantados ou sistemas existentes que venham a ser comprometidos devem ser instalados ou restaurados a partir dessas imagens ou *templates*.	Proteger		X	X
5.3	Armazenar as imagens e *templates* em servidores configurados de forma segura, validados por meio de ferramentas de monitoramento de integridade, de forma a garantir apenas modificações autorizadas nas imagens e *templates*.	Proteger		X	X
5.4	Implantar ferramentas de gerência de configuração de sistemas que automaticamente imponham e reapliquem opções de configuração sobre os sistemas em intervalos regulares agendados.	Proteger		X	X
Manutenção, Monitoramento e Análise de *Logs* de Auditoria					
6.1	Utilizar ao menos três fontes de horário sincronizadas, a partir das quais todos os servidores e dispositivos de rede atualizem informações sobre horário de forma regular, a fim de que os *timestamps* dos *logs* sejam consistentes.	Detectar		X	X
6.2	Garantir que o *log* local tenha sido habilitado em todos os sistemas e dispositivos de rede.	Detectar	X	X	X

6.3	Habilitar o *log* dos sistemas de forma a incluir informações detalhadas, tais como origem do evento, data, usuário, horário, endereços de origem, endereços de destino e outros elementos úteis.	Detectar		X	X
6.4	Garantir que todos os sistemas que armazenem *logs* tenham espaço de armazenamento adequado para os *logs* gerados.	Detectar		X	X
6.5	Garantir que os *logs* apropriados sejam agregados em um sistema central de gerenciamento de *logs* para análises e revisões.	Detectar		X	X
6.6	Implantar *Security Information and Event Management* (SIEM) ou ferramenta analítica de *logs* para correlação e análise de *logs*.	Detectar		X	X
6.7	Em uma base regular, revisar os *logs* para identificar anomalias ou eventos anormais.	Detectar		X	X
6.8	Em uma base regular, ajustar as configurações do SIEM de forma a melhor identificar eventos que requeiram ações e diminuir o ruído proveniente de eventos não importantes.	Detectar			X
Proteções de *e-mail* e navegadores web					
7.1	Garantir que apenas navegadores *web* e clientes de *e-mail* suportados possam ser executados na organização, idealmente utilizando apenas a versão mais recente disponibilizada pelo fabricante.	Proteger	X	X	X
7.2	Desinstalar ou desabilitar *plug-ins* ou aplicações *add-on* não autorizados para navegadores *web* e clientes de e-mail.	Proteger		X	X
7.3	Utilizar filtros de URL baseados em rede de forma a limitar a possibilidade de sistemas se conectarem a *websites* não aprovados pela organização. Tais filtros devem ser impostos a todos os sistemas da organização, quer se encontrem dentro do espaço físico da organização, quer não.	Proteger		X	X

7.4	Subscrever serviços de categorização de URLs de forma a garantir que o filtro esteja atualizado com base nas mais recentes definições de categorias de sítios eletrônicos disponíveis. Sites não categorizados devem ser bloqueados por padrão.	Proteger		X	X
7.5	Realizar registros de *log* de todas as requisições a URLs a partir de cada um dos sistemas da organização, quer nas dependências corporativas, quer em dispositivos móveis, de forma a identificar potenciais atividades maliciosas e auxiliar operadores de incidentes com a identificação de sistemas potencialmente comprometidos.	Detectar		X	X
7.6	Utilizar serviços de filtragem de DNS para auxiliar no bloqueio de acessos a domínios maliciosos.	Proteger	X	X	X
7.7	Com o objetivo de diminuir a possibilidade de recebimento de *e-mails* forjados ou modificados de domínios válidos, implementar políticas e verificações com base no padrão *Domain-based Message Authentication, Reporting and Conformance* (DMARC), iniciando pela implementação dos padrões *Sender Policy Framework* (SPF) e *DomainKeys Identified Mail* (DKIM).	Proteger		X	X
7.8	Bloquear todos os anexos de *e-mail* no *gateway* de correio eletrônico para os tipos de arquivos que sejam desnecessários ao negócio da organização.	Proteger		X	X
Defesas contra malware					
8.1	Utilizar *software antimalware* gerenciado de forma central para monitorar continuamente e defender cada uma das estações de trabalho e servidores.	Proteger		X	X
8.2	Garantir que o *software antimalware* atualize seu motor de varredura e base de assinaturas de *malware* de forma regular.	Proteger	X	X	X

8.3	Habilitar funcionalidades *anti-exploits,* tais como *Data Execution Prevention* (DEP) ou *Address Space Layout Randomization* (ASLR) que estejam disponíveis no sistema operacional, ou implantar ferramentas apropriadas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.	Proteger		X	X
8.4	Configurar os dispositivos de forma que automaticamente conduzem uma varredura *antimalware* em mídias removíveis assim que sejam inseridas ou conectadas.	Detectar	X	X	X
8.5	Configurar os dispositivos para que não autoexecutem conteúdo em mídia removível.	Proteger	X	X	X
8.6	Enviar todos os eventos de detecção de *malware* para as ferramentas de administração de *antimalware* e para servidores de *logs*, para análises e alertas.	Detectar		X	X
8.7	Habilitar *log* de pesquisas sobre *Domain Name System* (DNS) de forma a detectar buscas por nomes de *hosts* em domínios reconhecidamente maliciosos.	Detectar		X	X
8.8	Habilitar *log* de auditoria sobre ferramentas de linha de comando, tais como *Microsoft Powershell* e *Bash*.	Detectar		X	X
Capacidades de recuperação de dados					
9.1	Garantir que todos os dados dos sistemas tenham cópias de segurança (*backups*) realizados automaticamente de forma regular.	Proteger	X	X	X
9.2	Garantir que todos os sistemas chave da organização tenham suas cópias de segurança (*backups*) realizadas como um sistema completo, por meio de processos como a geração de imagem, de forma a permitir uma rápida recuperação de todo o sistema.	Proteger	X	X	X

9.3	Testar a integridade dos dados nas mídias das cópias de segurança de forma regular, por meio da realização de um processo de restauração dos dados, de forma a garantir que o processo de cópia de segurança (*backup*) esteja sendo executado de forma apropriada.	Proteger		X	X
9.4	Garantir que as cópias de segurança (*backups*) sejam apropriadamente protegidas por meio de segurança física ou criptografia quando forem armazenadas, assim como quando são movimentadas através da rede. Isso inclui cópias de segurança (*backup*s) remotas e em serviços de nuvem.	Proteger	X	X	X
9.5	Garantir que todas as cópias de segurança contenham ao menos uma localização que não seja endereçável de forma contínua por meio de chamadas do sistema operacional.	Proteger	X	X	X
Proteção de dados					
10.1	Manter um inventário de todas as informações sensíveis armazenadas, processadas ou transmitidas pelos sistemas de tecnologia da organização, incluindo aquelas localizado nas próprias dependências da organização ou em um provedor de serviços remoto.	Identificar	X	X	X
10.2	Remover da rede dados sensíveis ou sistemas não acessados regularmente pela organização. Tais sistemas devem ser utilizados somente como sistemas isolados (desconectados da rede) pela unidade de negócios que necessite de acesso ocasional, ou devem ser completamente virtualizados e desligados até que sejam necessários.	Proteger	X	X	X
10.3	Permitir apenas o acesso de *cloud storage* e\ou provedores de e-mail autorizados.	Proteger		X	X
10.4	Utilizar ferramentas aprovadas para criptografia total dos discos rígidos de todos os dispositivos móveis.	Proteger	X	X	X

10.5	Configurar os sistemas para não gravar dados em mídia externa removível, caso não haja requisito de negócio que exija tais dispositivos.	Proteger			X
10.6	Caso seja necessária a utilização de dispositivos de armazenamento USB, todos os dados devem ser armazenados de forma criptografada.	Proteger			X

Poder Judiciário

Conselho Nacional de Justiça

ANEXO V DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

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

Sumário

Introdução 28
1. Principais *frameworks* de referência utilizados 29
2. MITRE ATT&CK 30
3. Norma ABNT NBR ISO/IEC 27000:2018 30
4. Norma ABNT NBR ISO/IEC 27001:2013 31
5. Norma ABNT/NBR ISO/IEC 27005:2019 31
6. Norma ABNT NBR ISO/IEC 27007:2018 31
7. Norma ABNT NBR ISO/IEC 19011:2018 32
8. Norma Complementar nº 11/IN01/DSIC/GSIPR, de 2012 32
9. NIST SP 800-160 v2 32
10. Resolução CNJ nº 309/2020 33
11. Padrões mínimos de Gestão de Riscos de Segurança da Informação 33
12. Princípios 34
13. Diretrizes 35
14. Objetivos 36
15. Estrutura e Competências 36
16. Comitê de Governança de Segurança da Informação (CGSI) 37
17. Unidade dirigente de TIC do órgão 37
18. Unidade responsável pela Gestão de Segurança da Informação de TIC do Órgão 38
19. Gestores de riscos 38
20. Gestores de processos 39
21. Processo de Gestão de Riscos de Segurança da Informação 39

22. Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas 42
23. Princípios e Diretrizes 42
24. Objetivos 42
25. Estrutura e Competências 43
26. Confiança digital, prevenção e mitigação de ameaças cibernéticas 43
27. Metas 43
28. Objetivos 44
29. Princípios de *design* da resiliência cibernética 44
30. Framework de resiliência cibernética 46
31. Requisitos de resiliência cibernética 48
32. Da identificação 48
33. Da proteção 49
34. Da detecção 52
35. Da resposta 53
36. Da recuperação 54
37. *Checklist* 54
38. Anexo I – modelo de *checklist* 55

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 instituição 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, em https://attack.mitre.org/

3. Norma ABNT NBR ISO/IEC 27000:2018

3.1 A norma ISO/IEC 27000:2018[2] 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.

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[3].

[1] https://attack.mitre.org/.
[2] A versão original da norma ISO/IEC 27000:2018 está publicamente disponível em https://standards.iso.org/ittf/PubliclyAvailableStandards/.
[3] http://www.abnt.org.br/noticias/5777-iso-iec-27000-norma-internacional-de-seguranca-da-informacao-e-revisada.

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[4].

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

5.1 Fornece diretrizes para o processo de gestão de riscos de segurança da informação[5].

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[6], em complemento às diretrizes descritas na norma ABNT NBR ISO/IEC 19011:2018

[4] https://www.abntcatalogo.com.br/norma.aspx?ID=306580.
[5] https://www.abntcatalogo.com.br/norma.aspx?ID=429058.
[6] https://www.abntcatalogo.com.br/norma.aspx?ID=401077.

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[7]. Essas atividades incluem a(s) pessoa(s) que gerencia(m) o programa de auditoria, os auditores e a equipe de auditoria.

8. Norma Complementar nº 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)[8].

9. NIST SP 800-160 Vol. 2

9.1 A publicação NIST Special Publication 800-160, Volume 2 (Desenvolvendo Sistemas Cyber Resilientes: Uma – Abordagem de Engenharia de Segurança de Sistemas) 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

[7] http://www.abnt.org.br/noticias/6215-abnt-nbr-iso-19011-finalmente-publicada.
[8]https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=10/02/2012&jornal=1&pagina=2&totalArquivos=264.

Gerenciamento de Risco para Sistemas de Informação e Organizações – uma Abordagem do Ciclo de Vida do Sistema para Segurança e Privacidade)[9].

9.2 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 nº 309/2020

10.1 Aprova as Diretrizes Técnicas das Atividades de Auditoria Interna Governamental do Poder Judiciário (DIRAUD-Jud) e dá outras providências[10].

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.

[9] https://csrc.nist.gov/publications/detail/sp/800-160/vol-2/final.
[10] https://atos.cnj.jus.br/atos/detalhar/3289.

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[11]".

11.3 Também compreendendo essa importância, o Conselho Nacional de Justiça (CNJ) instituiu, por meio da Portaria nº 277/2019, o "Manual de Gestão de Riscos[12]" 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 ABNT NBR ISO 31000:2018), 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;

[11] https://portal.tcu.gov.br/data/files/FA/B6/EA/85/1CD4671023455957E18818A8/Referencial_basico_governanca_2_edicao.PDF.
[12] 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; e
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 de Governança 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
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 de Governança de Segurança da Informação (CGSI)

16.1 Compete ao Comitê de Governança 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; e
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; e

IV. analisar e encaminhar o Relatório de Riscos de Segurança da Informação não tratados ao CGSI.

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; e

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; e

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; e

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; e

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; e
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; e
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 nº 309/2020, 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[13], é a capacidade de uma entidade resistir, responder e se recuperar de um incidente cibernético, mantendo os seus serviços operacionais.

27. Metas

27.1 Para a garantia de um nível de segurança cibernética adequado deve-se estabelecer, no mínimo, 4 (quatro) metas[14]:

[13] Hausken, Kjell (9/2020). "Cyber resilience in firms, organizations and societies".
[14] NIST SP 800-160 v2 (11/2019) https://csrc.nist.gov/publications/detail/sp/800-160/vol.2/final.

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[15]:

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[16]:

a) Focalizar em ativos comuns e críticos

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

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.

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[17] e a implementação de times de ataque (*red team*) e jogos de guerra (*war gaming*).

30. *Framework* de resiliência cibernética

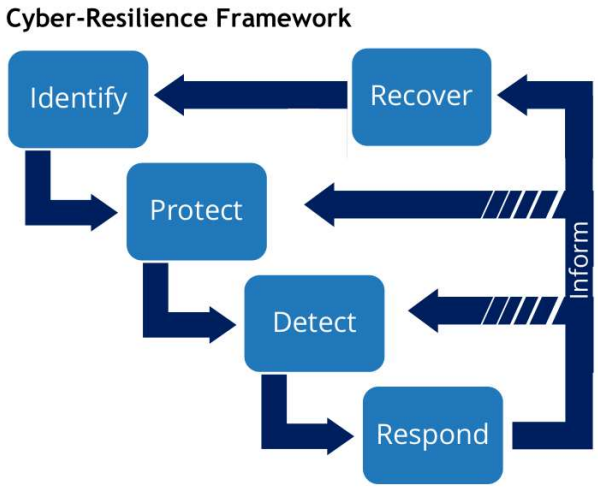
30.1 Um *framework* de resiliência cibernética possui os seguintes componentes[18].

[17] https://attack.mitre.org
[18] IDC (10/2020). Five Key Technologies for Enabling a Cyber-Resilience Framework.

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[19]

[19] 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; e
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 lógico 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; e

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 sejam contidos ou mitigados no menor tempo possível;

e) seja realizada 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); e

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; e
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.					

Poder Judiciário

Conselho Nacional de Justiça

ANEXO VI DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

.

Manual de Referência – Gestão de Identidade e de Controle de Acessos

Manual de Referência

GESTÃO DE IDENTIDADE E CONTROLE DE ACESSOS

Material de referência com os principais controles e padrões para o gerenciamento de identidade e controle de acessos baseados em frameworks de segurança

Sumário

1. Visão geral 1
2. Principais frameworks de referência utilizados 1
2.1. CIS Controls 7.1 1
2.2. MITRE ATT&CK 2
2.3. Norma ABNT NBR ISO/IEC 27001:2013 2
2.4. NIST SP 800-53 2
3. Diretrizes gerais 3
4. Tipos de contas 4
5. Autenticação 5
6. Autorização 6
7. Responsabilidades dos usuários 7
8. Check-list 8
9. Anexo I – Modelo de *checklist* 9

1. Visão geral

1.1 Este Manual estabelece as diretrizes principais para a gestão de identidades e credenciais eletrônicas bem como para o controle de acessos aos sistemas, serviços e equipamentos de tecnologia da informação (TI).

1.2 Orienta, também, quanto à criação de identidades e contas, formas de autenticação, gerenciamento de autorizações, remoção de contas e privilégios e registro das ações executadas para fins auditoria.

1.3 Este Manual é aplicável aos titulares de contas individuais e define as responsabilidades deles quanto à proteção de suas contas e ao uso adequado de suas autorizações, bem como aos operadores responsáveis pelo Gerenciamento de Identidade e Acesso para sistemas de informação.

2. Principais *frameworks* de referência utilizados

2.0.1. 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 as orientações que se adequam melhor ao cenário em que as instituições se encontram e buscar melhorias que possibilitem alcançar uma visão de futuro.

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

2.1. CIS Controls 7.1

2.1.1. O *Center for Internet Security Critical Security Controls for Effective Cyber Defense*[20] é uma publicação de diretrizes de práticas recomendadas para segurança cibernética.

2.1.2. O projeto foi concebido em 2008 em resposta a perdas de dados por organizações na base industrial de defesa dos EUA. A publicação foi desenvolvida inicialmente pelo SANS *Institute*, transferida para o *Council on Cyber Security* (CCS) em 2013 e, em posteriormente, transferida para o *Center for Internet Security* (CIS) em 2015.

[20] https://www.cisecurity.org/controls/

2.1.3. A versão 7.1 dos controles CIS foi disponibilizada em abril de 2019 para se adequar aos dados de ameaças cibernéticas mais atuais.

2.2. MITRE ATT&CK

2.2.1 A MITRE ATT&CK é uma base de conhecimento de táticas e técnicas adversárias pautada em observações do mundo real[21]. A base de conhecimento da MITRE é fundamental 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.

2.3. Norma ABNT NBR ISO/IEC 27001:2013

2.3.1. Especifica os requisitos para estabelecer, implementar, manter e melhorar continuamente um sistema de gestão da segurança da informação dentro do contexto da organização. Essa norma também inclui requisitos para a avaliação e tratamento de riscos de segurança da informação voltados para as necessidades da organização[22].

2.4. NIST SP 800-53

2.4.1. Fornece um catálogo de controles de segurança e privacidade para os sistemas de informações e organizações para proteger operações e ativos organizacionais, indivíduos e outras organizações de um conjunto diversificado de ameaças. É publicado pelo *National Institute of Standards and Technology* (NIST)[23] e busca estabelecer controles flexíveis e personalizáveis, implementados como parte de um processo de toda a organização para gerenciar riscos.

[21] https://attack.mitre.org.
[22] https://www.abntcatalogo.com.br/norma.aspx?ID=306580.
[23] https://csrc.nist.gov/Projects/risk-management/sp800-53-controls/release-search#!/800-53.

3. Diretrizes gerais

3.1. Os órgãos do Poder Judiciário devem efetuar a gestão de identidade e o controle de acessos de seus usuários, sejam magistrados ou magistradas, servidores ou servidoras, prestadores ou prestadoras de serviços, usuários ou usuárias dos serviços e equipe de TIC.

3.2. Deve ser estabelecido, em normativo próprio, o regramento de cada órgão, considerando as boas práticas de segurança da informação e em observância às seguintes diretrizes:

3.2.1. Definição de padrão de identidade do órgão, que contemple, no mínimo, os critérios para padronização de nome de usuário e de conta de *e-mail*;

3.2.2. Consideração do princípio de privilégio mínimo e de segregação de funções, visando a evitar acessos indevidos e reduzir os riscos de vazamento de informações;

3.2.3. Estabelecimento de processo e de responsáveis por solicitação, gerenciamento e revogação de contas de acesso, preferencialmente de forma automática;

3.2.4. Utilização de *login* único para acesso a serviços de diretório corporativo e para acesso aos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação e evitar a criação de contas e autorizações locais;

3.2.5. Adoção de modelo de controle de acesso, preferencialmente utilizando controle de acesso baseado em funções (RBAC) em que as credenciais recebam os privilégios de acesso conforme os papéis e as responsabilidades executadas pelos usuários;

3.2.6. Criação de processos de verificação de identidade nas interações entre sistemas, internos ou externos, com vinculação das credenciais aos usuários e às suas autorizações;

3.2.7. Registro de trilhas de auditoria que vise ao registro dos acessos a sistema de informação, quais operações foram realizadas e em qual período;

3.2.8. Definição de requisitos de tamanho, reutilização, critérios de complexidade e período de expiração de senhas;

3.2.9. Empenho pela adoção de múltiplo fator de autenticação;

3.2.10. Busca pela unificação de plataformas de autenticação, autorização e autenticação (AAA);

3.2.11. Estabelecimento de regras quanto ao acesso remoto e forma de disponibilização de sistemas e serviços na internet;

3.2.12. Gestão de credenciais privilegiadas e restrição ao uso de credenciais genéricas e de uso compartilhado;

3.2.13. Rastreabilidade de acessos e ações executadas por administradores de TI;

3.2.14. Utilização de mecanismos seguros de criptografia para o armazenamento e trânsito de credenciais de acesso;

3.2.15. Segregação de redes conforme o grupo dos serviços, sistemas ou usuários;

3.2.16. Controle do acesso físico aos ativos de tecnologia da informação e comunicação (TIC);

3.2.17. Implementação de controles de acesso proporcionais à classificação da informação;

3.2.18. Monitoração dos acessos e tentativas de acesso para identificação de ataques.

4. Tipos de contas

4.1. Contas de usuário: estão exclusivamente associadas a uma pessoa específica. Essas contas podem existir em um repositório central ao qual os sistemas podem federar para consumir as informações de identidade e autenticação ou podem ser criadas localmente em um sistema ou dispositivo em que a federação não é prática ou possível. O uso da conta criada centralmente com autenticação federada é sempre o método preferido.

4.2. Contas compartilhadas: as contas compartilhadas são criadas para oferecer suporte a vários usuários que utilizam a mesma identidade. Por exemplo, elas podem ser criadas quando há necessidade de compartilhar um conjunto de recursos ou porque uma implementação deficiente do produto exige isso. O uso de contas compartilhadas não é recomendado, pois são insuficientes para fins de responsabilização e auditoria.

4.3. Contas de serviço: uma conta de serviço é usada quando é necessário que sistemas ou serviços se autentiquem em outros sistemas ou serviços sem qualquer associação a uma pessoa. Essas contas devem ser criadas com moderação e a documentação da finalidade para elas deve ser mantida. Seu uso deve ser revisado

periodicamente. Além disso, os requisitos de senha para contas de serviço não devem ser menos rigorosos do que contas de usuário. Finalmente, as contas de serviço não podem ser usadas por pessoas para autenticação, exceto no teste inicial. Contas de serviço com privilégios elevados devem ser monitoradas com atenção.

4.4. Contas privilegiadas: certas contas podem ter privilégios adicionais relacionados ao gerenciamento de um dispositivo ou sistema. Geralmente, isso é considerado um tipo de conta, mas é descrito com mais precisão como uma conta com autorizações privilegiadas. O privilégio administrativo pode ser adicionado a qualquer um dos três tipos anteriores de conta. Ter pelo menos uma conta com privilégios geralmente é inevitável, mas o uso de privilégios deve ser limitado e o uso direto de contas compartilhadas com privilégios deve ser fortemente desencorajado ou vedado.

4.5. Serviços de Diretório Coorporativos: as informações sobre contas e identidades criadas centralmente são armazenadas no diretório central gerenciado pela área de TI. As implementações mais comuns do serviço de diretório são *Active Directory* (AD) e *Lightweight Directory Access Protocol* (LDAP). Os sistemas de informação do Poder Judiciário devem utilizar serviços de diretório corporativo, utilização das credenciais de *login* único com o objetivo de uniformizar e garantir a experiência única de interação e evitar a criação de contas e autorizações locais.

5. Autenticação

5.1. A autenticação é o processo pelo qual um sistema ou serviço confirma que uma pessoa ou dispositivo realmente é quem afirma ser e por meio do qual o acesso ao recurso solicitado é autorizado. É necessário a autenticação antes do uso de qualquer conta.

5.2. Devem ser empregados protocolos de autenticação seguros para a proteção das informações pessoais e do órgão e evitar o uso indevido.

5.3. A autenticação geralmente é dividida em três tipos:

5.3.1. Algo que você sabe: as formas mais comuns são senha, *pin* ou padrão;

5.3.2. Algo que você tem: as formas mais comuns são *token* de *hardware*, certificado ou um autenticador de *software* como o *Google Authenticator*, *Duo* ou outros;

5.3.3 Algo que você é: essa categoria costuma ser chamada de autenticação biométrica e a forma mais comum são os leitores de impressão digital.

5.3.4. A autenticação *multifator* (MFA) envolve a combinação de mais de um tipo de autenticação e geralmente fornece garantia mais forte da identidade da pessoa. A combinação de apenas dois dos tipos é chamada de autenticação de dois fatores (2FA).

5.3.5. É dispensada a autenticação quando se tratar de informação pública, conforme previsão legal e definição em política de classificação de informações.

6. Autorização

6.1. Autorizações são a permissão implícita ou explícita para usar um recurso associado a uma conta. Depois que o uso de uma conta é autenticado, um sistema ou recurso pode determinar se a pessoa ou *software* que solicita acesso está autorizado a usá-lo. O gerenciamento e a manutenção das autorizações são de responsabilidade compartilhada da área de tecnologia da informação e dos gestores de sistemas.

6.2. Todas as unidades envolvidas na concessão de autorizações são incentivadas a desenvolver procedimentos que atendam aos requisitos articulados a seguir na política de autorização.

6.3. **Princípios de autorização**

6.3.1 Menor privilégio

6.3.1.1. Uma autorização deve fornecer apenas os privilégios necessários para a função a ser executada e nada mais. Observar esse princípio ajuda a garantir que os fluxos de trabalho adequados sejam seguidos e o acesso às funções que podem expor os dados seja contido tanto quanto possível.

6.3.2 Separação de funções

6.3.2.1. Quando uma autorização é concedida a uma conta, ela deve ser aprovada preferencialmente por um ou vários indivíduos. Múltiplos aprovadores garantem que o princípio do menor privilégio seja seguido tanto do ponto de vista técnico quanto do processo, diminui a oportunidade de conflito de interesses ou fraude e reduz o risco de erro. Conforme aplicada a autorização, exige-se que as funções de aprovador administrativo e de aprovador técnico não sejam exercidas pela mesma pessoa ou, quando for o caso, que o custodiante de dados não desempenhe nenhuma dessas funções.

6.3.3 Custodiantes de dados

6.3.3. Em geral, essas autorizações são concedidas por custodiantes de dados, que são responsáveis pela manutenção dos dados. Normalmente, são administradores de sistemas, administradores de banco de dados ou administradores de aplicativos. Esses indivíduos são responsáveis por executar a solicitação de definição, modificação, remoção de conta aprovada, depois de validar se as aprovações apropriadas foram concedidas.

6.3.4. Desprovisionamento.

6.3.4.1. Os sistemas e aplicativos devem ser projetados e implantados de forma que facilite a remoção das autorizações e contas de uma pessoa nos momentos apropriados.

7. Responsabilidades dos usuários

7.1. Cada pessoa com credencial de acesso é responsável por selecionar senhas fortes, mantê-las seguras e relatar à unidade de TI qualquer uso não autorizado de contas. Os usuários devem:

7.1.1. Criar senhas que estejam em conformidade com os critérios de senhas seguras estabelecidos pelo órgão.

7.1.2. Não compartilhar senhas relacionadas a algum sistema corporativo com qualquer outra pessoa.

7.1.3. Não reutilizar senhas relacionadas a qualquer sistema corporativo em contas pessoais.

7.1.4. Alterar imediatamente as senhas e notificar o gestor do sistema apropriado e/ou área de segurança da informação se houver motivos para acreditar que uma senha foi divulgada, acessada ou utilizada indevidamente por uma pessoa não autorizada.

7.1.5. Utilizar os privilégios associados a uma conta apenas para a finalidade para a qual foram autorizados e nada mais.

7.1.6. Valer-se de contas e autorizações privilegiadas apenas quando tal privilégio for necessário para completar uma função.

7.1.7. Fazer *logoff* ou utilizar bloqueio de tela que exija autenticação ao deixar um dispositivo sem supervisão.

8. Checklist

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

8.2. 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.

8.3. 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.

8.4. 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 de normativos, processos e iniciativas em segurança cibernética da organização.

8.5. O quadro a seguir apresenta 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.

9. Anexo I – Modelo de *checklist*

Checklist de controles para o gerenciamento de identidade e controle de acessos.

Nr.	Item	Referencial	Maturidade				
			1	2	3	4	5
1.	Gestão de identidade e controle acesso						
2.1	Formalizar Política de Gestão de Identidade e Controle de Acesso em conformidade com as diretrizes previstas neste Manual e boas práticas de segurança.	CIS Controls v7.1					
2.2	Aplicação dos critérios de padronização de nome de usuário e de conta de *e-mail*.	CIS Controls v7.1					
2.3	Realizar processo de revisão para identificar privilégios excessivos de usuários, administradores de TI e de contas de serviço.	CIS Controls v7.1					
2.4	Definir e utilizar um processo para a revogação de direitos de acesso, desabilitando imediatamente as contas no momento do término do vínculo ou da alteração das responsabilidades de um servidor ou prestador de serviços.	CIS Controls v7.1					
2.5	Manter um inventário de cada um dos sistemas de autenticação da organização, incluindo aqueles internos ou em provedores de serviços remotos.	CIS Controls v7.1					
2.6	Adotar modelo de controle de acesso baseado em funções (RBAC).	CIS Controls v7.1					
2.7	Registrar em *logs* acessos, operações e período para fins de auditoria.	CIS Controls v7.1					
2.8	Garantir que todas as contas tenham uma data de expiração de senha e que isso seja configurado e monitorado.	CIS Controls v7.1					
2.9	Gerenciar acessos e ações executadas com credenciais privilegiados, não utilizando credenciais genéricas e de uso compartilhado.	CIS Controls v7.1					
2.10	Criptografar ou embaralhar (*hash*) com a utilização de *salt* as credenciais de autenticação armazenadas.	CIS Controls v7.1					
2.11	Utilizar criptografia no canal de comunicação ao trafegar credenciais de acesso.	CIS Controls v7.1					
2.14	Configurar o acesso a todas as contas por meio da menor quantidade de pontos de autenticação centralizados possível, incluindo sistemas de rede, segurança e sistemas em nuvem.	CIS Controls v7.1					
2.15	Garantir que todas as contas (*usernames*) e senhas sejam transmitidas em rede utilizando canais criptografados.	CIS Controls v7.1					
2.16	Manter um inventário de todas as contas organizadas por sistema de autenticação.	CIS Controls v7.1					
2.17	Desabilitar contas, em vez de excluí-las, visando à preservação de trilhas de auditoria.	CIS Controls v7.1					

2.18	Desabilitar qualquer conta que não possa ser associada a um processo de negócio ou a um usuário.	CIS Controls v7.1					
2.19	Desabilitar automaticamente contas não utilizadas após um período de inatividade pré-definido.	CIS Controls v7.1					
2.20	Bloquear automaticamente as estações de trabalho após um período de inatividade pré-definido.	CIS Controls v7.1					
2.21	Monitorar tentativas de acesso a contas desativadas, por meio de *logs* de auditoria.	CIS Controls v7.1					
2.22	Segregar as redes de comunicação a depender do grupo dos serviços, sistemas ou usuários.	CIS Controls v7.1					
2.23	Implementar controles de acesso físico aos ativos de TIC.	CIS Controls v7.1					

Poder Judiciário

Conselho Nacional de Justiça

ANEXO VII DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

Manual de Referência – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário

Manual de Referência

Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário

Material de referência com as principais diretrizes necessárias para implantação da política de educação e cultura em segurança cibernética do Poder Judiciário

Sumário

Introdução 14
1. Disposições Gerais 14
1.1 Finalidade 14
1.2 Objetivo 15
1.3 Abrangência 15
1.4 Público-alvo ..... **Erro! Indicador não definido.**
2. Programa de Capacitação em Segurança Cibernética do Poder Judiciário (PCASC-PJ) 16
2.1 Tipo de Ações 16
2.2 Temas abrangidos 18
3. Competências para Implementação das Ações 18
3.1 Escolas de Formação 18
3.2 Área de Gestão de Pessoas 19
3.3 Área de Comunicação Social e Institucional 19
4. Resultados previstos 19

Introdução

0.1. Esta política visa estabelecer as diretrizes necessárias consubstanciadas em ações permanentes de capacitação, de educação, de engenharia social e de formação de cultura especializada que constituem fatores indispensáveis para a efetividade de ações de segurança cibernética.

0.2. O tema formação de cultura e de educação em segurança cibernética deve ser tratado de forma equânime, uniforme e articulado com todos os órgãos do Poder Judiciário e em conformidade com os mais atualizados paradigmas, procedimentos e padrões nacionais e internacionais.

0.3. É importante ressaltar a necessidade de ações constantes de formação de cultura, de educação, de atualização tecnológica e de reciclagem e atualização técnica no tema da segurança cibernética, que devem ser desenvolvidas de forma colaborativa entre os órgãos do Poder Judiciário, além de envolvimento multissetorial de instituições de ensino, pesquisa e fomento.

0.4. Vale destacar a diversidade e a multiplicidade de opções de cursos; programas de treinamento; modalidades de aquisição e disseminação de conhecimentos; formação técnica e gerencial; e plataformas tecnológicas educacionais presentes no mercado educacional contemporâneo, que devem pautar as ações a serem desenvolvidas por todos os órgãos do Poder Judiciário.

1.Disposições Gerais

1.1 Finalidade

1.1.1. A Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário - PECSC-PJ tem a finalidade de desenvolver e fortalecer a cultura, a educação, a conscientização e as habilidades em segurança cibernética dos usuários de Tecnologia da Informação e Comunicação (TIC) e de Segurança da Informação (SI), bem como fomentar o desenvolvimento, o aprimoramento e a disseminação de conhecimentos,

pesquisas e inovações dos profissionais de Tecnologia da Informação e Comunicação e de Segurança da Informação.

1.2 Objetivos

1.2.1. São objetivos da PECSC-PJ:

a) propiciar o constante aprimoramento dos níveis de segurança cibernética nos ativos e serviços de Tecnologia da Informação e Comunicação nos órgãos do Poder Judiciário;
b) inserir o tema da segurança cibernética como tópico estratégico e primordial a constar das pautas institucionais de todos os órgãos do Poder Judiciário;
c) promover a elevação do grau de conhecimento e de consciência quanto à cultura da segurança da cibernética no âmbito do Poder Judiciário;
d) assegurar que todo usuário dos serviços de informação do Poder Judiciário tenha a devida compreensão de suas responsabilidades na proteção das informações dos órgãos do Poder Judiciário;
e) assegurar que novos conhecimentos atinentes ao tema da segurança cibernética sejam permanentemente ofertados aos profissionais das áreas de Tecnologia da Informação e Comunicação e de Segurança da Informação, em nível acadêmico, técnico, gerencial, entre outros aplicáveis.

1.3 Abrangência

1.3.1. Para os fins do disposto na PECSC-PJ, a segurança cibernética abrange:

a) a segurança da informação de forma geral;
b) a segurança física e a proteção de dados pessoais e institucionais;
c) a segurança física e a proteção de ativos de tecnologia da informação de forma geral;
d) as ações destinadas a assegurar a disponibilidade, integridade, confidencialidade e autenticidade de dados e informações;
e) as ações destinadas a assegurar o funcionamento dos processos de trabalho, a continuidade operacional e a continuidade da prestação jurisdicional e administrativa dos órgãos do Poder Judiciário;

f) as ações de planejamento, sistematização e normatização sobre temas atinentes à segurança cibernética;
g) as ações de comunicação, conscientização, formação de cultura e direcionamento institucional com vistas à segurança cibernética; e
h) as ações de formação acadêmica, formação técnica, qualificação e reciclagem de profissionais de Tecnologia da Informação e Comunicação que atuam na área de segurança cibernética.

1.3.2 A PECSC-PJ aplica-se a todos os usuários internos do Poder Judiciário, a saber:

a) magistrados e magistradas;
b) servidores e servidoras;
c) estagiários e estagiárias;
d) terceirizados e terceirizadas; e
e) colaboradores em geral.

2. Programa de Capacitação em Segurança Cibernética do Poder Judiciário (PCASC-PJ)

2.1 Tipo de Ações

2.1.1. Os órgãos do Poder Judiciário deverão desenvolver ações de capacitação, formação, reciclagem, fomento e conscientização em segurança cibernética, podendo incluir, entre outras:

a) programas de formação;
b) programas de reciclagem;
c) programas de extensão educacional;
d) programas de pesquisa e fomento de natureza técnica, acadêmica e científica;
e) elaboração de artigos, materiais e publicações de natureza técnica, acadêmica e científica;
f) programas de intercâmbio, imersão e cooperação educacional;
g) ações periódicas de capacitação;
h) cursos em plataformas do tipo *MOOC – Massive Open On-line Courses*;

i) programas de certificação especializada;
j) palestras, congressos, seminários e afins;
k) concursos, competições e premiações; e
l) *workshops*.

2.1.2. Além das ações direcionadas para públicos-alvo específicos os órgãos do Poder Judiciário devem estabelecer concomitantemente as seguintes ações de alcance amplo:

a) campanhas;
b) produção de fôlderes, cartazes, folhetos, notas informativas e/ou boletins periódicos; e
c) testes públicos de segurança.

2.1.3. Cada órgão do Poder Judiciário deverá estabelecer uma carga horária mínima de capacitação, podendo as ações previstas neste Manual serem efetuadas em diversas cargas horárias e níveis de formação, assim divididas:

a) ações de capacitação em geral;
b) cursos de educação executiva de curta duração;
c) cursos de graduação;
d) cursos de especialização;
e) cursos de mestrado;
f) cursos de doutorado; e
g) cursos de pós-doutorado.

2.1.4. As ações previstas neste Manual deverão ser priorizadas no formato considerado mais efetivo em termos de adequação ao aprendizado, ao aproveitamento e aos objetivos pretendidos, podendo ser realizada, em âmbito nacional ou internacional, nas seguintes modalidades:

a) presencial;
b) telepresencial;
c) on-line; ou
d) híbrida.

2.2 Temas abrangidos

2.2.1. Para efeitos deste Manual, os seguintes temas devem ser contemplados obrigatoriamente, além de outros:

a) governança e gestão de segurança cibernética;
b) elaboração de políticas institucionais de segurança cibernética;
c) tratamento de incidentes de segurança cibernética;
d) forense computacional;
e) inteligência e investigação em crimes cibernéticos;
f) gerenciamento de identidades, acesso e privilégios;
g) segurança no desenvolvimento de *software*;
h) gestão de continuidade de negócios;
i) gestão de riscos de TIC e SI;
j) auditoria e conformidade de sistemas de informação;
k) segurança em computação em nuvem;
l) segurança em aplicações móveis; e
m) segurança em redes sociais.

3. Competências para Implementação das Ações

a. Escolas de Formação

3.1.1. Compete às Escolas de Formação, aos Centros de Educação e Capacitação e às demais unidades administrativas responsáveis pela capacitação de magistrados e magistradas e de servidores e servidoras do Poder Judiciário:

a) adotar medidas para a concretização da PECSC-PJ descrita neste Manual.

b) elaborar Programas de Formação, Capacitação e Reciclagem de magistrados e magistradas e de servidores e servidoras que descrevam, com previsão bianual e de forma detalhada, as ações a serem realizadas, as metas a serem atingidas, os quantitativos previstos, os critérios de participação e a contabilização de horas, entre outros elementos que evidenciem o cumprimento dos itens previstos neste Manual.

c) propor celebração de parcerias, de acordos de cooperação técnica, de convênios, entre outros instrumentos afins, tanto em âmbito nacional como internacional, com instituições multissetoriais, a fim de maximizar os resultados descritos como objetivos deste Manual; e

d) atuar de forma coordenada com outros órgãos do Poder Judiciário e de outros Poderes com vistas ao oferecimento mútuo de vagas, ao compartilhamento de capacitações, à troca materiais e de experiências, à organização conjunta de eventos e de treinamentos, ao compartilhamento de ações de instrutoria interna, entre outras ações afins, para a máxima efetividade dos objetivos previstos neste Manual.

3.2 Área de Gestão de Pessoas

3.2.1. É responsabilidade da área de gestão de Pessoas de cada órgão do Poder Judiciário a adoção de procedimentos, normativos e práticas administrativas que viabilizem a inscrição, a participação e o pagamento de ações de capacitação previstas neste Manual, principalmente no caso de formas diversas de pagamento, tais como cartões de crédito, boletos bancários, meios eletrônicos de pagamento, entre outras.

3.2.2. Os normativos e procedimentos previstos poderão incluir regras, procedimentos, critérios e condições para o pagamento prévio por parte do participante e posterior ressarcimento, integral ou parcial, por parte do órgão.

3.3 Área de Comunicação Social e Institucional

3.3.1. Compete às áreas de Comunicação Social e Institucional dos órgãos do Poder Judiciário, incluírem, em seus planejamentos anuais, programas de divulgação, conscientização, informação e esclarecimentos aos seus públicos-alvo, tanto internos como externos, referentes a temas de Segurança Cibernética.

4 Resultados previstos

4.1. Os programas de formação, capacitação e reciclagem deverão propiciar que os órgãos do Poder Judiciário possuam:

a) profissionais de Tecnologia da Informação e Comunicação e de Segurança da Informação em seus quadros, qualificados em segurança cibernética em nível de graduação, pós-graduação ou de certificações especializadas;
b) todos os usuários internos com educação básica e cultura em segurança cibernética.

4.2. Os órgãos do Poder Judiciário deverão apresentar ao CNJ, no início do ano seguinte, relatório que comprove a efetividade das ações realizadas no exercício anterior e o respectivo desempenho dos usuários e profissionais treinados.

ANEXO VIII DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021.

Glossário

Material com definições e conceitos dos termos técnicos utilizados em Segurança Cibernética neste ato

Definição e Conceitos dos Termos Utilizados

A lista de termos com suas respectivas definições constante neste Anexo é aplicável no âmbito dos documentos de Segurança Cibernética produzidos pelo Comitê Gestor de Segurança Cibernética do Poder Judiciário e de quaisquer discussões acerca deles.

1. **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;
2. **Agente responsável pela ETIR**: servidor público do Poder Judiciário incumbido de chefiar e gerenciar a ETIR;
3. **Alta administração**: unidades organizacionais com poderes deliberativos ou normativos no âmbito da organização;
4. **Ameaças**: conjunto de fatores externos ou causa potencial de um incidente indesejado que pode resultar em dano para um sistema ou organização;
5. **Apetite a risco**: nível de risco que a organização está disposta a aceitar para atingir os objetivos identificados no contexto analisado;
6. **Aquisição de evidência**: processo de coleta e cópia das evidências de incidente de segurança em redes computacionais;
7. **Ativo**: qualquer coisa que represente valor para uma instituição, tal como a informação;
8. **Ativos de informação**: meios de armazenamento, transmissão e processamento de informação, sistemas de informação e locais onde se encontram esses meios e as pessoas que a eles têm acesso;
9. **Atividades críticas**: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão, de maneira que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;
10. **Auditoria**: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se estão de acordo com as disposições

planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos;

11. **Autenticação**: processo de identificação das partes envolvidas em um processo;
12. **Autenticidade**: propriedade indicativa de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
13. **Autorização**: processo que visa a garantir que as informações são acessíveis exclusivamente àqueles com permissão de acesso;
14. **Classificação da informação**: atribuição, pela autoridade competente, de grau de sigilo dado à informação, ao documento, ao material, à área ou à instalação;
15. **Coleta de evidências de segurança em redes computacionais**: processo de obtenção de itens físicos que contém potencial evidência, mediante a utilização de metodologia e ferramentas adequadas. Esse processo inclui a aquisição, ou seja, a geração das cópias das mídias, ou coleção de dados que contenham evidências do incidente;
16. **Competência**: habilidade para aplicar conhecimentos e habilidades para atingir resultados pretendidos;
17. **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada à pessoa física, ao sistema, ao órgão ou à entidade não autorizada;
18. **Conformidade**: preenchimento de um requisito;
19. **Continuidade de serviços**: capacidade estratégica e tática do órgão de se planejar e de responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos da informação das atividades críticas, de forma a manter suas operações em nível aceitável, previamente definido;
20. **Crise**: um evento ou série de eventos danosos que apresenta propriedades emergentes capazes de exceder as habilidades de uma organização em lidar com as demandas de tarefas que eles geram; e que apresenta implicações que afetam proporção considerável da organização e de seus constituintes;

21. **Crise cibernética**: crise que ocorre em decorrência de incidente em dispositivos, serviços e redes de computadores. É decorrente de incidentes que causam dano material ou de imagem, atraem a atenção do público e da mídia e fogem ao controle direto da organização;
22. **Controle**: providência que modifica o risco, incluindo qualquer processo, política, dispositivo, prática ou ação;
23. **Dado pessoal**: informação relacionada à pessoa natural identificada ou identificável;
24. **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
25. **Escopo de auditoria**: extensão e fronteiras de uma auditoria;
26. **Endereço IP (*Internet Protocol*)**: refere-se ao conjunto de elementos numéricos ou alfanuméricos que identifica um dispositivo eletrônico em uma rede de computadores;
27. **ETIR**: Equipe de Tratamento e Resposta a Incidentes de Segurança de Cibernética. Denominação tradicionalmente atribuída a grupos de resposta a incidentes de segurança da informação, embora os incidentes não mais se limitem a tecnologia;
28. **Estratégia de continuidade de serviços**: abordagem do órgão que garante a recuperação dos ativos de informação e a continuidade das atividades críticas ao se defrontar com um desastre, uma interrupção ou com outro incidente maior;
29. **Evento**: qualquer ocorrência observável em um sistema ou rede de uma organização;
30. **Evidência digital**: informação ou dado, armazenado ou transmitido eletronicamente, em modo binário, que pode ser reconhecida como parte de um evento;
31. **Evidência de auditoria**: registros, declarações de fato ou outras informações verificáveis e relevantes para os critérios de auditoria;
32. **Gerenciamento de crise**: decisões e atividades coordenadas que ocorrem em uma organização durante uma crise corporativa, incluindo crises cibernéticas;

33. **Gestão de continuidade de serviços**: processo de gestão global que identifica as potenciais ameaças para uma organização e os impactos nas operações da instituição que essas ameaças, concretizando-se, poderiam causar, fornecendo e mantendo nível aceitável de serviço diante de rupturas e desafios à operação normal do dia a dia;
34. **Gestão de Riscos de Segurança da Informação**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e para equilibrá-los com os custos operacionais e financeiros envolvidos;
35. **Gestão de Segurança da Informação e Comunicações**: conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos;
36. **Gestor da informação**: pessoa responsável pela administração de informações geradas em seu processo de trabalho e/ou sistemas de informação relacionados às suas atividades;
37. **Gestor de Segurança da Informação e das Comunicações**: responsável pelas ações de segurança da informação e comunicações no âmbito do órgão ou entidade da administração pública federal (APF);
38. **Impacto do risco**: efeito resultante da ocorrência do risco;
39. **Informação**: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
40. **Informação sigilosa**: informação submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado e aquela abrangida pelas demais hipóteses legais de sigilo;

41. **Incidente de segurança**: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;
42. **Incidente grave**: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;
43. **Incidente de Segurança da Informação**: evento que viola ou representa ameaça iminente de violação de política de segurança, de política de uso aceitável ou de prática de segurança padrão;
44. **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
45. ***Log* ou registro de auditoria**: registro de eventos relevantes em um dispositivo ou sistema computacional;
46. **Metadados**: conjunto de dados estruturados que descrevem informação primária;
47. **Nível de risco**: magnitude do risco, expressa pelo produto das variáveis impacto e probabilidade;
48. **Plano de Gerenciamento de Incidentes**: plano de ação claramente definido e documentado para ser usado quando ocorrer incidente que basicamente cubra as principais pessoas, recursos, serviços e outras ações que sejam necessárias para implementar o processo de gerenciamento de incidentes;
49. **Política de Segurança da Informação e das Comunicações (POSIC)**: documento aprovado pela autoridade responsável pelo órgão ou entidade da administração pública federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
50. **Preservação de evidência de incidentes em redes computacionais**: processo que compreende a salvaguarda das evidências e dos dispositivos, de modo a garantir que os dados ou metadados não sofram alteração, preservando-se a integridade e a confidencialidade das informações;
51. **Probabilidade do risco**: possibilidade de ocorrência do risco;

52. **Procedimento**: conjunto de ações sequenciadas e ordenadas para o atingimento de um determinado fim;
53. **Quebra de segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
54. **Requisito**: necessidade ou expectativa declarada, geralmente implícita ou obrigatória;
55. **Resiliência**: poder de recuperação ou capacidade de determinada organização resistir aos efeitos de um incidente;
56. **Recursos computacionais**: recursos que processam, armazenam e/ou transmitem informações, tais como aplicações, sistemas de informação, computadores, *notebooks*, servidores de rede, equipamentos de conectividade e infraestrutura;
57. **Resumo criptográfico**: é um método criptográfico que, quando aplicado sobre uma informação, independentemente do tamanho desta, gera resultado único e de tamanho fixo, também chamado de *hash*;
58. **Risco de Tecnologia da Informação e Comunicação (TIC)**: evento capaz de afetar positiva ou negativamente os objetivos da organização nos níveis estratégico, tático e operacional;
59. **Segurança cibernética:** é um conjunto de práticas que protege informação armazenada nos computadores e aparelhos de computação e transmitida através das redes de comunicação, incluindo a Internet e telefones celulares. A Segurança Cibernética se aplica a uma parte da segurança da informação com foco na proteção digital, cuidando das ameaças as informações transportadas por meios cibernéticos. Já a Segurança da informação tem um foco mais amplo, cuidando da redução de riscos no transporte de dados por qualquer meio, seja digital ou não.
60. **Segurança da Informação e Comunicações**: ações que objetivam viabilizar e assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações;
61. **Sistema de gestão de segurança da informação (SGSI)**: políticas, procedimentos, manuais e recursos associados e atividades coletivamente

gerenciadas por uma organização na busca de proteger seus ativos de informação;

62. **Tolerância a risco**: margem que a administração permite aos gestores de suportar o impacto de determinado risco em troca de benefícios específicos, ainda que esse seja superior ao "apetite ao risco" determinado pela organização;
63. **Tratamento da informação classificada**: conjunto de ações referentes à produção, à recepção, à classificação, à utilização, ao acesso, à reprodução, ao transporte, à transmissão, à distribuição, ao arquivamento, ao armazenamento, à eliminação, à avaliação, à destinação ou ao controle de informação classificada em qualquer grau de sigilo; e
64. **Vulnerabilidades:** conjunto de fatores internos ou causa potencial de um incidente indesejado que pode resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.