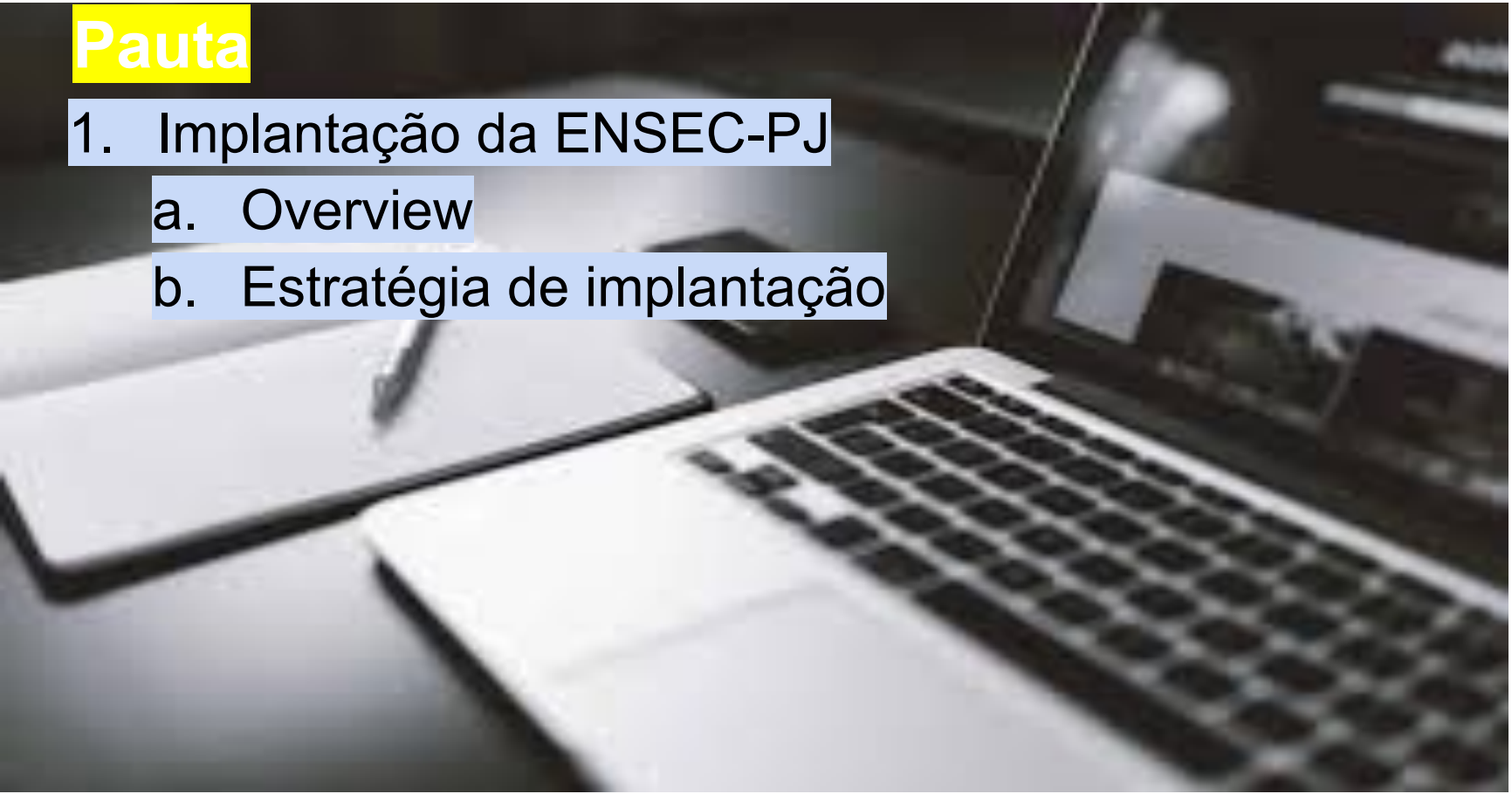
JUSTIÇA DO TRABALHO
TRT da 3ª Região (MG)

Subcomitê de TIC (STIC)

Seção de Segurança da Informação e Comunicação - SINC

JUNHO 2021



Pauta

1. Implantação da ENSEC-PJ
   a. Overview
   b. Estratégia de implantação

Dados atualizados em 23 de junho de 2021

You weren't hacked because you lacked space-age network defenses. Nor because cyber-gurus picked on you. It's far simpler than that

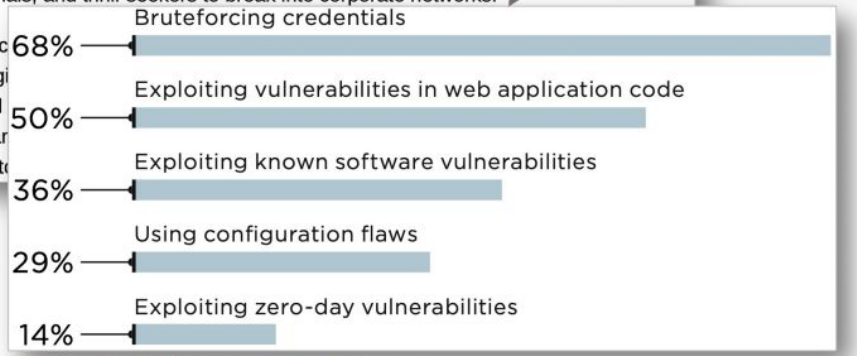
Three little words: Patches, passwords, policies

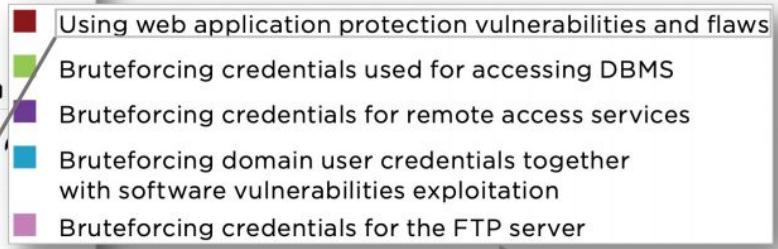
Thu 13 Aug 2020 // 07:06 UTC 31

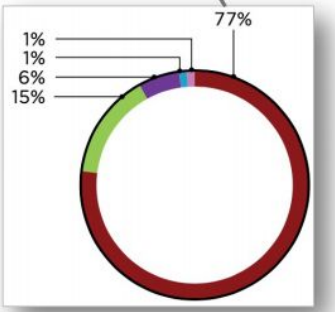
Shaun Nichols in San Francisco BIO EMAIL TWITTER

The continued inability of organizations to patch security vulnerabilities in a timely manner, combined with guessable passwords and the spread of automated hacking tools, is making it pretty easy for miscreants, professionals, and thrill-seekers to break into corporate networks.

This is acc
Technologi
and found
its red tear
available t







https://www.theregister.com/2020/08/13/pentest_networks_fail/
https://www.ptsecurity.com/upload/corporate/ww-en/analytics/external-pentests-2020-eng.pdf

SC MEDIA

NEWS REVIEWS IN DEPTH EVENTS RESOURCE LIBRARY SC SECURITY OPS CENTER SC UK

THE CYBERSECURITY SOURCE SINCE 1989

August 6, 2020

Lesson learned: Failure to patch led to password leak of 900 VPN enterprise servers

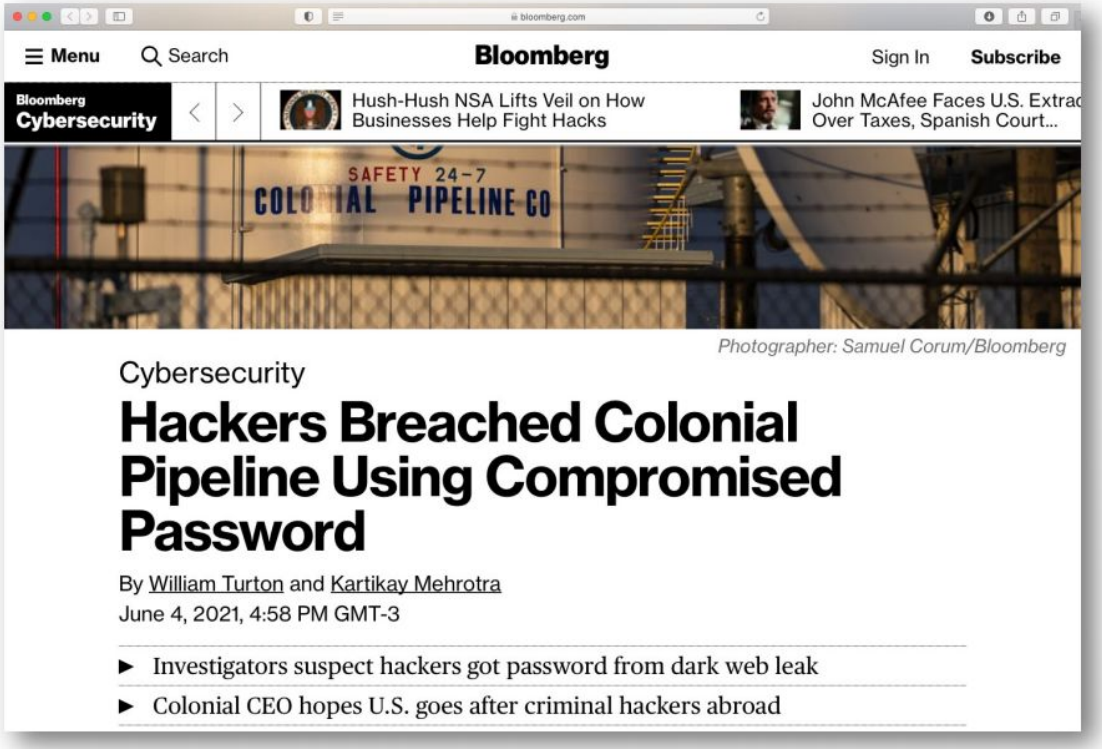
Teri Robinson

Follow @TeriRnNY

Applying a security update to a CVE released more than a year ago could have prevented a hacker from publishing plaintext usernames and passwords, as well as IP addresses, for more than 900 Pulse Secure VPN enterprise servers.

"The lesson here? Patch, patch, patch," said Laurence Pitt, global security strategy director at Juniper Networks. "The fact that this vulnerability allowed for username/cleartext password combinations to be exposed is bad enough, but what makes it unacceptable is that this was reported in a CVE, released over a year ago and fixed in a later version of the product."

https://www.scmagazine.com/home/security-news/patch-fail-led-to-password-leak-of-900-vpn-enterprise-servers/



bloomberg.com

Menu Search **Bloomberg** Sign In **Subscribe**

Bloomberg Cybersecurity

Hush-Hush NSA Lifts Veil on How Businesses Help Fight Hacks

John McAfee Faces U.S. Extrad Over Taxes, Spanish Court...

Photographer: Samuel Corum/Bloomberg

Cybersecurity

Hackers Breached Colonial Pipeline Using Compromised Password

By William Turton and Kartikay Mehrotra
June 4, 2021, 4:58 PM GMT-3

- Investigators suspect hackers got password from dark web leak
- Colonial CEO hopes U.S. goes after criminal hackers abroad

https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password

Resumo sobre os Incidentes Observados pelo CERT.br: **Causas Mais Comuns de Invasões e Vazamentos de Dados**

Ataques mais reportados e mais observados em sensores:

- Força bruta de senhas em serviços protegidos só com conta e senha. Exemplos:
  - *e-mails* e serviços em nuvem
  - acesso remoto e gestão remota de ativos de rede e servidores
- Comprometimento via exploração de vulnerabilidades conhecidas
  - falta de aplicação de correções
  - erros de configuração
  - falta/falha de processos

Veja também: Principais Ataques na Internet: Dados do CERT.br
https://youtu.be/nHh8hHaomFE?t=714
https://cert.br/stats/

Mais de 80% dos incidentes seriam evitados se

- todas as correções (*patches*) fossem aplicadas
- houvesse mais atenção a erros e configurações
- todos os serviços tivessem 2FA/MFA

É necessário focar no básico

- *Patches* + configuração segura (*hardening*)
- Adotar MFA (*Multi-Factor Authentication*)
  - ex: aplicativo autenticador ou *token* (ex: Yubikey)
  - motivos usuais para não adoção
    - diminui a conveniência e pode ter custos
    - requer treinamento dos técnicos e usuários
    - medo de perder acesso aos serviços

Resolução CNJ nº 396/2021 (ENSEC-PJ)

Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ)

Art. 6º São objetivos da ENSEC-PJ:
I – tornar o Judiciário mais seguro e inclusivo no ambiente digital;
II – aumentar a resiliência às ameaças cibernéticas;
III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário; e
IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

Resolução Nº 396 de 07/06/2021

Portaria CNJ n° 162/2021

Art. 1º Aprovar os Anexos I, II e III, desta Portaria, que contêm os seguintes protocolos:
I – Prevenção de Incidentes Cibernéticos do Poder Judiciário (PPINC-PJ);
II – Gerenciamento de Crises Cibernéticas do Poder Judiciário (PGCRC-PJ); e
III – Investigação de Ilícitos Cibernéticos do Poder Judiciário (PIILC-PJ).

Art. 2º Aprovar os Anexos IV, V, VI e VII desta Portaria, que contêm os seguintes Manuais:
I – Proteção de Infraestruturas Críticas de TIC;
II – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital;
III – Gestão de Identidades; e
IV – Política de Educação e Cultura em Segurança Cibernética do Poder Judiciário.

Prazo para implantação:

- Protocolos: imediato
- Manuais: dez/2021

ANEXOS DA PORTARIA Nº 162, DE 10 DE JUNHO DE 2021

Manual de Referência – Proteção de Infraestruturas Críticas de TIC

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.

Manual de Referência – Proteção de Infraestruturas Críticas de TIC

● Controles Mínimos Recomendados

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.

Manual de Referência – Proteção de Infraestruturas Críticas de TIC

- **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

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

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

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 (*backups*) 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

Manual de Referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

- **Capítulo 1: Principais frameworks de referência utilizados**
- **Capítulo 2: Padrões mínimos de Gestão de Riscos de Segurança da Informação**
- **Capítulo 3: Previsões para a fiscalização da adequação dos requisitos de segurança inclusive sob contratação externa e/ou criação de rotina de auditorias cruzadas**
- **Capítulo 4: Confiança digital, prevenção e mitigação de ameaças cibernéticas**
- **Capítulo 5 e Anexo I: Modelo de checklist**

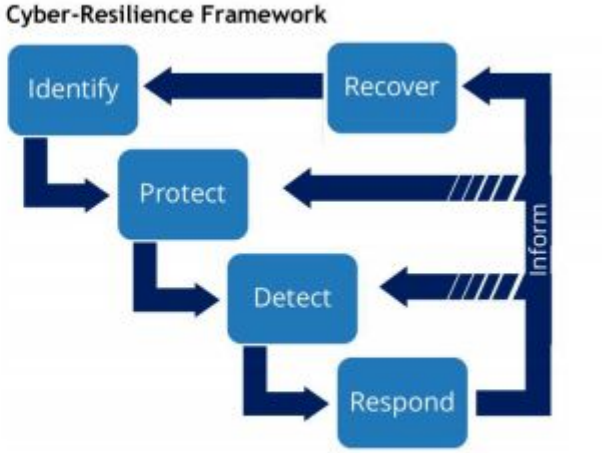
Manual de Referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

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

  *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**.*

Manual de Referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital

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



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

Manual de Referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital - Checklist

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.

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					

Manual de Referência – Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital - Checklist

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					

2.23.	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					

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

- princípio de privilégio mínimo e de segregação de funções,
- processo e de responsáveis por solicitação, **gerenciamento e revogação de contas de acesso, preferencialmente de forma automática**;
- Utilização de login único;
- Registro de trilhas de auditoria que vise ao registro dos acessos a sistema de informação, quais operações foram realizadas e em qual período;
- Definição de requisitos de tamanho, reutilização, critérios de complexidade e período de **expiração de senhas**;
- Empenho pela adoção de **múltiplo fator de autenticação**;
- **regras quanto ao acesso remoto e forma de disponibilização de sistemas e serviços na internet;**
- Gestão de credenciais privilegiadas e restrição ao uso de credenciais genéricas e de uso compartilhado;

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

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					

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

- **Projeto Gestão de Identidade**

Sugestão: revisar o projeto para adequar aos requisitos deste manual

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

- desenvolver ações de capacitação, formação, reciclagem, fomento e conscientização em segurança cibernética;
- 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.
- Competências para Implementação das Ações:
  - Escolas de Formação
  - Área de Gestão de Pessoas
  - Área de Comunicação Social e Institucional

Sugestões para deliberação

1. Inserir projetos/ações no PDTIC.
    - Priorizar, diante do cenário dos principais causas de incidentes de segurança da informação:
        - Gestão de Identidade e Acessos
        - Gerenciamento Contínuo de Vulnerabilidades
2. A SINC nomeará as secretarias responsáveis pelos checklists, depois, compartilhará o documento para que seus gestores confirmem e preencham os itens de controle que já foram atendidos.
3. Propor sugestões para o CTSeg (CSJT).