SENADO FEDERAL
Auditoria

RELATÓRIO DE AUDITORIA N. 02/2023-COAUDTI/AUDIT

Auditoria de Segurança nas Comunicações

-

Ação 5.2 / 2022

Brasília
2023

SENADO FEDERAL
Auditoria

COORDENAÇÃO DE AUDITORIA DE TI

COAUDTI

AUDITOR-GERAL	André Luis Soares da Paixão
COORDENADOR GERAL	David Amaral dos Santos
ASSESSOR TÉCNICO	Allan Del Cistia Mello Bruno Martins Borba
COORDENAÇÃO DE AUDITORIA DE TECNOLOGIA DE INFORMAÇÃO	Yuri Morais Bezerra
COORDENAÇÃO DE AUDITORIA CONTÁBIL E FINANCEIRA	Juliana do Nascimento Leite
COORDENAÇÃO DE AUDITORIA DE CONTRATAÇÕES	Filipe Mesquita Botrel
COORDENAÇÃO DE AUDITORIA DE GESTÃO DE PESSOAS	João Vicente da Rocha Pessoa

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

SENADO FEDERAL
Auditoria

Sumário Executivo

Com a crescente transformação digital e dependência tecnológica dos negócios públicos e privados, a Segurança da Informação e a Segurança Cibernética tornaram-se pré-requisitos para sobrevivência. Diante das ameaças e ataques cibernéticos cada vez mais globalizados, complexos, sofisticados e monetizados, as palavras de ordem são prevenção e resposta tempestiva. Para tal, o primeiro passo reside em identificar e conhecer todos os ativos corporativos (hardware) e de software, bem como promover proativamente a gestão de suas vulnerabilidades.

A Auditoria de Segurança nas Comunicações, Ação 5.2 do PAInt 2022, endereçou essas questões. Teve, portanto, como objetivos "Avaliar se o Senado Federal busca garantir a proteção das informações em suas redes por meio dos recursos de processamento da informação (ativos) que as suportam"; e "Avaliar se o Senado Federal busca garantir a proteção das informações em suas redes por meio do monitoramento e gestão proativa de vulnerabilidades dos seus ativos corporativos e de software".

Durante a execução da presente auditoria cabe ressaltar que o Senado Federal:

- criou o Núcleo de Segurança da Informação em Tecnologia da Informação - NSITI (Ato do Presidente nº 22 de 2022), estrutura vinculada ao Prodasen; e
- designou servidor (Ato do Diretor do Prodasen Nº 1 de 2022) para que assessore tecnicamente o Prodasen no planejamento da implantação do NSITI.

Ao final, a Auditoria de Segurança nas Comunicações encontrou os seguintes 5 (cinco) achados com suas respectivas recomendações, apresentados de forma simplificada:

Achado	Recomendação
O Prodasen emprega ferramentas para o inventário e controle de ativos corporativos (hardware), mas há limitações na abrangência do inventário e na integração entre as ferramentas.	Analisar a viabilidade de aperfeiçoar a prática levando em consideração o Controle 01 do CIS.

SENADO FEDERAL
Auditoria

Achado	Recomendação
O Prodasen emprega ferramentas para o inventário e controle de ativos de software, mas há limitações na abrangência do inventário.	Analisar a viabilidade de aperfeiçoar a prática levando em consideração o Controle 02 do CIS.
O Prodasen emprega ferramentas para a gestão contínua de vulnerabilidades de ativos corporativos e de software, mas há limitações na abrangência de vulnerabilidades geridas e na integração entre as ferramentas.	Analisar a viabilidade de aperfeiçoar a prática levando em consideração o Controle 03 do CIS.
Atuação incipiente do Comitê de Segurança da Informação, tendo em vista a ausência de ações sistemáticas de planejamento, coordenação, acompanhamento, monitoramento e avaliação das ações de Segurança da Informação do Senado Federal.	Aperfeiçoar a atuação do CSI conforme a Política Corporativa de Segurança da Informação do Senado Federal - PCSI e as normas ABNT NBR ISO/IEC 38.500:2015 e ABNT NBR ISO/IEC 27.002:2013.
Ausência de ações de capacitação em segurança da informação para os responsáveis pela implementação dos controles e projetos relativos ao tema.	Elaborar e executar projeto de capacitação em Segurança da Informação e Segurança Cibernética para o corpo técnico alinhando-os ao PDTI e ao PCASF.

SENADO FEDERAL
Auditoria

Lista de Siglas (opcional)

Sigla	Descrição
ABNT	Associação Brasileira de Normas Técnicas
APR	Ato do Presidente
APS	Ato do Primeiro-Secretário
ATC	Ato da Comissão Diretora
APF	Administração Pública Federal
AUDIT	Auditoria do Senado Federal
BASF	Boletim Administrativo do Senado Federal
BRB	Banco de Brasília
CGTI	Comitê de Governança de TI
CIS	Center for Internet Security
CNJ	Conselho Nacional de Justiça
CNN	Cable News Network
COAUDIT	Coordenação de Auditoria de TI
CSI	Comitê de Segurança da Informação
DDoS	Distributed denial of service
DNS	Domain Name System
DSI	Departamento de Segurança da Informação
ENISA	European Union Agency for Cybersecurity
ES	Espírito Santo
EUA	Estado Unidos da América
FBI	Federal Bureau of Investigation
GDF	Governo Distrito Federal
GSI	Gabinete de Segurança Institucional)
IBRASPD	Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados
IoT	Internet da Coisas
JF	Justiça Federal

ILB	Instituto Legislativo Brasileiro
ISO/IEC	International Organization for Standardization / International Electrotechnical Commission
LAI	Lei de Acesso à Informação
MA	Matriz de Achados
MANOP/SF	Manual de Normas Operacionais da Auditoria do Senado Federal
MAVP	Matriz de Achados Versão Preliminar
MITM	Man-in-the-Middle
MP	Matriz de Planejamento
NBR	Norma Brasileira
NIA	Notificação de Início de Auditoria
NIST	National Institute of Standards and Technology
NSITI	Núcleo de Segurança da Informação em Tecnologia da Informação
NUP	Número Único de Protocolo
OGS	Órgãos Governantes Superiores
PAInt	Plano Anual de Auditoria Interna
PCASF	Plano de Capacitação Anual dos Servidores do Senado
PDTI	Plano Diretor de Tecnologia da Informação
PCSI	Política Corporativa de Segurança da Informação
PDG	Portaria do Diretor-Geral
PE	Pernambuco
RA	Relatório de Auditoria
RASF	Regulamento Administrativo do Senado Federal
ROASF	Regulamento Orgânico Administrativo do Senado Federal
RS	Rio Grande do Sul
SA	Solicitação de Informações de Auditoria
SEAUDGTI	Serviço de Auditoria de Governança de TI
SEFTI	Secretaria de Fiscalização de Tecnologia da Informação
SF	Senado Federal
SQL	Structured Query Language

STF	Supremo Tribunal Federal
STJ	Superior Tribunal de Justiça
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TJ	Tribunal de Justiça
TRF	Tribunal Regional Federal
TRT	Tribunal Regional do Trabalho
TSE	Tribunal Superior Eleitoral
US	United States

SENADO FEDERAL
Auditoria

Índice

SENADO FEDERAL
Auditoria

1. Introdução

A presente Auditoria de Segurança nas Comunicações é do tipo Operacional, consta como Ação 5.2 do PAInt 2022 (NUP 00100.089342/2021-75), o qual foi autorizado pela Portaria do 1º Secretário APS nº 5 de 2022 de 17 de março de 2022, publicada no BASF 8246 Seção 1 de 21/03/2022. Segurança nas Comunicações (Seção 13 da ABNT NBR ISO/IEC 27.002:2013) é um dos temas de auditoria elencados como prioritário no "**Estudo de temas de auditorias em segurança da informação para os anos 2021-2024 - COAUDTI/AUDIT/2021**" (NUP 00100.083403/2021-91). Além desta ação de controle, a COAUDTI realizou anteriormente outras duas auditorias relacionadas ao tema de segurança da informação:

- Auditoria de Segurança em Tecnologia da Informação (TI) - RA Nº 1/2019-COAUDTI/AUDIT (NUP 00100.162412/2019-22); e
- Auditoria de Continuidade de Negócios - RA Nº 2/2019-COAUDTI/AUDIT (NUP 00100.160282/2019-93).

Estimativas do TCU[1] de 2021 apontam que "*73,1% dos serviços públicos prestados pelo Governo Federal já são totalmente digitais e 86,7% parcialmente digitais*", entretanto permanecem problemas estruturais remanescentes, entre eles alguns relacionados a Segurança da Informação:

- *"inadequação da macroesturura nacional responsável pela governança e gestão de Segurança da Informação e Segurança Cibernética"*;
- *"incapacidade da APF em responder e tratar incidentes de segurança"*; e
- *"diversas vulnerabilidades de Segurança da Informação e de Segurança Cibernética em grande parte das organizações públicas federais"*.

Frente à crescente transformação digital e dependência tecnológica, bem como aos recorrentes ataques cibernéticos amplamente noticiados na mídia, o tema de Segurança da Informação e Segurança Cibernética vem se tornando cada vez mais crítico e relevante para as organizações públicas e privadas.

Por ocasião da elaboração da Notificação de Início de Auditoria Nº 5.2/2022 - COAUDTI/AUDIT/SF (NUP 00100.058693/2022-15), a COAUDTI elencou no subitem 4.1 alguns possíveis Riscos Institucionais Relacionados:

- Inoperância de serviços e sistemas institucionais;

[1] https://sites.tcu.gov.br/listadealtorisco/seguranca_da_informacao_e_seguranca_cibernetica.html

- Roubo e/ou sequestro de dados sensíveis ou sigilosos;
- Danos à confidencialidade, integridade e disponibilidade das informações críticas para a instituição;
- Extravio de dados, descumprimento de procedimentos e da legislação e/ou regulamentações, invasão de privacidade ou vulnerabilidades nas redes;
- Comprometimento da transparência;
- Imagem e reputação institucional;
- Processos tecnológicos essenciais executados por terceiros e/ou materialização de riscos não conhecidos pela contratante; e
- Tecnologias emergentes.

No setor público, o TCU publicou, em 11/08/2022, matéria sobre análise realizada em instituições federais, na qual verificou-se que ***"menos da metade (44,3%) das organizações realizam algum tratamento sobre ativos não autorizados***"[2].

1.1. Ataques cibernéticos em organizações públicas e privadas no Brasil

Analisando o país como um todo, a Rede CNN publicou em seu portal a matéria jornalística "***Levantamento mostra que ataques cibernéticos no Brasil cresceram 94% - País é o 2º na América Latina com mais ataques cibernéticos em 2022***"[3], dando destaque especial para o protagonismo negativo do Brasil na América Latina.

Informações sobre os principais ataques cibernéticos notificados por fontes oficiais de organizações brasileiras vítimas de incidentes, incluindo as públicas, são publicadas periodicamente pela revista Security Report no "**Painel de Incidentes Cibernéticos**":

2022: https://www.securityreport.com.br/email/InfoSR2022_.html

2021: https://www.securityreport.com.br/email/InfoSR2021_Jan_a_dez.html

O Instituto Brasileiro de Segurança, Proteção e Privacidade de Dados - IBRASPD - também publica os incidentes relevantes ocorridos no mercado brasileiro e que são acompanhados pelo instituto: https://www.ibraspd.org/incidentes. Diversos órgãos públicos e empresas estatais constam dessa publicação.

[2] https://portal.tcu.gov.br/imprensa/noticias/tcu-analisa-seguranca-cibernetica-de-instituicoes-federais.htm
[3] https://www.cnnbrasil.com.br/tecnologia/levantamento-mostra-que-ataques-ciberneticos-no-brasil-cresceram-94/

1.2. Cenário de incidentes cibernéticos na Administração Pública do Brasil

Infelizmente, ataques cibernéticos têm sido recorrentes contra organizações públicas, atingindo administração direta e indireta, nas três esferas (Federal, Estadual e Municipal) e nos três poderes (Executivo, Judiciário e Legislativo). A tabela abaixo exemplifica uma breve lista de ataques divulgados pela mídia oficial / especializada / jornalística que se destacaram:

Data	Título	Link
25/06/11	Veja lista de sites do **governo** afetados por onda de ataques virtuais[4]	https://g1.globo.com/tecnologia/noticia/2011/06/veja-lista-de-sites-do-governo-afetados-por-onda-de-ataques-virtuais.html
09/11/20	**STJ** é vítima de ransomware e tem seus dados e os backups criptografados	https://thehack.com.br/stj-e-vitima-de-ransomware-e-tem-seus-dados-e-os-backups-criptografados/
27/11/20	**TRF-1** sofre ataque hacker e site está fora do ar nesta sexta-feira	https://www.conjur.com.br/2020-nov-27/trf-sofre-ataque-hacker-site-fora-ar-nesta-sexta-feira
17/12/20	Em 2020, órgãos do **GDF** sofreram 1,9 mil ataques cibernéticos por dia. Até novembro, a Secretaria de Economia registrou 652.080 tentativas de acesso aos servidores virtuais do governo	https://www.sinafite-df.org.br/2020/12/17/em-2020-orgaos-do-gdf-sofreram-19-mil-ataques-ciberneticos-por-dia-ate-novembro-a-secretaria-de-economia-registrou-652-080-tentativas-de-acesso-aos-servidores-virtuais-do-governo/
06/07/21	**Governo** é o principal alvo de ataques cibernéticos no Brasil, revela análise	https://canaltech.com.br/seguranca/governo-e-o-principal-alvo-de-ataques-ciberneticos-no-brasil-revela-analise-189050/
30/11/21	Site da **Assembleia Legislativa do Amapá** é alvo de ataque hacker	https://g1.globo.com/ap/amapa/noticia/2021/11/30/site-da-assembleia-legislativa-do-amapa-e-alvo-de-ataque-hacker.ghtml
13/12/21	Órgãos do **governo** sofrem novo ataque de hackers, diz GSI	https://agenciabrasil.ebc.com.br/geral/noticia/2021-12/orgaos-do-governo-sofrem-novo-ataque-de-hackers-diz-gsi
10/01/22	Um mês após ataque hacker, **Ministério da Saúde** diz que integração entre sistema de dados foi restabelecida na sexta	https://oglobo.globo.com/saude/um-mes-apos-ataque-hacker-ministerio-da-saude-diz-que-integracao-entre-sistema-de-dados-foi-restabelecida-na-sexta-1-25347878
11/03/22	**Procuradoria-Geral da República** foi alvo de ataque criminoso de hackers	https://diariodopoder.com.br/coluna-claudio-humberto/procuradoria-geral-da-republica-foi-alvo-de-ataque-criminoso-de-hackers
06/04/22	7 dias após ataque hacker, sistemas do **TRF-3** continuam fora do ar	https://www.conjur.com.br/2022-abr-06/ataque-hacker-sistemas-trf-continuam-fora-ar
28/04/22	**Escola Superior do Ministério Público da União** sofre ataque hacker	https://www.convergenciadigital.com.br/Seguranca/Escola-Superior-do-Ministerio-Publico-da-Uniao-sofre-ataque-hacker-60135.html
08/09/22	Após ataque hacker, **Prefeitura do Rio** precisa trocar 20 mil computadores	https://www.gazetadopovo.com.br/republica/breves/apos-ataque-hacker-prefeitura-do-rio-precisa-trocar-20-mil-computadores/
06/10/22	**Banco BRB** sofre ataque cibernético e chantagem milionária, diz site	https://www.istoedinheiro.com.br/banco-brb-sofre-ataque-cibernetico-e-chantagem-milionaria-diz-site/

[4] Inicialmente apresentado no "Estudo de temas de auditorias em segurança da informação para os anos 2021-2024 - COAUDTI/AUDIT/2021" (NUP 00100.083386/2021-91).

SENADO FEDERAL
Auditoria

Data	Título	Link
12/12/22	**Planalto** diz que 191 PCs foram afetados em suposto ciberataque	https://www.cisoadvisor.com.br/planalto-diz-que-191-pcs-foram-afetados-em-suposto-ciberataque/
05/01/23	Ataque hacker ao sistema do **CNJ** faz Moraes determinar a sua própria prisão	https://www.correiobraziliense.com.br/politica/2023/01/5063985-ataque-hacker-ao-sistema-do-cnj-faz-moraes-determinar-a-sua-propria-prisao.html
11/01/23	Incidente em terceiro impacta operação da **Câmara Municipal de Curitiba**	https://www.securityreport.com.br/destaques/incidente-em-terceiro-impacta-operacao-da-camara-municipal-de-curitiba/#.Y87mCJLMJPY

As consequências são quase sempre desastrosas, incluindo paralisação dos principais serviços prestados por dias ou semanas, perda permanente de dados e alteração de dados sensíveis.

A situação dos ataques hackers no Poder Judiciário, p.ex., é bem peculiar e a revista Consultor Jurídico publicou matéria intitulada "**Em 18 meses, hackers violaram sistemas de tribunais no Brasil a cada 41 dias**"[5], na qual relata os principais ataques vividos pela Justiça, entrevista magistrados e advogados especialistas em direito digital além de apresentar a seguinte relação de tribunais atacados entre novembro de 2020 e abril de 2022. Importante notar que nesse intervalo de 18 meses ocorreram ataques em diversos tribunais superiores e até estaduais, do sul ao nordeste do Brasil e que alguns tribunais sofreram ataques mais de uma vez.

Data	Tribunal	Data	Tribunal
Nov/20	TRF-1	Abr/21	TJ-RS
Nov/20	STJ	Ago/21	TSE
Nov/20	TSE	Out/21	TRT-RS
Jan/21	TRF-3	Fev/22	TRT-ES
Jul/21	7ª Vara Criminal Federal SP	Mar/22	TRF-3
Mai/21	STF	Abr/22	JF-PE

Destaca-se o comentário do juiz auxiliar da presidência do Conselho Nacional de Justiça à época da publicação, Alexandre Libonati de Abreu [6]: "*A média de um (ataque) a cada 41 dias não é alta se comparada a ataques sofridos por estabelecimentos bancários ou sítios de compra, por exemplo, mas, independentemente da frequência, qualquer ataque a um órgão do Judiciário pode*

[5] https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais
[6] https://www.conjur.com.br/2022-abr-15/onda-invasoes-hackers-estruturas-tecnologicas-tribunais

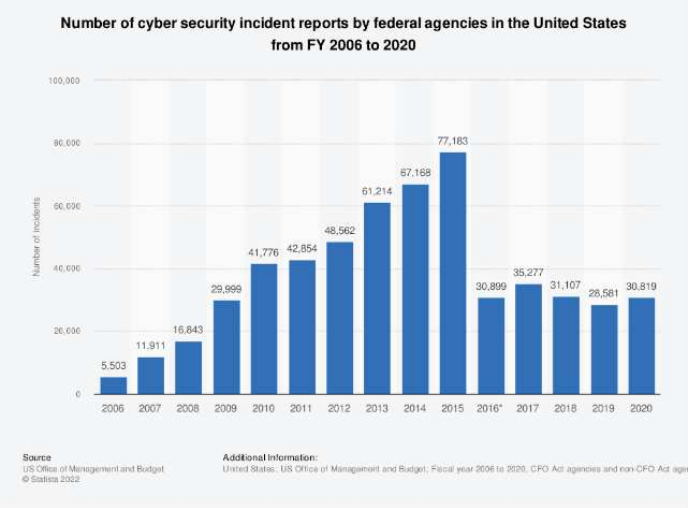
gerar consequências gravíssimas, e deve servir de alerta para que o assunto 'segurança cibernética' seja visto com a mesma (ou até maior) seriedade com que se vê a segurança física de instalações".

1.3. Cenário de Incidentes Cibernéticos na Administração Pública nos EUA e na Europa

Os Estados Unidos é o país nas américas com mais ataques cibernéticos e conforme pode-se notar também tem seus órgãos governamentais envolvidos em ataques de Segurança Cibernética:

Data	Título	Link
18/12/20	O que se sabe sobre o pior ataque hacker ao **governo americano**	https://www.gazetadopovo.com.br/mundo/o-que-se-sabe-sobre-o-pior-ataque-hacker-ao-governo-americano/
22/12/20	Ataque hacker contra **governo dos EUA** atingiu dezenas de contas email do Tesouro	https://www1.folha.uol.com.br/mundo/2020/12/ataque-hacker-contra-governo-dos-eua-atingiu-dezenas-de-contas-de-email-do-tesouro.shtml
10/02/21	Ransomware attacks against U.S. government entities: 5 key observations and takeaways for municipalities	https://www.sungardas.com/en-us/blog/ransomware-attacks-on-us-government-entities/
05/11/21	EUA pagam US$ 10 mi por hackers do ransomware que atacou Colonial Pipeline	https://tecnoblog.net/noticias/2021/11/05/eua-oferecem-10-milhes-dolares-informacoes-ransomware-darkside/
25/08/22	10 Notable Cyber Attacks on Government Agencies	https://arcticwolf.com/resources/blog/notable-cyber-attacks-on-government-agencies/

O gráfico a seguir do site Statista apresenta o número de incidentes de Segurança Cibernética reportado por agências federais norte-americanas entre 2006/2020[7]:

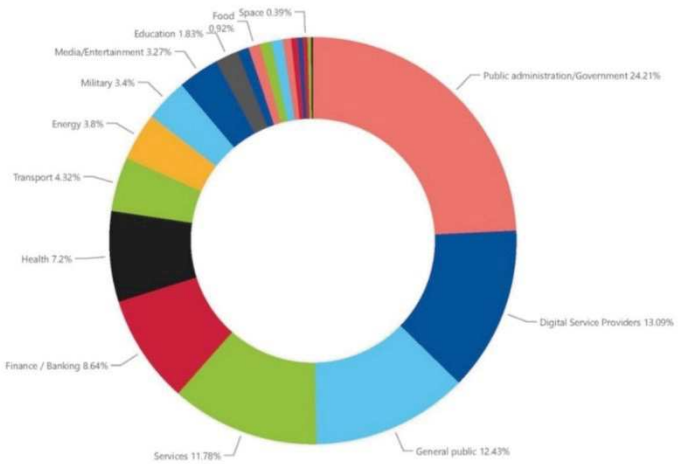


[7] https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/

Frente a esse cenário importantes estruturas governamentais como o Departamento de Justiça e o FBI (Federal Bureau of Investigation) já se dedicam ao tema há anos. Nota do Departamento de Justiça Norte Americano[8] sobre a fala do representante do Procurador-geral, Rod J. Rosenstein, no Cambridge Cyber Summit em 04/10/2017, p.ex., dá o tom da ameaça e destaca que o FBI estima que ataques de ransomware infectaram mais de 100 mil computadores diariamente mundo afora e que esse número continua a crescer, bem como que o pagamento de resgate (*ransom*) se aproxima de US$ 1 bilhão anualmente.

Já na Europa a ENISA - European Union Agency for Cybersecurity monitora e publica anualmente o relatório **ENISA Threat Landscape**, que está em sua décima edição, com o panorama das ameaças cibernéticas. Na edição de 2022 (horizonte de tempo de julho 2021 a junho de 2022) gráfico a seguir do "ENISA Threat Lands 2022" [9] expressa, sobre o estudo europeu, que praticamente 1/4 (24,21%) dos incidentes ocorreram no segmento **Administração Pública / Governo**.

Figure 4: Targeted sectors per number of incidents (July 2021-June 2022)



O Apêndide I apresenta uma série de informações complementares relacionados à Segurança da Informação e Segurança Cibernética em nível global.

[8] https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-cambridge-cyber-summit
[9] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

1.4. Indução de Boas Práticas pelo TCU

O Tribunal de Contas da União (TCU), Secretaria de Fiscalização de Tecnologia da Informação (Sefti), tem tido forte atuação em fiscalizações relacionadas à Segurança da Informação há pelo menos 10 anos. Nessa linha de atuação do controle externo, merece destaque o guia "**Boas práticas em segurança da informação**", publicado inicialmente em 2012 e hoje em sua 4ª edição[10].

Mais recentemente, com o objetivo de conscientizar e induzir a adoção de boas práticas de Segurança da Informação e Segurança Cibernética na APF, o TCU publicou o Sumário Executivo da "**Estratégia de Fiscalização do TCU em Segurança da Informação e Segurança Cibernética 2020-2023**"[11] onde apresenta um conjunto de ações que irá promover no período, concernentes ao tema.

Resultante de uma das ações elencadas nessa estratégia de fiscalização, o Acórdão 1.768/2022-TCU-Plenário contém recomendações para diversos Órgãos Governantes Superiores – OGS, inclusive para o Senado. Ainda nessa linha, o TCU publicou, em agosto de 2022, o Sumário Executivo "***Cinco Controles de Segurança Cibernética para ontem***"[12] onde recomenda aos órgãos a adoção de cinco controles críticos do CIS - Center for Internet Security, "para ontem" expressando assim a urgência da implementação de medidas de controle institucionais.

Para o **Senado Federal**, em particular, o TCU fez recomendações explicitadas por meio do Aviso nº 274 - GP/TCU de 21/03/2022 (NUP 00100.034925/2022-40) e do Acórdão 1.768/2022 TCU-Plenário[13] de 03/08/2022:

Aviso nº 274	Acórdão 1.768	Recomendação
280.3.	9.3.	*recomendar, com fundamento no art. 11 da Resolução - TCU 315/2020, ao Senado Federal [...] que adotem as ações a seguir:*
280.3.1.	9.3.1.	***implementar com urgência controles críticos e medidas de segurança cibernética**, de modo a tratar, em especial, as deficiências apontadas neste ciclo do acompanhamento, naquilo que lhes for aplicável, **observando boas práticas como as preconizadas pelo Center for***

[10] https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24F0A728E014F0B226095120B
[11] https://portal.tcu.gov.br/estrategia-de-fiscalizacao-do-tcu-em-seguranca-da-informacao-e-seguranca-cibernetica-2020-2023.htm
[12] https://portal.tcu.gov.br/5-controles-de-seguranca-cibernetica.htm
[13] https://pesquisa.apps.tcu.gov.br/#/documento/processo/*/NUMEROSOMENTENUMEROS%253A3630120213/DTAUTUACAOORDENACAO%2520desc%252C%2520NUMEROCOMZEROS%2520desc/0/%2520

SENADO FEDERAL
Auditoria

Aviso nº 274	Acórdão 1.768	Recomendação
		Internet Security e pela norma técnica ABNT NBR ISO/IEC 27002:2013;
280.3.2.	9.3.2.	*adotar, na inexistência de normativo próprio tratando desses temas,* ***as práticas previstas nos Decretos 9.637/2018 e 10.222/2020****, que regem aspectos gerais relacionados à segurança da informação e à segurança cibernética no âmbito da Administração Pública federal, bem como as constantes das instruções normativas e de normas complementares editadas pelo Gabinete de Segurança Institucional da Presidência da República aplicáveis a esse respeito;* *(https://www.gov.br/gsi/pt-br/assuntos/dsi/legislacao)*
280.3.3.	9.3.3.	***formalizar, junto ao Gabinete de Segurança Institucional da Presidência da República, ato de adesão à Rede Federal de Gestão de Incidentes Cibernéticos****, nos termos do § 4º do art. 7º do Decreto 10.748/2021;*

1.5. Organização da Segurança da Informação e Cibernética no Senado Federal

No Senado Federal o **Prodasen** é o órgão responsável por "***gerir a segurança da informação do Senado no âmbito da tecnologia da informação***" conforme estabelecido no regulamento administrativo, Art. 24 do ROASF 2022 (APR 22/2022)[14]:

> *À Secretaria de Tecnologia da Informação (Prodasen) compete prover, por meio de recursos próprios ou de terceiros, serviços, soluções, suporte e infraestrutura de tecnologia da informação; gerir a tecnologia da informação do Senado Federal; implementar a estratégia de tecnologia da informação; propor inovações nos processos finalísticos e de apoio do Senado, com uso de tecnologia da informação; propor padrões, normas, métodos e processos para uso da tecnologia da informação e monitorar sua aplicação; integrar iniciativas de adoção de novas soluções de tecnologia da informação por outras unidades da Casa;* ***gerir a segurança da informação do Senado no âmbito da tecnologia da informação; gerenciar os riscos operacionais do Senado com origem em tecnologia da informação****; e executar outras atribuições correlatas.*

O Senado possui uma **Política Corporativa de Segurança da Informação - PCSI**, conforme preconizado pelas boas práticas, a qual estabelece responsabilidades e dá diretrizes sobre como o tema deve ser tratado na instituição. Nessa política, tem papel central na governança da Segurança da Informação o **Comitê de Segurança da**

[14] Na fase de planejamento desta auditoria, as competências do Prodasen estavam definidas no Art. 224 do RASF 2018 (ATC 02/2018), as quais, após atualização do RASF, passaram a ser definida pelo APR 22/2022, mas as competências do Prodasen não sofreram mudanças.

Informação - CSI, o qual tem suas competências estabelecidas no Art. 15 do ATC nº 9 de 2017:

> *I - **planejar, coordenar, acompanhar, monitorar e avaliar, em conjunto com os setores competentes, a implementação da PCSI** e das normas complementares e as ações de segurança da informação;*
>
> *II - **analisar e formular ações de segurança da informação** para o Senado Federal, considerando a conformidade com a legislação e as recomendações e boas práticas pertinentes;*
>
> *III - fomentar a cultura de segurança da informação no Senado Federal;*
>
> *IV - **planejar a capacitação dos usuários em segurança** da informação;*
>
> *V - apresentar propostas de compatibilização das normas do Senado Federal que tenham impacto em segurança da informação com a PCSI;*
>
> *VI - prestar assessoria em segurança da informação ao Senado Federal;*
>
> *VII - **propor alocação de recursos necessários às ações de segurança da informação;***
>
> *VIII - apoiar as áreas competentes do Senado Federal na definição de metodologias, processos e tecnologias em segurança da informação, contemplando a classificação da informação, a gestão de riscos em segurança da informação, o uso dos recursos de informação, a gestão da continuidade de negócios e a gestão de incidentes de segurança da informação;*
>
> *IX - **formular, avaliar, monitorar e divulgar indicadores de segurança da informação** no âmbito do Senado Federal;*
>
> *X - instituir CTSI para tratar de assunto específico afeto à segurança da informação, o qual será integrado por servidores indicados pelos titulares das áreas temáticas relacionadas;*
>
> *XI - revisar a PCSI no máximo a cada três anos;*
>
> *XII - estabelecer permanente interlocução com outros comitês de segurança da informação criados no âmbito da Administração Pública.*

O **Núcleo de Segurança da Informação em Tecnologia da Informação - NSITI**, também previsto na Política Corporativa de Segurança da Informação - PCSI, foi criado recentemente, em novembro de 2022, e terá papel fundamental na implementação das ações de Segurança da Informação no Senado Federal, tendo em vista suas competências definidas no inciso IV do § 2º do Art. 24 do ROASF 2022:

> *"ao Núcleo de Segurança da Informação em Tecnologia da Informação compete secretariar o Comitê de Segurança da Informação - CSI; atuar como gestor de segurança da informação do Senado Federal; receber e encaminhar ao CSI as demandas de ações corporativas de segurança da informação; oficiar as áreas envolvidas no âmbito dos Comitês Temáticos de Segurança da Informação - CTSI para a indicação de participantes; propor e coordenar, em conjunto com as demais áreas competentes do Senado Federal: a formulação, a avaliação e o monitoramento de indicadores de segurança da informação*

em tecnologia da informação - TI; as ações de segurança da informação em TI; os processos de gestão da continuidade de TI; os processos de gestão de riscos de segurança da informação em TI; e os processos de tratamento de incidentes de segurança da informação em TI; prestar assessoria em segurança da informação em TI às demais áreas do Senado Federal; prospectar tecnologias aplicáveis à segurança da informação em TI, sem prejuízo da atuação das demais áreas competentes do Senado Federal; reportar os incidentes de segurança da informação em TI ao CSI; apresentar os indicadores de segurança da informação em TI ao CSI; receber das unidades administrativas, dos usuários internos e colaboradores as ocorrências de incidentes de segurança da informação de que tenham conhecimento; e executar outras atribuições correlatas".

Frente ao exposto, a presente Ação de Auditoria se prestou a analisar os controles implementados nos processos relacionados à Segurança da Informação e Cibernética do Senado Federal, possibilitando assim fornecer subsídios para a gestão aprimorar seus mecanismos e sistemáticas.

2. Objetivos

O Objeto da presente Ação de Auditoria é "*Sistemas de Gestão da Segurança da Informação e Segurança Cibernética dos ativos corporativos e de software das redes do Senado Federal, bem como suas vulnerabilidades*".

É Objetivo da presente Ação de Auditoria "*Avaliar em que medida o Senado garante a proteção das informações em redes e dos recursos de processamento da informação que os apoiam*", conforme explicitado no Plano Individual de Auditoria Nº 5.2/2022 - COAUDTI/AUDIT/SF.(NUP 00100.047173/2022-87).

São Objetivos Específicos da presente Ação de Auditoria, conforme o plano mencionado anteriormente:

Objetivo Específico 1: "*Avaliar se o Senado Federal busca garantir a proteção das informações em suas redes por meio dos recursos*[15] *de processamento da informação (ativos) que as suportam*"; e

Objetivo Específico 2: "*Avaliar se o Senado Federal busca garantir a proteção das informações em suas redes por meio do monitoramento e gestão proativa de vulnerabilidades dos seus ativos corporativos e de software*".

[15] Explica-se: por meio da gestão do inventário dos recursos de processamento.

Com a finalidade de alcançar os objetivos supracitados, selecionaram-se inicialmente como Áreas Envolvidas o Comitê de Segurança da Informação (CSI) e a Secretaria de Tecnologia da Informação (Prodasen) e, posteriormente, o Instituto Legislativo Brasileiro (ILB). Adotaram-se ainda os seguintes critérios na condução da presente Ação de Auditoria:

- Principais:
    - Estudo de temas de auditorias em segurança da informação para os anos 2021-2024 - COAUDTI/AUDIT/2021, NUP 00100.083403/2021-91;
    - Política Corporativa de Segurança da Informação do Senado Federal - PCSI, instituída pelo ATC nº 9 de 2017;
    - Estratégia de Fiscalização do TCU em segurança da informação e segurança cibernética 2020-2023;
    - Normas ABNT NBR ISO/IEC 27.002, sobre Segurança da Informação e Segurança Cibernética;
    - Framework de Segurança Cibernético do NIST - *National Institute of Standards and Technology;*
    - Framework de Controles Críticos de Segurança do CIS - *Center for Internet Security;*
- Subsidiários:
    - Política de Gestão de Riscos Organizacionais do Senado Federal, instituída pelo ATC nº 16 de 2013;
    - Política de Governança Corporativa e Gestão Estratégica do Senado Federal, instituída pelo ATC nº 3 de 2022;
    - Acórdãos do TCU sobre Segurança da Informação e Segurança Cibernética;
    - Acórdãos do TCU sobre Governança de TI e Governança Corporativa Pública;
    - Guia de Boas práticas em segurança da informação do TCU, 4ª edição de 2012;
    - Estratégia Nacional de Segurança Cibernética - E-Ciber, Decreto Nº 10.222, de 5 de fevereiro de 2020;

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

- Guias e publicações do DSI/GSI (Departamento de Segurança da Informação/Gabinete de Segurança Institucional) sobre Segurança da Informação;
- Cartilha de Segurança para Internet - Versão 4.0 CERT.BR, 2012; e
- Estratégia e Governança Cibernéticas do Poder Judiciário, CNJ – Conselho Nacional de Justiça.

3. Escopo

O Escopo da presente Ação de Auditoria ateve-se aos "*Mecanismos e sistemáticas empregados pelo Senado Federal visando garantir a proteção das informações que trafegam pelos recursos de processamento de informação (ativos) das redes do Senado Federal*" com foco na:

- Identificação e ciência/conhecimento atualizado de todos os ativos corporativos (hardware) e de software das redes do Senado Federal; e na
- Gestão contínua e proativa de vulnerabilidades associadas a esses ativos.

À luz do Aviso nº 274 - GP/TCU de 21/03/2022 (NUP 00100.034925/2022-40)[16], foi dado enfoque nos Controles Críticos do CIS, Versão 8[17]:

- Controle 01 - Inventário e controle de ativos corporativos;
- Controle 02 - Inventário e controle de ativos de software; e
- Controle 07 - Gestão contínua de vulnerabilidades.

4. Questões de Auditoria

A fim de conduzir a presente Ação de Auditoria formularam-se as seguintes Questões de Auditoria, conforme explicitado no Plano Individual de Auditoria Nº 5.2/2022 - COAUDTI/AUDIT/SF (NUP 00100.047173/2022-87):

Questão de Auditoria 1: "*Em que medida o SF implementa mecanismos e sistemáticas com o objetivo de assegurar a proteção das informações em redes e dos recursos de processamento da informação (ativos de hardware e software) que as suportam?*" e

[16] https://portal.tcu.gov.br/fiscalizacao-de-tecnologia-da-informacao/atuacao/fiscalizacoes/
[17] https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7BE7E97D017C4DAEAD1E11B4

SENADO FEDERAL
Auditoria

Questão de Auditoria 2: "*Em que medida o SF implementa mecanismos e sistemáticas com o objetivo de avaliar, rastrear e corrigir continuamente as vulnerabilidades dos ativos (hardware e software) das redes do Senado Federal?*".

5. Metodologia

Com a finalidade de alcançar os Objetivos e responder as Questões da presente Ação de Auditoria empregaram-se junto às áreas envolvidas os seguintes procedimentos de Auditoria:

I - Inspeção;

II - Observação;

III - Análise Documental; e

IV - Indagação escrita ou oral (entrevista).

A COAUDTI encaminhou, em 25/05/2022, a Notificação de Início de Auditoria – NIA para as áreas envolvidas:

- Ofício Nº 30/2022/AUDIT/SF para o CSI (NUP 00100.060006/2022-21); e
- Ofício Nº 31/2022/AUDIT/SF para o Prodasen (NUP 0100.060009/2022-65).

Realizou a Reunião de Abertura da Auditoria de Segurança nas Comunicações (Ação 5.2) com o CSI e o Prodasen em 08/06/2022 (NUP 00100.067345/2022-39-2).

Realizou nova reunião com as áreas envolvidas em 29/06/2022 (NUP 00100.083560/2022-87) para que essas áreas apresentassem seus processos internos (*modus operandi*) para a gestão da segurança nas comunicações e para a gestão de riscos relacionados.

A COAUDTI encaminhou então a Solicitação de Informações de Auditoria – Sas para as áreas envolvidas:

- Solicitação de Auditoria Nº05/COAUDTI/AUDIT/SF para o Prodasen (NUP 00100.082398/2022-80) de 15/07/2022; e
- Solicitação de Auditoria Nº06/COAUDTI/AUDIT/SF para o CSI (NUP 00100.085248/2022-28) de 22/07/2022.

A COAUDTI teve também a oportunidade de participar do Workshop Prodasen promovido pelo NQPPPS sobre "Vulnerabilidades em Aplicações – identificação e

tratamento de vulnerabilidades conhecidas em aplicações" (NUP 0100.150583/2022-12) ocorrido em 08/09/2022.

Diante das respostas recebidas e informações colhidas, a COAUDTI promoveu reuniões/diligências virtuais com as áreas envolvidas:

- Reunião com o Prodasen para demonstração dos procedimentos empregados para Gestão de Ativos e de Vulnerabilidades (NUP 00100.150583/2022-12-1) em 22/09/2022;
- Reunião com o CSI para explicação da atuação do Comitê e entendimento das Atas do Colegiado no que tange a Gestão de Ativos e de Vulnerabilidades (NUP 00100.150583/2022-12-2) em 22/09/2022; e
- Reunião com o Prodasen para continuação da demonstração dos procedimentos empregados para Gestão de Ativos e de Vulnerabilidades (NUP 00100.150583/2022-12-3) em 26/09/2022.

A documentação com informações e evidências recebidas das áreas envolvidas, bem como a documentação gerada pela COAUDTI, no âmbito desta auditoria foram classificadas como "reservadas", por conterem informações relacionadas à segurança cibernética da organização. A classificação da informação foi feita nos termos do art. 23, inciso VII, c/c o art. 24, § 1º, inciso III, da Lei 12.527/2011 (Lei de Acesso à Informação - LAI), bem como com o Manual de Transparência e Classificação de Informações do Senado Federal, aprovado pelo ATC 06/2017, conforme trecho a seguir:

> *São passíveis de classificação em reservadas, secretas ou ultrassecretas as informações cuja divulgação ou acesso irrestrito possam:*
>
> *(...)*
>
> *Pôr em risco a segurança de instituições ou de altas autoridades nacionais ou estrangeiras e seus familiares, dentre as quais:*
>
> *(...)*
>
> *Análises de risco e achados de auditorias que exponham fragilidades relacionadas à segurança física de pessoas e à segurança da informação, enquanto as recomendações aceitas pela autoridade administrativa não tenham sido integralmente implementadas.*

Ato contínuo, a COAUDTI em 16/11/22 cadastrou no SIGAD a Matriz de Achados Versão Preliminar - MAVP (NUP 00100.143047/2022-52) e encaminhou às áreas envolvidas para manifestação das mesmas. Foi proposto pela COAUDTI uma reunião para esclarecer e sanar dúvidas quanto ao conteúdo da MAVP, mas os interlocutores

das unidades auditadas entenderam não haver necessidade, considerando que o conteúdo da Matriz, em conjunto com as explicações dadas durante a execução do trabalho, estavam claros o suficiente para elaboração da manifestação da gestão. Cabe ainda salientar que, frente a realidade encontrada, envolveu-se mais uma área, a saber: ILB - Instituto Legislativo Brasileiro.

Todas as áreas envolvidas manifestaram-se tempestivamente e suas manifestações são abordadas no item 8. Por fim passou-se então a construção do presente Relatório de Auditoria.

6. Alinhamento aos Objetivos Estratégicos

A presente Ação de Auditoria endereça e contribui direta ou indiretamente com os seguintes Objetivos Estratégicos do Senado Federal explicitados no Ato da Comissão Diretora - ATC Nº 5, de 2015:

1) **Aumentar a eficiência e a racionalidade no uso dos recursos públicos** - Iniciativas que, direta ou indiretamente, tenham como consequência o aumento da eficiência e da racionalidade devem ser valorizadas. O alcance da eficiência será monitorado e avaliado com o auxílio de indicadores de gestão.
2) **Melhorar de maneira contínua os processos de trabalho** - Os processos de trabalho devem estar definidos, mapeados e normatizados, bem como monitorados e avaliados de maneira periódica e contínua. Deve ocorrer o fortalecimento e capacitação da gestão para que seja mais eficiente, econômica e sustentável.
3) **Valorizar as pessoas** - A valorização das pessoas deve ser um dos pilares da eficiência do Senado Federal. Essa valorização deve ocorrer por meio do desenvolvimento de competências necessárias para que exerçam suas funções, da melhoria do ambiente de trabalho e especialmente do tratamento equânime e da ética e do respeito nas relações.
4) **Fortalecer a transparência e a comunicação** - Deve-se valorizar iniciativas que tornem o processo de comunicação mais célere, com mais qualidade, mais adequado às necessidades dos receptores e mais moderno. Todas as ações devem ser comunicadas com transparência para a sociedade.
6) **Preservar a memória do Senado** - Promover a proteção e organização dos documentos e bens materiais e imateriais do Senado, de forma a preservar sua memória e permitir, de acordo com a lei, acesso amplo e fácil ao acervo, que é parte importante da história e da cultura da nossa instituição e do nosso País.

7) **Priorizar as atividades fim do Senado** - Aperfeiçoar continuamente o processo legislativo e as ações de fiscalização, por meio de recursos tecnológicos, processuais e da avaliação do impacto legislativo, visando fortalecer a representatividade do Parlamento.

7. Achados de Auditoria

Frente às informações coletadas na presente Ação de Auditoria a COAUDTI apresentou a Matriz de Achados Versão Preliminar - MAVP (NUP 00100.143047/2022-52) para manifestação das áreas evolvidas. Cabe salientar que no decorrer da presente Ação verificou-se a necessidade de envolver mais uma área, o ILB - Instituto Legislativo Brasileiro, a fim de aprimorar a gestão de recursos humanos, sobretudo no que tange a capacitação em Segurança da Informação e Segurança Cibernética.

A Auditoria de Segurança nas Comunicações, Ação 5.2 do PAInt 2022, encontrou os seguintes Achados de Auditoria:

Nº Achado	Descrição
1	O Prodasen emprega ferramentas para o inventário e controle de ativos corporativos (hardware), mas há limitações na abrangência do inventário e na integração entre as ferramentas.
2	O Prodasen emprega ferramentas para o inventário e controle de ativos de software, mas há limitações na abrangência do inventário.
3	O Prodasen emprega ferramentas para a gestão contínua de vulnerabilidades de ativos corporativos e de software, mas há limitações na abrangência de vulnerabilidades geridas e na integração entre as ferramentas.
4	Atuação incipiente do Comitê de Segurança da Informação, tendo em vista a ausência de ações sistemáticas de planejamento, coordenação, acompanhamento, monitoramento e avaliação das ações de Segurança da Informação do Senado Federal.
5	Ausência de ações de capacitação em segurança da informação para os responsáveis pela implementação dos controles e projetos relativos ao tema.

Informações detalhadas sobre os achados de Auditoria não são explicitadas neste Relatório de Auditoria no intuito de não expor possíveis vulnerabilidades relativas à Segurança da Informação e Segurança Cibernética. O Apêndice **II contém a Matriz de Achados completa da presente Auditoria classificada como "reservada**", por conter informações relacionadas à Segurança da Informação e Segurança Cibernética da instituição. A classificação da informação foi feita nos termos do art. 23, inciso VII, c/c o art. 24, § 1º, inciso III, da Lei 12.527/2011 (Lei de Acesso à Informação – LAI), bem como com o Manual de Transparência e Classificação de Informações do Senado Federal, aprovado pelo ATC 06/2017.

A opção por retirar do relatório informações críticas ou sensíveis tem o objetivo de permitir a livre publicação do relatório, mantendo as em caráter "reservado" somente um pequeno conjunto de informações específicas.

8. Manifestação das Unidades Auditadas

O CSI e o Prodasen manifestaram-se conjuntamente por meio do Despacho nº 4034/2022-DGER (assunto: Matriz de Achados Preliminar da Auditoria de Segurança nas Comunicações), em 05/12/22 (NUP 0100.152814/2022-14).

Consideraram, frente às informações apresentadas, a matéria como relevante e complexa e informaram que as situações relatadas serão tratadas no Plano Diretor de Tecnologia da Informação (PDTI) 2023 / 2025, o qual está fase de elaboração.

Também informaram que o Núcleo de Segurança da Informação em Tecnologia da Informação - NSITI, estrutura vinculada ao Prodasen, previsto na Política Corporativa de Segurança da Informação - PCSI - do Ato da Comissão Diretora nº 9, de 2017 foi criado recentemente e ainda está sendo estruturado.

Comprometeram-se, ainda, a apresentar até a data de 31/03/2023 um Plano de Ação endereçando as questões levantadas pela COAUDTI "*relativa aos achados e recomendações de auditoria de nos 1, 2, 3, 4 e 5, contidos na Matriz de Achados Preliminar da Auditoria de Segurança nas Comunicações*".

Depreende-se, portanto, que as áreas citadas acima estão de acordo com os achados e recomendações exaradas no presente Relatório de Auditoria.

O ILB manifestou-se respeito do achado nº 5 por meio do Ofício nº 189/2022–DEXILB/ILB (NUP 00100.158155/2022), indicando, em resumo, que grande parte das capacitações não foram realizadas por motivos alheios à gestão daquele instituto. Informou também que parte das capacitações planejadas foram canceladas pelas

empresas prestadoras de serviço e outros tiveram a tramitação suspensa por outras áreas do Senado. Aponta ainda as dificuldades com a complexidade dos trâmites internos necessários para as contratações de treinamentos externos, as quais requerem manifestação e aprovação de diversos órgãos do Senado Federal.

9. Aspectos Positivos da Gestão

As áreas envolvidas mostraram-se ao longo da realização da presente ação sensibilizadas com a importância do tema e interessadas em colaborar com a equipe da COAUDTI, fornecendo de forma tempestiva todas as explicações e evidências solicitadas.

Constatou-se que há diversas ações relacionadas ao tema Segurança da Informação sendo executadas no âmbito da Secretaria de Tecnologia da Informação (Prodasen), o que demonstra que o tema é considerado de grande importância pelas equipes técnicas da área de tecnologia da informação.

Destacam-se também dois atos formais publicados durante a execução da auditoria:

- Ato do Diretor da Secretaria de Tecnologia da Informação nº 1 de 2022 designou servidor para que assessore tecnicamente o Prodasen no planejamento da implantação do Núcleo de Segurança da Informação em Tecnologia da Informação – NSITI;
- Ato do Presidente nº 22 de 2022 criou o Núcleo de Segurança da Informação em Tecnologia da Informação – NSITI, órgão gestor de segurança da informação previsto na Política Corporativa de Segurança da Informação do Senado desde 2017, mas que até então ainda não havia sido criado na estrutura administrativa de órgãos do Senado.

A criação desse núcleo ajudará sobremaneira a estruturação e sistematização das atividades de Segurança da Informação e Segurança Cibernética.

A equipe técnica do Prodasen externou a dificuldade de promover uma gestão mais proativa e institucional da Segurança da Informação, sobretudo quando os ativos em questão não estão sob a responsabilidade / gestão do Prodasen, como ocorre com os ativos de TI geridos por outras áreas do Senado. Além disso, externaram a carência de mão de obra especializada e em quantidade, bem como a ausência, até novembro de 2022, de estrutura competente (NSITI) para estruturação e sistematização das atividades de Segurança da Informação e Segurança Cibernética.

SENADO FEDERAL
Auditoria

10. Conclusão

A presente auditoria buscou acompanhar os mecanismos, sistemáticas, processos e atividades desempenhados pelo Senado Federal, tendo o CSI e o Prodasen a frente, que têm como objetivo garantir a proteção das informações em suas redes por meio:

- dos recursos de processamento da informação (ativos corporativos e de software) que as suportam; e
- do monitoramento e gestão proativa de vulnerabilidades desses ativos corporativos e de software.

Verificou-se a existência de iniciativas e projetos com essas finalidades, no entanto com limitações na abrangência do inventário de ativos e no nível de correção/remediação de vulnerabilidades, bem como na integração entre as ferramentas empregadas.

Isto posto conclui-se que se faz necessário maior nível de planejamento, coordenação, acompanhamento, monitoramento e avaliação das ações de Segurança da Informação e Segurança Cibernética do Senado Federal por parte do CSI, bem como maior envolvimento do ILB para garantir a realização das ações de capacitação dos servidores quanto ao assunto em questão.

11. Recomendações

A Auditoria de Segurança nas Comunicações, Ação 5.2 do PAInt 2022, frente aos achados de auditoria encontrados, explicitou as seguintes recomendações:

Nº Recomendação / Responsável	Descrição
1 / para o CSI e Prodasen	Analisar a viabilidade de aperfeiçoar e expandir a presente prática (Inventário e controle de ativos corporativos) de forma holística e integrada para os demais ativos da Rede do Senado Federal levando em consideração os controles preconizados pelo Controle 01 do Framework de Controles Críticos do CIS (Center for Internet Security), referendados no Acórdão 1.768/2022 do TCU - Plenário, em especial: • a gestão ativa (registro, acompanhamento / rastreamento e correção) e detalhada de ativos,

SENADO FEDERAL
Auditoria

Nº Recomendação / Responsável	Descrição
	• a manutenção periódica de um inventário detalhado de ativos, • o tratamento de ativos não autorizados e • a descoberta automatizada de ativos
2 / para o CSI e Prodasen	Analisar a viabilidade de aperfeiçoar e expandir a presente prática (Inventário e controle de ativos de software) de forma holística e integrada para os demais ativos da Rede do Senado Federal levando em consideração os controles preconizados pelo Controle 02 do Framework de Controles Críticos do CIS (Center for Internet Security), referendados no Acórdão 1.768/2022 do TCU - Plenário, em especial: • a gestão ativa (registro, acompanhamento / rastreamento e correção) e detalhada de ativos, • o suporte aos ativos autorizados, • o tratamento de ativos não autorizados, • a descoberta automatizada de ativos e • a implementação de listas de permissões de software, bibliotecas e scripts autorizados.

SENADO FEDERAL
Auditoria

Nº Recomendação / Responsável	Descrição
3 / para o CSI e Prodasen	Analisar a viabilidade de aperfeiçoar e expandir a presente prática (Gestão contínua de vulnerabilidades) de forma holística e integrada para os demais ativos da Rede do Senado Federal levando em consideração os controles preconizados pelo Controle 07 do Framework de Controles Críticos do CIS (Center for Internet Security), referendados no Acórdão 1.768/2022 do TCU – Plenário, em especial: • o processo de gestão contínua de vulnerabilidades, • os processos de remediação e correção, • a gestão automatizada de patches de sistemas operacionais e aplicações e • a varredura automatizada de vulnerabilidades em ativos internos e ativos expostos externamente.
4 / para o CSI	Planejar, coordenar, acompanhar, monitorar e avaliar ações de segurança da informação para o Senado Federal, com base nos controles críticos preconizados pelo Center for Internet Security (CIS) e nas boas práticas previstas na norma técnica ABNT NBR ISO/IEC 27.002:2013, conforme competência deste Comitê disposta no Art. 15, do ATC nº 9, de 2017 que Institui a Política Corporativa de Segurança da Informação do Senado Federal - PCSI.
5 / para o Prodasen e ILB	Elaborar projeto conjunto prevendo os principais treinamentos a respeito do tema Segurança da Informação e Segurança Cibernética, monitorar os prazos de solicitação e tramitação, visando garantir a execução das capacitações previstas no Plano Diretor de Tecnologia da Informação (PDTI) e no Plano de Capacitação Anual dos Servidores do Senado (PCASF), conforme competência do ILB, disposta no art. 12 da Política de Capacitação e Desenvolvimento dos Servidores do Senado Federal.

As recomendações acima podem atuar como ponto de partida para que as áreas envolvidas e competentes, em especial o CSI, o Prodasen/NSITI e o ILB, elaborarem

SENADO FEDERAL
Auditoria

um Plano de Ação endereçando as questões levantadas pela COAUDTI "*relativa aos achados e recomendações de auditoria de nos 1, 2, 3, 4 e 5, contidos na Matriz de Achados Preliminar da Auditoria de Segurança nas Comunicações*".

COAUDTI, 30 de janeiro de 2023.

assinado digitalmente
MARCELO SILVA CUNHA
Auditor Líder

assinado digitalmente
HELEN CRISTINA BRAGA COUTINHO
Auditora

em gozo de férias
HELIO MARÇOLA JUNIOR
Auditor

assinado digitalmente
YURI MORAIS BEZERRA
Coordenador da COAUDTI

SENADO FEDERAL
Auditoria

Apêndice I
Auditoria de Segurança nas Comunicações
Informações Complementares

O presente Apêndice apresenta algumas informações complementares, em nível global, relacionados à Segurança da Informação e Segurança Cibernética com o intuito de promover reflexões.

I.1. Custos relacionados a prevenção e recuperação de incidentes cibernéticos

O whitepaper "The Costs of Cyber Security in Prevention Vs Recovery"[1] apresenta de forma sintética os principais fatores de custos de prevenção e recuperação relacionados a ataques hackers. A lista a seguir enumera alguns custos relacionados a recuperação de incidentes cibernéticos:

- perda financeira direta;
- disrupção da continuidade de negócios;
- perda do valor da marca / reputação / imagem;
- perda de consumidores / clientes;
- remediação para as partes afetadas; e
- custos legais.

O Gartner estima para 2023 um crescimento dos gastos com serviços e produtos de Segurança da Informação e Gestão de Riscos da ordem de 11,3% alcançando a cifra de US$ 188 bilhões conforme tabela[2] a seguir:

[1] https://www.nicitpartner.com/costs-cyber-security-prevention-vs-recovery/
[2] https://futurecio.tech/three-factors-influencing-security-budgets-in-2023/

Table 1

Worldwide Information Security & Risk Management End-User Spending by Segment, 2021-2023 (Millions of U.S. Dollars)

Market Segment	2021 Spending	2021 Growth (%)	2022 Spending	2022 Growth (%)	2023 Spending	2023 Growth (%)
Application Security	4,963	20.8	6,018	21.3	7,503	24.7
Cloud Security	4,323	36.3	5,276	22.0	6,688	26.8
Data Privacy	1,140	14.2	1,264	10.8	1,477	16.9
Data Security	3,193	6.0	3,500	9.6	3,997	14.2
Identity Access Management	15,865	22.3	18,019	13.6	20,746	15.1
Infrastructure Protection	24,109	22.5	27,408	13.7	31,810	16.1
Integrated Risk Management	5,647	15.4	6,221	10.1	7,034	13.1
Network Security Equipment	17,558	12.3	19,076	8.6	20,936	9.7
Other Information Security Software	1,767	26.2	2,032	15.0	2,305	13.4
Security Services	71,081	9.2	71,684	0.8	76,468	6.7
Consumer Security Software	8,103	13.7	8,659	6.9	9,374	8.3
TOTAL	**157,749.7**	**14.3**	**169,156.2**	**7.2**	**188,336.2**	**11.3**

Source: Gartner (October 2022)

I.2. Impactos de incidentes cibernéticos

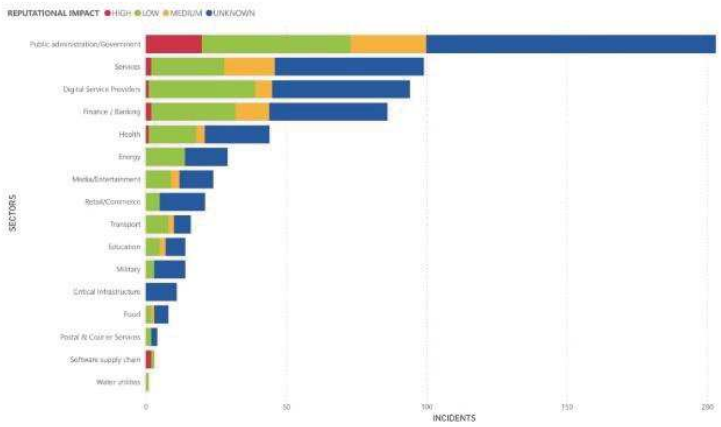
Os gráficos a seguir, extraídos do relatório "ENISA Threat Lands 2022"[3], trazem informações do estudo europeu a respeito dos impactos reputacional, social, digital, econômico e físico de incidentes cibernéticos classificados por setores. Nota-se que o setor/segmento **Administração Pública / Governo** é dos mais impactados em quatro domínios com especial destaque para os impactos reputacional, social, digital e econômico que são bastante relevantes em se tratando de instituições governamentais.

[3] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

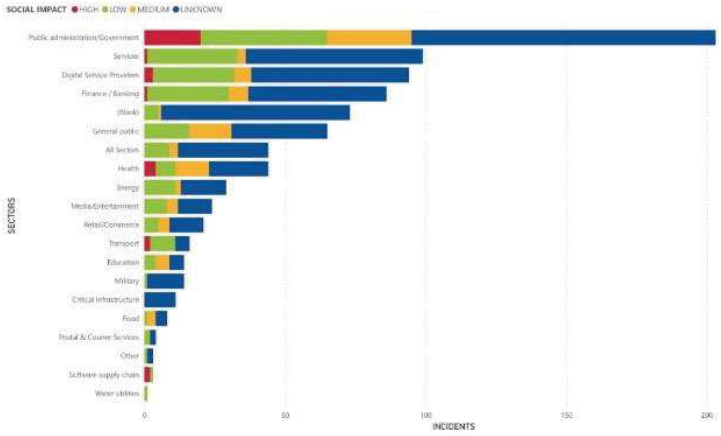
Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

SENADO FEDERAL
Auditoria

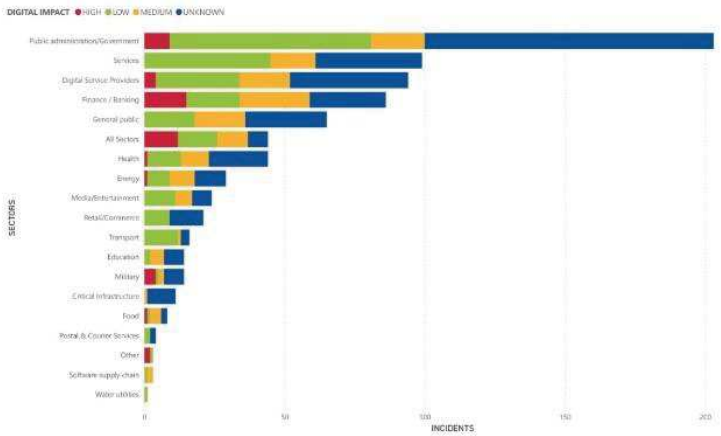
Reputational impact by sector



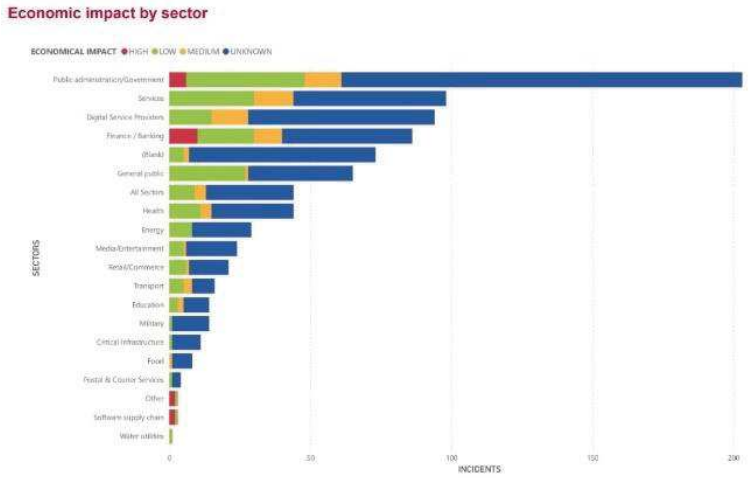
Social Impact by sector

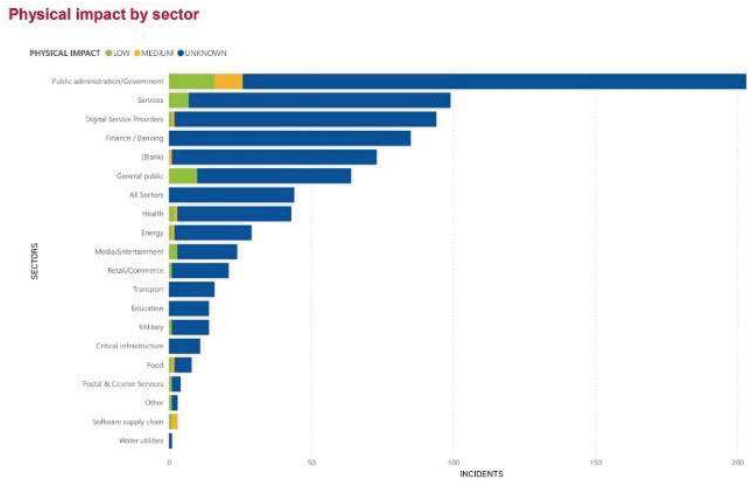


Digital impact by sector



Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611





I.3. Tipos mais comuns de ataques cibernéticos e prevalência ransomware

São considerados a título de classificação alguns ataques / ameaças / incidentes / falhas de Segurança da Informação e Segurança Cibernética mais comuns[4][5]:

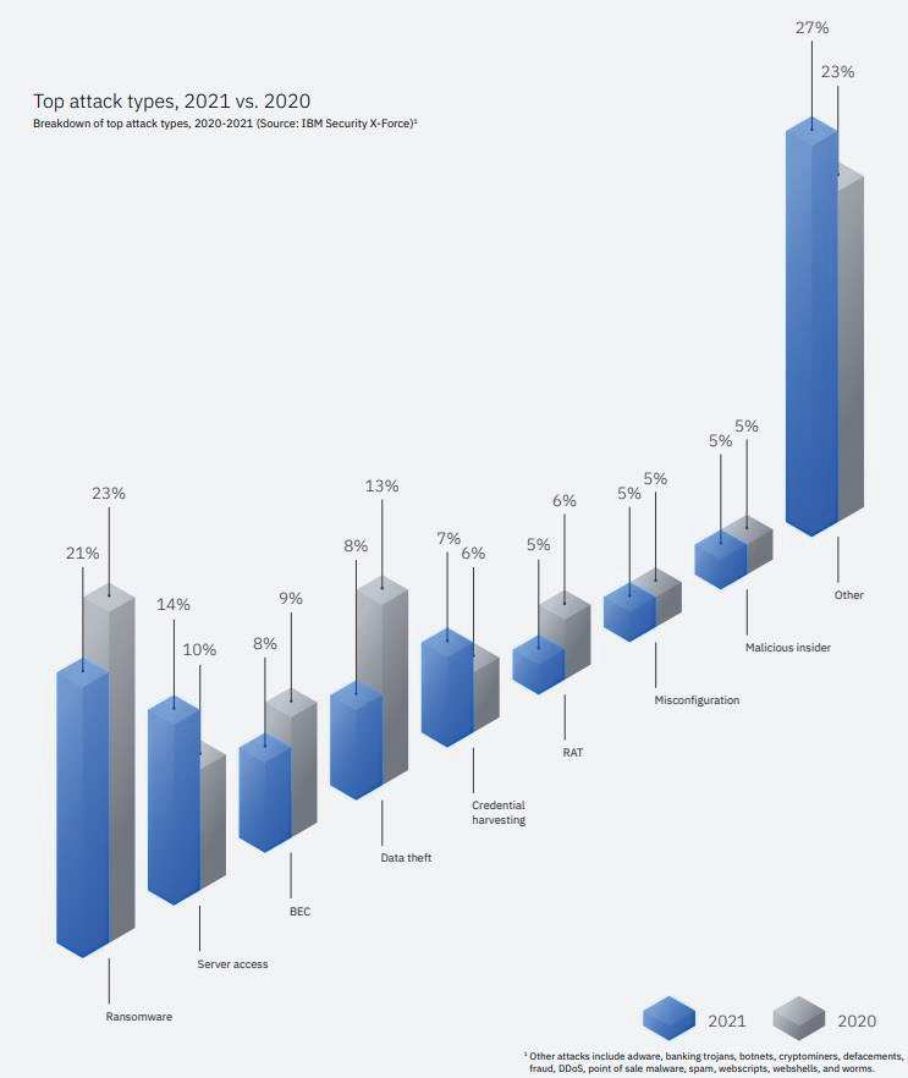
Tipo	Tipo
• Malware;	• Ransomware;
• Phishing;	• SQL injection;
• MITM - Man-in-the-Middle;	• Zero-day Exploit; e
• DDoS - Distributed denial of service;	• DNS Attack.

[4] https://www.nicitpartner.com/costs-cyber-security-prevention-vs-recovery/
[5] https://www.stealthlabs.com/blog/cyber-security-threats-all-you-need-to-know/

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

SENADO FEDERAL
Auditoria

A Figura a seguir apresenta os tipos de ataques mais frequentes em 2020 e 2021 conforme apresentado no relatório "X-Force Threat Intelligence Index 2022"[6] editado pela IBM Security.



Cabe destacar no gráfico acima a incomoda liderança de ataques do tipo **Ransomware** nos anos de 2020 (23% do total) e 2021 (21% do total) perdendo apenas para o tipo "Other" que na verdade é um agrupamento de subtipos de ataques. Cabe lembrar que foram ataques de **Ransomware** que sofreram o STJ em 2020 e o Banco BRB em 2022 que além de indisponibilizarem os sistemas e processos

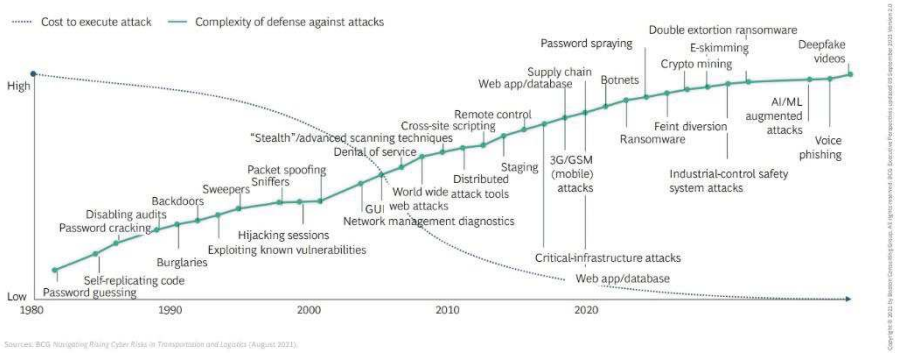
[6] https://www.ibm.com/downloads/cas/ADLMYLAZ

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

eletrônicos por semanas também repercutiram fortemente na mídia nacional e internacional.

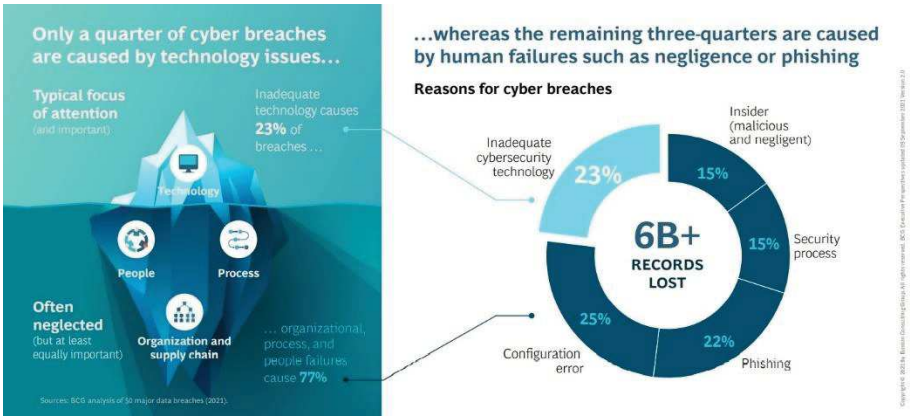
I.4. Barateamento dos ataques X aumento da complexidade de defesa

A apresentação do Boston Consulting Group - BCG - intitulada "**The CEO's Guide to Cybersecurity**"[7] nos apresenta ainda mais dois pontos que chamam muito a atenção. No primeiro gráfico a seguir é apresentada na linha do tempo a relação inversa entre o custo de execução de ataques e a complexidade de defesa contra esses ataques, realidade que beneficia sobremaneira os atacantes.



I.5. Apenas 1/4 das brechas cibernéticas decorrem de questões tecnológicas

Neste segundo gráfico o BCG explicita que praticamente 1/4 (23%) das brechas de Segurança Cibernética decorrem de questões tecnológicas. Portanto 77% decorrem de questões relacionadas ao comportamento humano (insider malicioso ou negligente, processo de segurança inexistente ou ineficiente, phishing e erro de configuração decorrente de falta de competência).

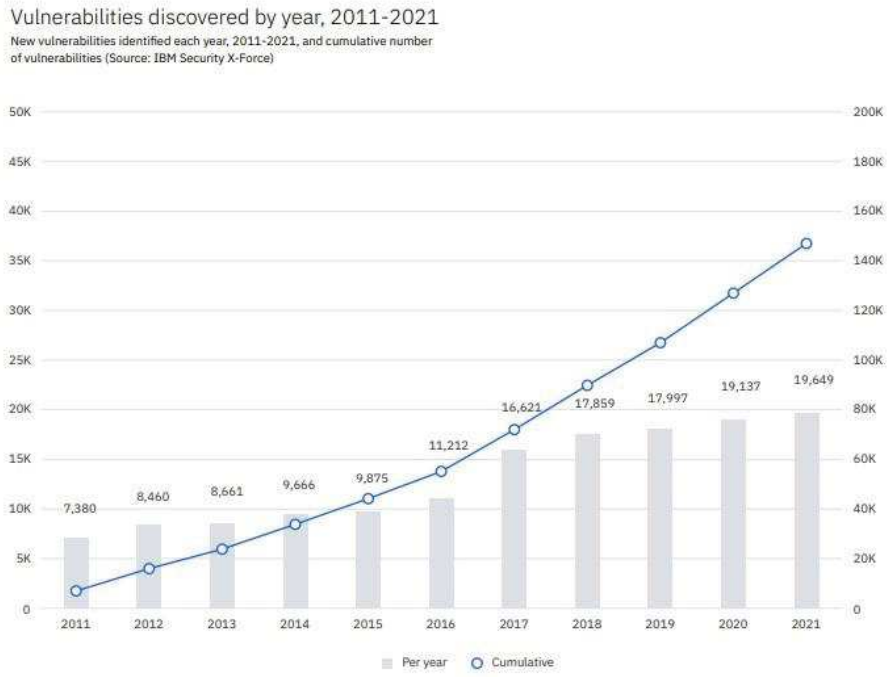


[7] https://media-publications.bcg.com/BCG-Executive-Perspectives-CEO-Guide-to-Cybersecurity.pdf

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

I.6. Da Escalada das Vulnerabilidades

Com relação à identificação de vulnerabilidades chama atenção o crescente número anual de novas identificações, bem como a assustadora curva cumulativa, destacados na figura no período de 2011 a 2021, a seguir, extraída do relatório "X-Force Threat Intelligence Index 2022"[8] editado pela IBM Security. Este cenário é bastante preocupante pois possibilita um arranjo sempre crescente de opções para os atores de ameaças cibernéticas em busca de explorar eficientemente as vulnerabilidades presentes no seu alvo.



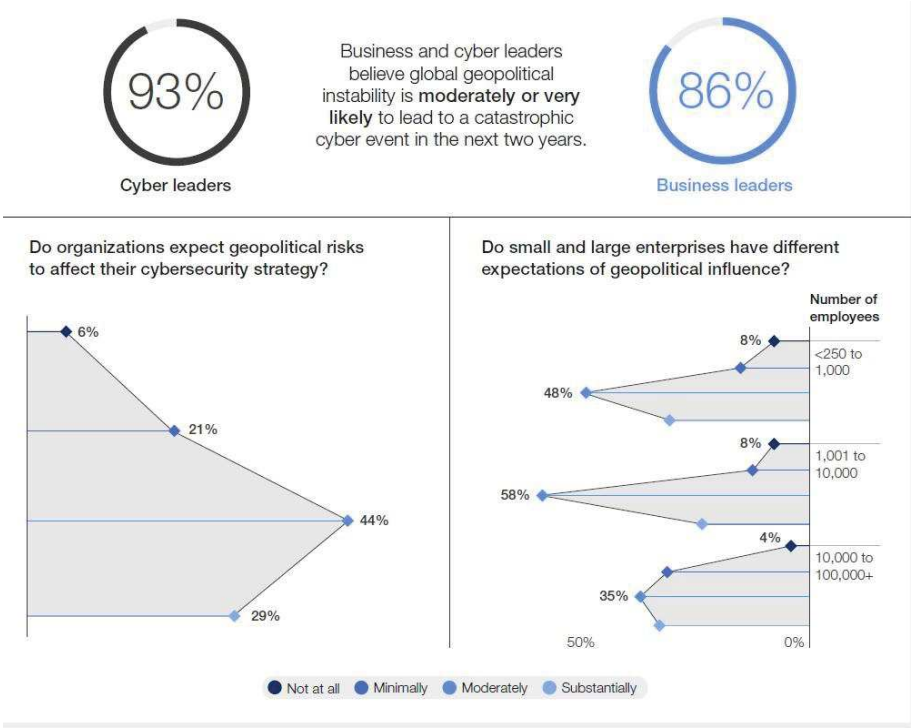
I.7. Tendências em Segurança da Informação e Segurança Cibernética

A questão da Segurança Cibernética é tão complexa e crítica tornando as sociedades e economias de países mais vulneráveis que o World Economic Forum - WEF - edita anualmente a pesquisa Global Cybersecurity Outlook. O WEF publica guias e relatórios sobre Segurança Cibernética desde 2018 e este relatório está em sua 17ª edição.

[8] https://www.ibm.com/downloads/cas/ADLMYLAZ

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

Nesta edição de 2023 da pesquisa Global Cybersecurity Outlook 2023[9] o WEF detectou, frente a instabilidade geopolítica mundial, que mais de 93% das lideranças de segurança cibernética e 86% das lideranças organizacionais acreditam que pode haver no mundo um evento cibernético de grandes proporções nos próximos dois anos:



A ENISA - European Union Agency for Cybersecurity monitora e publica anualmente pesquisa com o panorama das ameaças cibernéticas, que está em sua décima edição. Na edição do relatório ENISA Threat Landscape 2022 (horizonte de tempo de julho 2021 a junho de 2022) foram observadas as seguintes tendências[10] que merecem ser destacadas:

- exploração de Zero-day é o novo recurso empregado pelos atores de ameaças inteligentes para alcançarem seus objetivos;
- uma nova onda de hacktivismo foi observada desde a Guerra da Ucrânia;
- ataques DDoS então se tornando maiores e mais complexos movendo-se na direção de redes móveis e Internet da Coisas (IoT), que estão agora sendo usados em Guerra Cibernética; e

[9] https://www.weforum.org/reports/global-cybersecurity-outlook-2023/
[10] https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611

- desinformação e deepfakes habilitadas por IA. A proliferação de bots de modelagem de personas pode facilmente prejudicar o processo de regras "notice-and-comment", bem como a interação da comunidade, enchendo as agências governamentais com conteúdo e comentários falsos.

A revista **Cybercrime Magazine**, por sua vez, publicou em 10/12/2022 a matéria "***Top 10 Cybersecurity Predictions And Statistics For 2023 - Dez Principais Previsões e Estatísticas de Cibersegurança para 2023***"[11] (em tradução livre), sumarizando as predições para a indústria de Segurança Cibernética até 2025:

1. o dano global do crime cibernético deve alcançar até 2025 a cifra anual de US$10.5 trilhões;
2. os gastos globais com cibersegurança irão exceder cumulativamente de 2021-2025 a cifra de $1.75 Trilhões;
3. o mundo terá 3,5 milhões de postos de trabalho em cibersegurança não preenchidos em 2023;
4. os custos do dano global de ataques do tipo ransomware são previstos excederem a cifra de US$265 bilhões até 2031;
5. o mundo necessitará proteger ciberneticamente 200 zettabytes de dados até 2025;
6. o mercado de seguro cibernético deve alcançar a cifra de US$14.8 bilhões até 2025;
7. o criptocrime deve custar ao mundo a cifra de US$30 bilhões anualmente até 2025;
8. mulheres devem ocupar 30% das posições de cibersegurança globais até 2025;
9. noventa porcento da população humana com idade superior a 6 anos de idade estará online até 2030; e
10. o mundo deverá necessitará segurar 338 bilhões de novas linhas de código de software até 2025.

[11] https://cybersecurityventures.com/top-5-cybersecurity-facts-figures-predictions-and-statistics-for-2021-to-2025/#:~:text=Cybersecurity%20Ventures%20%40CybersecuritySF%20estimates%20that,%2410.5%20trillion%20annually%20by%202025

Senado Federal | Auditoria | Bloco 16 | Térreo | CEP 70165-900 | Brasília DF
Telefone: +55 (61) 3303-1611