RESULTADOS DA PESQUISA DE SEGURANÇA E PRIVACIDADE DO SISTEMA RNP

2021

RNP
ORGANIZAÇÃO SOCIAL DO MCTI

RESUMO EXECUTIVO_

Em 2021, pelo segundo ano consecutivo, tivemos a Covid-19 como pano de fundo. A pandemia deu um impulso e acelerou a adoção em massa de tecnologias digitais, trazendo mudanças sem precedentes no âmbito socioeconômico, no mundo todo. A digitalização das organizações avançou vertiginosamente. Isso se reflete na desmaterialização massiva dos sistemas de informação para a nuvem, na explosão da Internet das Coisas e no acúmulo de dados dos usuários em Big Data. As medidas de distanciamento social na maioria dos países do mundo forçaram grande parte do comércio mundial, em termos de bens e serviços, a se tornar *on-line*. Trabalho remoto e aprendizado *on-line* fazem hoje parte do "novo normal". Aliada a essa transformação digital, cresceu também a preocupação com ameaças e vulnerabilidades cibernéticas. A segurança das informações e a proteção dos dados tornaram-se críticas nas organizações, com isto, encontrar recursos humanos qualificados em segurança cibernética virou um verdadeiro desafio.

A RNP não é alheia a este novo cenário. Nesse sentido, segurança e privacidade continuam a ser temas prioritários, presentes nos seus processos e nas suas entregas de valor.

O objetivo da Pesquisa de Segurança e Privacidade do Sistema RNP – 2021 foi, precisamente, mapear a situação de segurança da informação e privacidade das instituições que compunham o Sistema RNP neste último ano, visando identificar os seus maiores *gaps* e principais desafios, subsidiando a RNP na definição de estratégias de apoio e planos de ação junto à comunidade de ensino, pesquisa e inovação. Este relatório compila e consolida os dados de 2021 das organizações do Sistema RNP.

A execução da pesquisa não teria sido possível sem a valiosa participação e contribuição das instituições que fazem parte do ecossistema de ensino, pesquisa, saúde e inovação, a quem a RNP novamente agradece.

A PESQUISA DE SEGURANÇA E PRIVACIDADE DO SISTEMA RNP GERA SUBSÍDIOS RELEVANTES PARA A DEFINIÇÃO DE ESTRATÉGIAS E A CONSTRUÇÃO DE PLANOS DE AÇÃO DE CIBERSEGURANÇA E PRIVACIDADE.

A RNP_

Somos a Rede Nacional de Ensino e Pesquisa. Disponibilizamos internet segura e de alta capacidade, serviços personalizados e promovemos projetos de inovação. Nascemos em 1989 e fomos pioneiros no uso da internet no Brasil.

Somos qualificados como uma organização social vinculada ao Ministério da Ciência, Tecnologia e Inovações (MCTI) e mantida por esse, em conjunto com os ministérios da Educação (MEC), das Comunicações (MCom), do Turismo (Mtur), da Saúde (MS) e da Defesa (MD), que participam do Programa Interministerial RNP (PRO-RNP).

SISTEMA RNP_

É uma rede que beneficia 4 milhões de alunos, professores e pesquisadores brasileiros. O Sistema RNP inclui universidades, institutos educacionais e culturais, agências de pesquisa, hospitais de ensino, parques e polos tecnológicos.

PESI_

Projetos Especiais em Segurança da Informação (PESI) é uma das três áreas sob coordenação da Diretoria Adjunta de Cibersegurança (DACS) da RNP. Em atuação desde 2020, PESI tem por missão promover ações estruturantes que fortaleçam o ecossistema em segurança e privacidade do Sistema RNP e do país, por meio de cooperações e relacionamentos institucionais estratégicos.

SUMÁRIO_

SOBRE A PESQUISA_

PÚBLICO-ALVO

256
INSTITUIÇÕES CONVIDADAS

152
QUESTIONÁRIOS ABERTOS

60
INSTITUIÇÕES RESPONDENTES

Diferentemente do ano 2020, quando apenas as instituições federais de ensino superior (IFES) e os institutos federais (IFs) foram convidados a participar da Pesquisa de Segurança e Privacidade, em 2021 optou-se por se fazer um mapeamento mais abrangente, considerando o Sistema RNP como um todo. Das 256 instituições convidadas que receberam o questionário, 59,4% (152) delas acessaram o questionário e 23,4% (60) responderam à pesquisa em plenitude. Para divulgação da pesquisa, contamos com o apoio da Associação Nacional dos Dirigentes das Instituições Federais de Ensino Superior (Andifes), do Conselho Nacional das Instituições da Rede Federal de Educação Profissional, Científica e Tecnológica (Conif) e da Rede Universitária de Telemedicina (RUTE).

O questionário foi endereçado aos gestores de TIC das respectivas instituições com o intuito de se ter um único ponto focal, entendendo-se, no entanto, que em muitos casos a pesquisa tenha sido preenchida internamente a várias mãos. Obteve-se apenas uma (1) resposta por instituição.

A RNP garante a confidencialidade dos dados, não sendo autorizado seu acesso e uso a terceiros.

Todas as informações fornecidas foram usadas pela RNP para os propósitos indicados.

QUESTIONÁRIO

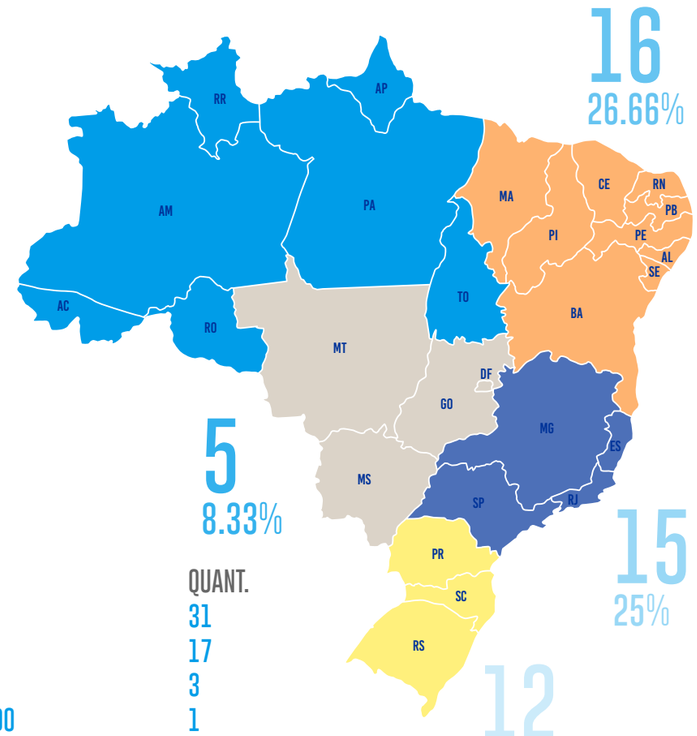
52
PERGUNTAS EM 04 SEÇÕES:

01 IDENTIFICAÇÃO DA ORGANIZAÇÃO [1]
02 SEGURANÇA DA INFORMAÇÃO [14]
03 PRIVACIDADE E TRANSPARÊNCIA [27]
04 DESENVOLVIMENTO DE COMPETÊNCIAS [10]

TEMPO ESTIMADO DE RESPOSTA **21** MINUTOS

RESPONDENTES

- NORTE
- CENTRO-OESTE
- NORDESTE
- SUDESTE
- SUL



TIPO DE ORGANIZAÇÃO	QUANT.
UNIVERSIDADES FEDERAIS	31
INSTITUTOS FEDERAIS	17
UNIVERSIDADES ESTADUAIS	3
INSTITUTOS DE ENSINO SUPERIOR PRIVADO	1
INSTITUTOS DE PESQUISA	6
ESTABELECIMENTOS DE SAÚDE COM ENSINO E PESQUISA	2

SEGURANÇA DA INFORMAÇÃO_

A cibersegurança tem a sua importância crescendo em todos os setores sociais, públicos e privados, de todos os países e inclusive no âmbito pessoal dos habitantes de quase todos eles.

Obviamente isso acontece devido à dependência crítica de nossas sociedades aos sistemas e redes de comunicação, que perante uma interrupção ou simples degradação do serviço que oferecem, colocariam setores essenciais desses países em situação calamitosa.

Um exemplo disso pode ser extraído do Global Risks Report, anualmente publicado pelo World Economic Forum (WEF), que ano após ano situa os ataques cibernéticos como um dos riscos mais relevantes. Assim, na 17ª edição desse relatório publicada em janeiro de 2022, que toma como referência o último ano de 2021, de um total de 37 riscos estudados, as "falhas de cibersegurança" aparecem como o 7º maior risco que mais piorou desde o início da crise Covid-19. A rápida digitalização em economias avançadas durante a pandemia levou a novas vulnerabilidades cibernéticas.

Por outro lado, o Global Cybersecurity Index, bienalmente publicado pela União Internacional das Telecomunicações (UIT), em sua edição de 2020, classificou os países de acordo com o seu nível de comprometimento com o tema cibersegurança. O Brasil demonstra vir aumentando seu nível de comprometimento no tema ao pular da posição 71 (2018) para a posição 18 (2020), dentre 194 países. No entanto, tendo em vista alguns levantamentos da situação de segurança no país nos vários setores – é o caso da Pesquisa de Segurança e Privacidade do Sistema RNP (2020), que teve como foco o ecossistema de ensino, pesquisa e inovação – constata-se que há ainda um grande *gap* neste setor e há a necessidade de continuar se investindo no tema e no estabelecimento de programas de governança em segurança da informação.

GLOBAL RISKS REPORT 2021

GLOBAL CYBERSECURITY INDEX 2020

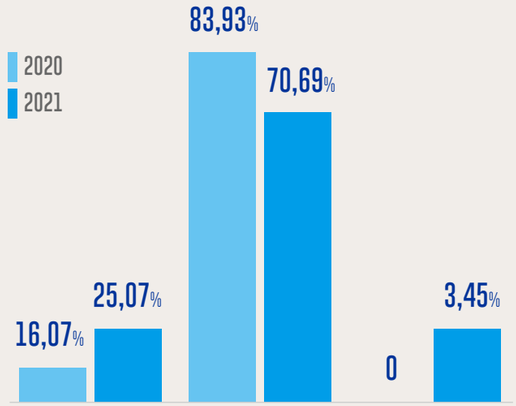
"O BRASIL DEMONSTRA VIR AUMENTANDO SEU NÍVEL DE COMPROMETIMENTO COM O TEMA CIBERSEGURANÇA AO PULAR DA POSIÇÃO 71 (2018) PARA A POSIÇÃO 18 (2020)" (GCI, 2020).

É fundamental que a organização conduza e priorize suas ações de segurança de forma coordenada e estruturada, alinhadas a um programa de segurança da informação. O planejamento é um processo inevitável da gestão de segurança, pois garante a execução de ações específicas para cada organização a partir de uma visão de riscos cibernéticos, que subsidia a construção de estratégias de mitigação, monitoramento de segurança, resposta e recuperação. Além disso, conduz a integração da segurança da informação em todos os processos de negócio. As ações compreendidas neste planejamento só poderão ser executadas se respaldadas por uma reserva orçamentária – infelizmente, muitas organizações têm dificuldades relacionadas com o orçamento de segurança, sendo levadas à execução de necessidades urgentes e pontuais de curto prazo.

No Sistema RNP ainda é bastante menor a porcentagem de instituições que possuem um planejamento formal anual em segurança (25,86%), a maioria (70,69%) não conta com ele. No entanto, comparando com os resultados obtidos no ano de 2020, em 2021 evidencia-se uma porcentagem maior de instituições sensibilizadas com a necessidade deste importante processo – passou de 16,07% para 25,86%, aumento de quase 10%. No que diz respeito à destinação orçamentária para assuntos de segurança da informação, a maioria (79,31%) não possui orçamento específico com este propósito.

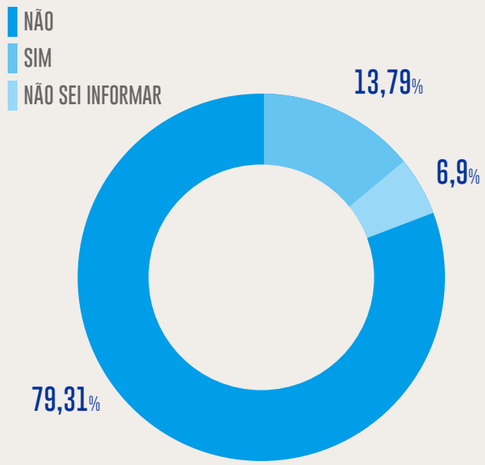
QUESTÃO

Sua organização possui um planejamento formal anual em segurança?



QUESTÃO

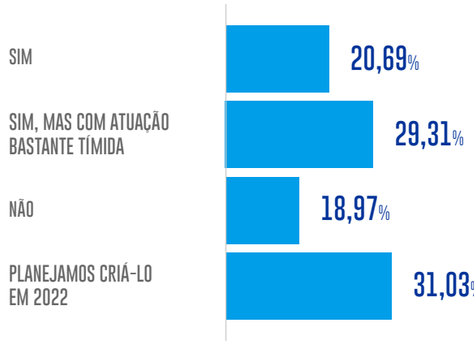
A sua organização possui destinação orçamentária interna para assuntos de segurança da informação?



É primordial que a organização conte com uma equipe que atue de forma dedicada nas ações necessárias de segurança da informação. Além de um gestor e sua equipe, a natureza holística da cibersegurança pode ser melhor tratada com um comitê multidisciplinar que atue como uma instância assessora da alta direção no tema e que tenha por missão avaliar, direcionar e monitorar a segurança da informação. Metade das instituições afirmaram ter um Comitê de Segurança da Informação, 29,31% com atuação bastante tímida; e 31,03% das instituições pretendem criar esta instância de governança em 2022.

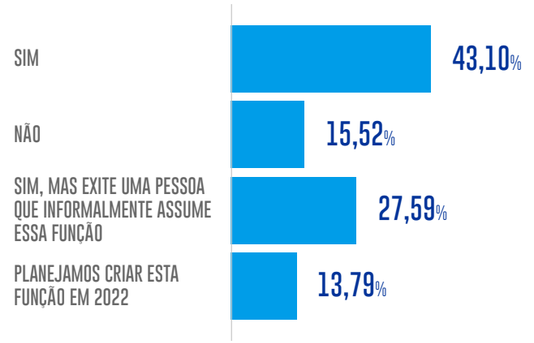
QUESTÃO

Foi formalmente instituído pela Alta Gestão um Comitê (específico e multidisciplinar) de Segurança da Informação?



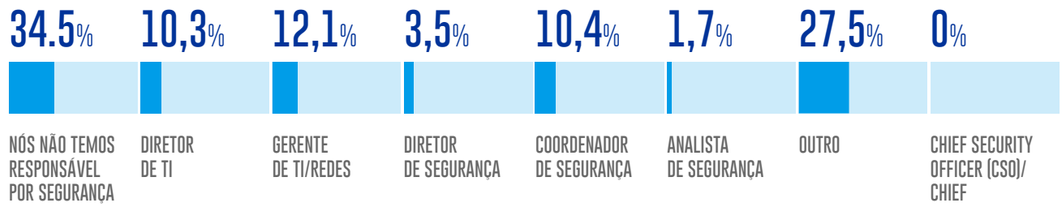
QUESTÃO

Existe a figura de um Gestor de Segurança da Informação indicado formalmente pela Alta Gestão para lidar com aspectos relacionados à segurança da informação?



QUESTÃO

Caso exista esta figura, qual o cargo que ele/ela ocupa?



A Segurança da Informação é constituída, basicamente, por um conjunto de controles físicos, organizacionais, tecnológicos e de pessoas, visando garantir a confidencialidade, integridade e disponibilidade.

A Política de Segurança da Informação é a que dá o direcionamento estratégico à organização, enquanto as normas estabelecem as regras no nível tático. Já os padrões e procedimentos facilitam o cotidiano das organizações no cumprimento da política e normas. É sumamente importante que a organização construa este arcabouço normativo, a partir da Política de Segurança da Informação (PSI/POSIC).

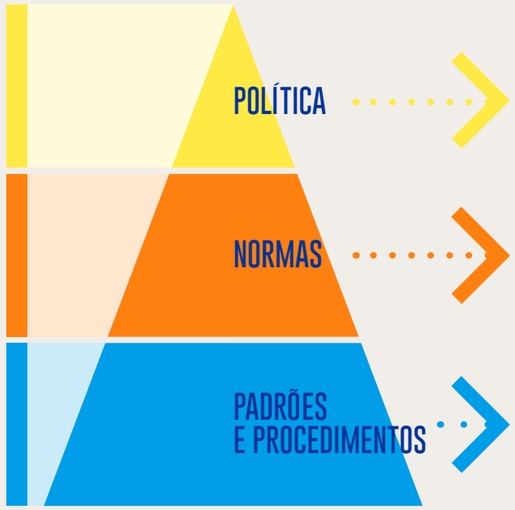
A maior parte das instituições indicou possuir uma Política de Segurança da Informação, porém em diferentes estágios:

32,76%
DEVIDAMENTE APROVADA E DIVULGADA

20,69%
EM PROCESSO DE DIVULGAÇÃO

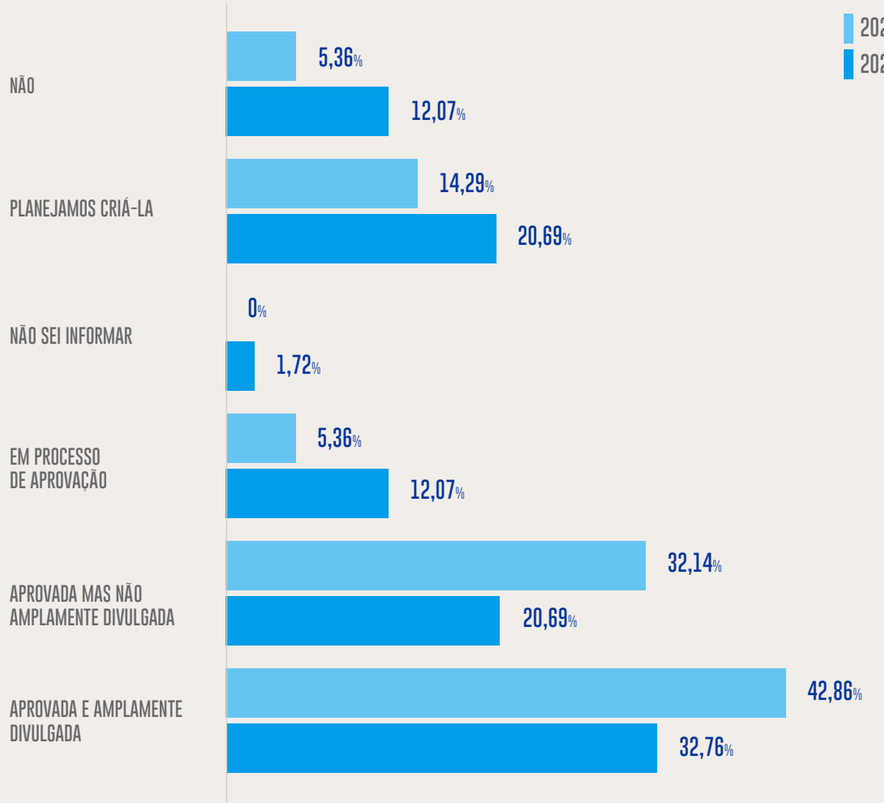
12,07%
AGUARDANDO APROVAÇÃO

SEGURANÇA DA INFORMAÇÃO_



QUESTÃO

Sua organização possui uma Política de Segurança da Informação (PSI/POSIC) devidamente aprovada pela alta gestão e divulgada a todos os colaboradores, além de parceiros e fornecedores?



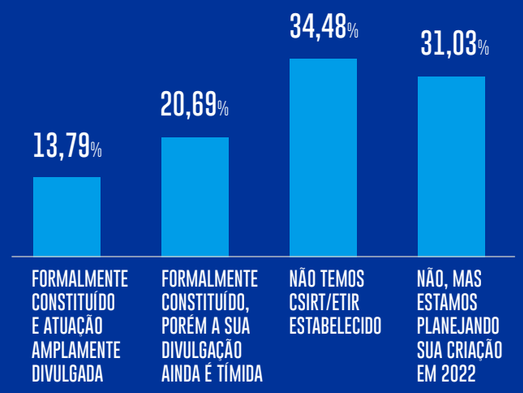
Aproximadamente 65% das instituições indicaram não possuir um CSIRT/ETIR. Dentre as instituições que contam com esta equipe, apenas 13,79% foram formalmente estabelecidos, e 20,69% do total tem ainda uma atuação muito tímida. É fundamental que toda organização divulgue de forma ampla, interna e externamente, o seu CSIRT/ETIR para que este possa ser acionado com agilidade quando necessário.

UM CSIRT OU ETIR É UMA EQUIPE QUE ATUA DE FORMA DEDICADA E OFERECE SERVIÇOS A UMA COMUNIDADE ESPECÍFICA, A FIM DE PREVENIR, GERIR, TRATAR E RESPONDER INCIDENTES DE SEGURANÇA DA INFORMAÇÃO, BEM COMO PROMOVER A CULTURA DE SEGURANÇA JUNTO AOS SEUS USUÁRIOS.

Na maioria dos casos, as equipes ativas contam com 4 ou mais membros, porém operam em formato misto, isto é, com alguns membros com dedicação parcial.

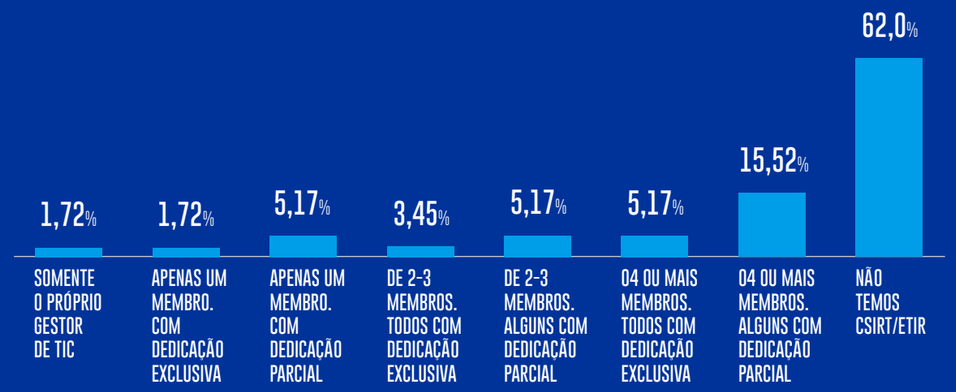
QUESTÃO

Sua organização possui um grupo de resposta a incidentes de segurança (CSIRT) ou equipe de prevenção, tratamento e resposta a incidentes (ETIR) formalmente constituído e divulgado na comunidade de usuários?



QUESTÃO

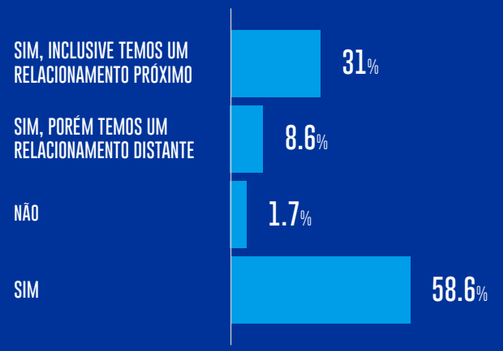
Se a resposta for positiva para a pergunta anterior, quantos membros compõem o CSIRT/ETIR?



O CAIS/RNP é um dos primeiros grupos de segurança de redes do Brasil, e vem apoiando as organizações de ensino, pesquisa e inovação. Quase 90% das organizações afirmaram conhecer o CAIS/RNP, sendo que 31% delas têm inclusive uma relação muito próxima.

QUESTÃO

Você conhece o que é o CAIS (Centro de Atendimento a Incidentes de Segurança)?



A RNP APOIA 15 EQUIPES DE RESPOSTA A INCIDENTES QUE ATUAM EM INSTITUIÇÕES ACADÊMICAS NO BRASIL.

SIGLA	NOME
CSIRT UFAM	EQUIPE DE RESPOSTA A INCIDENTES DE SEGURANÇA DA UNIVERSIDADE FEDERAL DO AMAZONAS
CEO/REDE RIO	COORDENAÇÃO DE ENGENHARIA OPERACIONAL DA REDE RIO
CERT-BAHIA	GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA BAHIA
CERT-RS	CENTRO DE EMERGÊNCIA EM SEGURANÇA DA REDE TCHÊ
CSIRT POP-SE	GRUPO DE RESPOSTA A INCIDENTES DE SEGURANÇA DO POP-SE
CSIRT UFAM	EQUIPE DE RESPOSTA A INCIDENTES DE SEGURANÇA DA UNIVERSIDADE FEDERAL DO AMAZONAS
CSIRT UNICAMP	GRUPO DE RESPOSTA A INCIDENTES DA UNIVERSIDADE ESTADUAL DE CAMPINAS
ETIR IFMG	EQUIPE DE TRATAMENTO DE INCIDENTES DE REDES DA IFMG
ETIR UFBA	EQUIPE DE TRATAMENTO A INCIDENTES DE REDES DE COMPUTADORES DA UFBA
GRC/UNESP	EQUIPE DE TRATAMENTO A INCIDENTES DE REDES DE COMPUTADORES DA UFBA
GSETI USP	GRUPO DE SEGURANÇA EM TI
GSR/INPE	GRUPO DE SEGURANÇA DE SISTEMAS E REDES DO INSTITUTO NACIONAL DE PESQUISAS ESPACIAIS
NARIS	NÚCLEO DE ATENDIMENTO E RESPOSTA A INCIDENTES DE SEGURANÇA
SEGTIC UFRJ	SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DA UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
TRI	TIME DE RESPOSTA A INCIDENTES DE SEGURANÇA DA UNIVERSIDADE FEDERAL DO RIO GRANDE DO SUL
TRIIF	TIME DE RESPOSTA A INCIDENTES DO INSTITUTO FEDERAL FARROUPILHA

Na jornada de estruturação do sistema de gestão de segurança da informação, além do arcabouço normativo, é fundamental que também sejam implementados alguns processos de segurança da informação. A tabela ao lado apresenta uma fotografia de como se encontram as instituições de ensino, pesquisa e inovação neste quesito.

Alguns processos mostraram-se prioritários para as organizações, são eles:

Apenas 5% das instituições respondentes têm seu processo de Gestão de Riscos devidamente implantado.

Nos processos de Gestão de Vulnerabilidades, Desenvolvimento Seguro e Gestão de Continuidade de Negócios caminhou-se pouco ou nada rumo à sua implantação.

20,69%
CONSCIENTIZAÇÃO E TREINAMENTO

20,69%
CLASSIFICAÇÃO DA INFORMAÇÃO

17,24%
GESTÃO DE INCIDENTES

QUESTÃO

Processos de Segurança da Informação (SI).

QUESTÕES	SIM	NÃO	NÃO SEI INFORMAR	EM DESENVOLVIMENTO	PLANEJAMOS TER PARA 2022
A sua organização possui um processo implantado de gestão de riscos de segurança?	5,17	44,83	1,72	34,48	13,79
Sua organização oferece periodicamente programas de conscientização e treinamento em SI aos usuários finais?	20,69	43,1	3,45	15,52	17,24
Sua organização segue um(a) processo/norma de classificação da informações?	20,69	31,03	25,86	17,24	5,17
Sua organização possui um processo implantado de desenvolvimento seguro de software?	15,52	51,72	5,17	22,41	5,17
A sua organização possui um processo implantado de gestão de incidentes de segurança?	17,24	43,1	1,72	17,24	20,69
A sua organização possui um processo implantado de gestão de vulnerabilidades?	12,07	55,17	1,72	18,97	12,07
A sua organização possui planos de continuidade operacional para atividades críticas?	12,07	50,00	3,45	22,41	12,07

A dificuldade maior apontada pela comunidade na implantação dos processos ausentes reside tipicamente na carência de recursos humanos qualificados. A RNP continua no seu propósito de apoiar as instituições no desenvolvimento de competências a fim de minimizar estes *gaps*.

Ainda quando 20,69% das instituições têm um processo de conscientização e treinamento implantado, parece não serem expressivos os frutos destes esforços – a maior parte das organizações apontou ter uma maturidade relativamente baixa (4/10) para a questão da cultura de segurança corporativa.

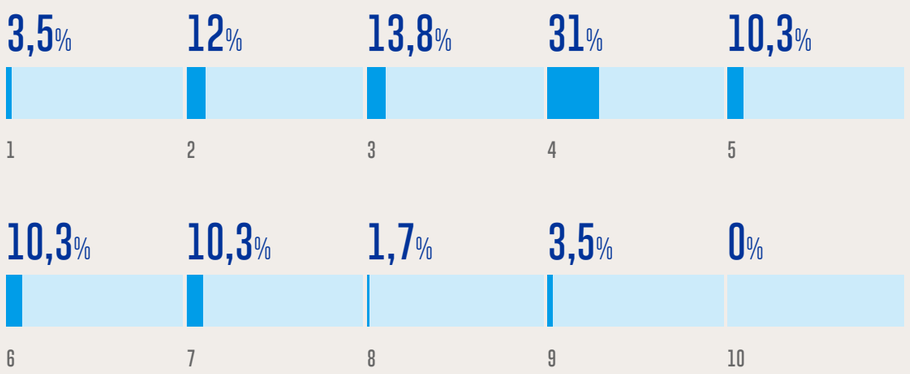
QUESTÃO

Se alguma das suas respostas na tabela anterior foi diferente de SIM, indique quais as principais dificuldades enfrentadas para não ter implantado cada um desses processos.

QUESTÕES	FALTA DE CONHECIMENTO TÉCNICO	FALTA DE RECURSOS FINANCEIROS	FALTA DE RECURSOS HUMANOS	NÃO É PRIORIDADE PARA A ORGANIZAÇÃO	NÃO SEI INFORMAR / NÃO SE APLICA
Processo de gestão de riscos de segurança	5,88	1,96	74,51	7,84	9,8
Programas de conscientização e treinamento em SI aos usuários finais	2,22	2,22	64,44	17,78	13,33
Processo/norma/plano/política de classificação da informação	15,22	0,00	54,35	8,7	21,74
Processo de desenvolvimento seguro	29,17	0,00	43,75	4,17	22,92
Processo de gestão de incidentes de segurança	17,39	4,35	60,87	8,7	8,7
Processo de gestão de vulnerabilidades	16,33	4,08	67,35	4,08	8,16
Planos de continuidade operacional para atividades críticas	18,00	12,00	52,00	6,00	12,00

QUESTÃO

Em uma escala de 1 a 10 (sendo 10 a maior), como você avalia a maturidade da cultura de segurança em sua organização?

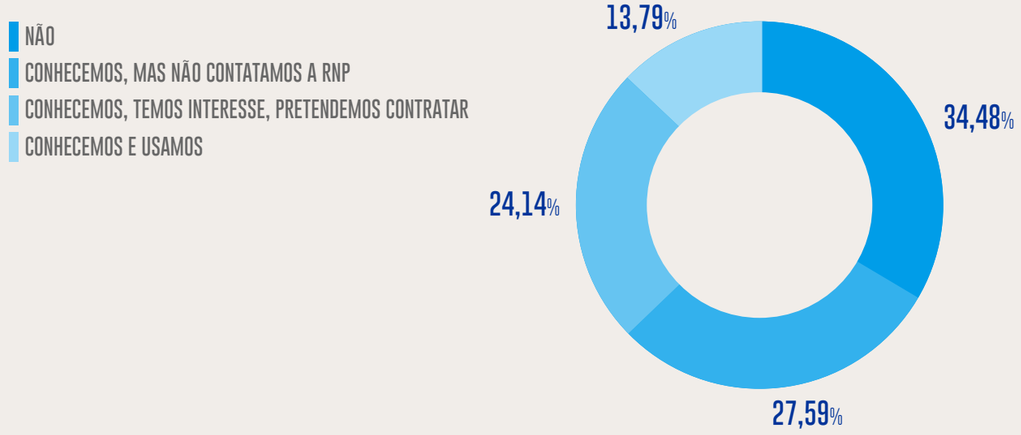


A falta de recursos humanos qualificados tem impactado negativamente as organizações e os seus esforços de elevar o nível de maturidade em segurança cibernética. A RNP, ciente deste cenário, oferece o serviço de consultoria em segurança para as organizações que compõem o Sistema RNP, de forma exclusiva. Com isso, é possível contar com uma solução customizada conforme as necessidades da instituição.

Constatou-se que 34,48% das instituições que participaram da pesquisa não conheciam este serviço, 13,79% já conheciam e usavam, e 24,14% ainda pretendem contratar. Os serviços de Estruturação do processo de gestão de vulnerabilidades (70,69%), bem como a Adequação à LGPD (62,07%) e o Diagnóstico de Maturidade em SI (62,07%) foram os serviços de maior interesse.

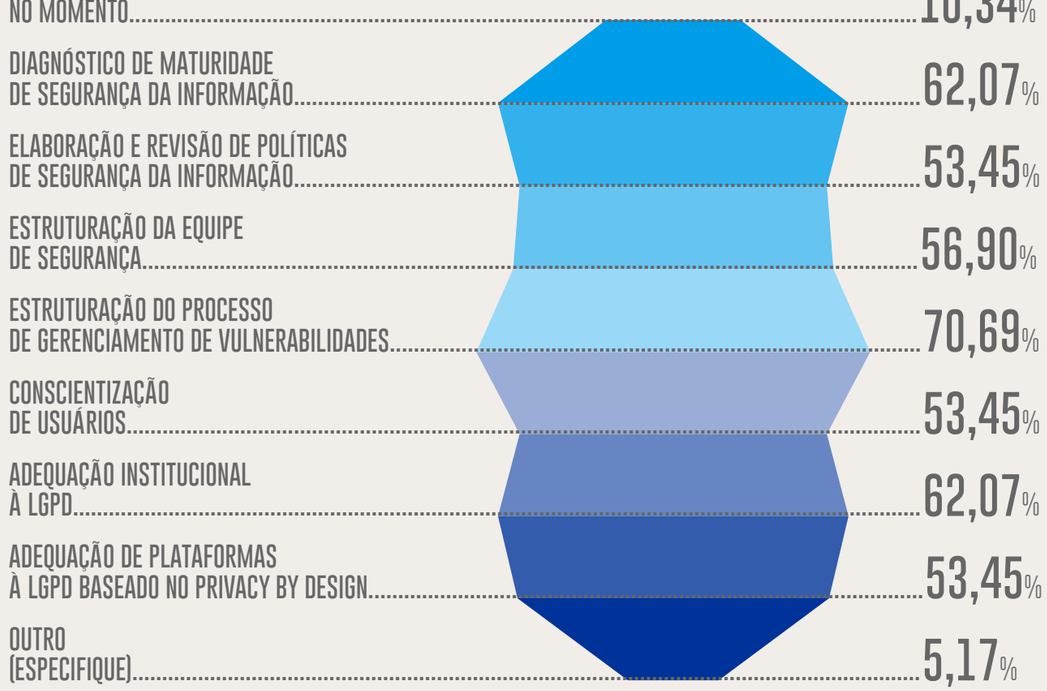
QUESTÃO

A sua organização conhece e usa os serviços consultivos em segurança da informação da RNP?



QUESTÃO

A sua organização se interessaria por alguns destes serviços consultivos da RNP? Se sim, por favor indique qual(is).



PRIVACIDADE E TRANSPARÊNCIA_

A privacidade tornou-se uma missão crítica para as organizações no mundo todo. Muitos países promulgaram leis de privacidade, e usuários optam hoje por não se relacionarem com organizações que não protejam seus dados. A privacidade vem ganhando relevância nas discussões corporativas e, em muitos casos, métricas de privacidade vêm sendo apresentadas à alta gestão. Além disso, as habilidades e competências em privacidade e proteção de dados vêm se tornando mais importantes, especialmente entre os profissionais de segurança.

De acordo com a SurfShark – empresa especializada em privacidade – o vazamento de dados vitimou 18,2 milhões de pessoas no mundo em 2021. O cenário não foi diferente no Brasil. No *ranking* mundial, o Brasil foi o 12º que mais contabilizou vazamento de dados. Ao todo, 286 mil brasileiros ficaram expostos por meio de suas informações na Internet.

Segundo o Cisco 2022 Data Privacy Benchmark Study, divulgado em janeiro de 2022, 84% dos respondentes da pesquisa disseram que no Brasil a regulação da privacidade teve impactos positivos, contra 4% que acreditam o contrário.

A RNP também tem sido sensível a esta vertiginosa transformação, que tem impactado também as instituições de ensino, pesquisa e inovação. Com a chegada da Lei nº 13.709, de 14 de agosto de 2018, mais conhecida como Lei Geral de Proteção de Dados Pessoais (LGPD), e com a necessidade das organizações estarem em conformidade com ela, a RNP inicia uma série de ações que mais tarde reverteriam no estabelecimento do chamado "Programa LGPD na RNP". Este programa inclui ações diversas de apoio às instituições de comunidade de ensino, pesquisa e inovação nos seus processos de adequação à LGPD, sustentadas em três pilares: capacitação, consultoria especializada e apoio metodológico.

A RNP TAMBÉM TEM SIDO SENSÍVEL A ESTA VERTIGINOSA TRANSFORMAÇÃO, QUE TEM IMPACTADO TAMBÉM AS INSTITUIÇÕES DE ENSINO, PESQUISA E INOVAÇÃO.

SURFSHARK DATA BREACH STATISTICS BY COUNTRY

CISCO 2022 DATA PRIVACY BENCHMARK STUDY

PORTAL DE PRIVACIDADE PROGRAMA LGPD PARA RNP

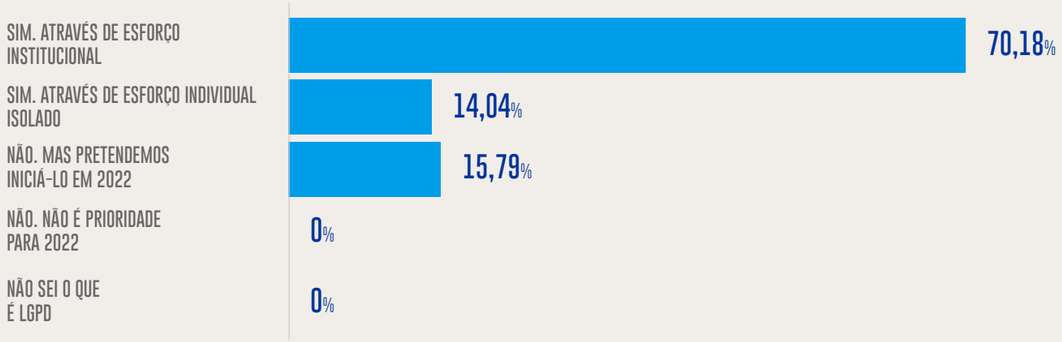
Mais do que uma jornada em busca de conformidade, é importante que o processo de adequação seja enxergado como o passo inicial para uma mudança organizacional que trará uma série de benefícios para todos.

As organizações encontram-se em diferentes estágios de maturidade no processo de adequação. A LGPD está no radar da maioria delas, 84,22% indicaram ter iniciado o processo de adequação, algumas por meio de esforço institucional (70%), outras por de esforços isolados. Dos que já iniciaram o processo, 42,11% encontram-se na fase de Preparação, 12,28% na de Organização, e uma boa parcela (31,58%) na fase de Desenvolvimento e Implantação. Do grupo das respondentes, nenhuma chegou à etapa de Governança e Melhoria contínua.

Nesta desafiadora jornada, o engajamento da alta gestão é primordial, é por onde tudo começa. É fundamental que ela reconheça, perante toda a organização, a importância de se adequar à lei e os benefícios de se implantar um programa de privacidade de forma permanente. O sucesso de um projeto de adequação à LGPD depende em muito do comprometimento da alta gestão, a jornada torna-se mais leve. De acordo com o resultado da pesquisa, o panorama é favorável, considerando uma nota 7/10 como "estar comprometido", em torno de 60% das organizações contam com uma alta gestão sensibilizada e comprometida com o processo de adequação.

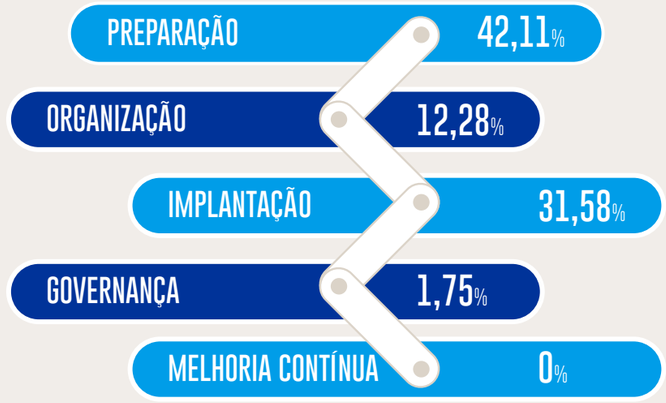
QUESTÃO

Sua organização já iniciou o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD)?



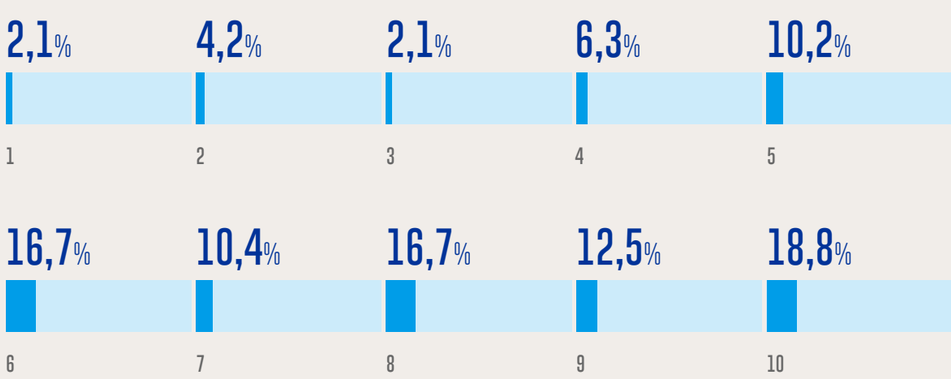
QUESTÃO

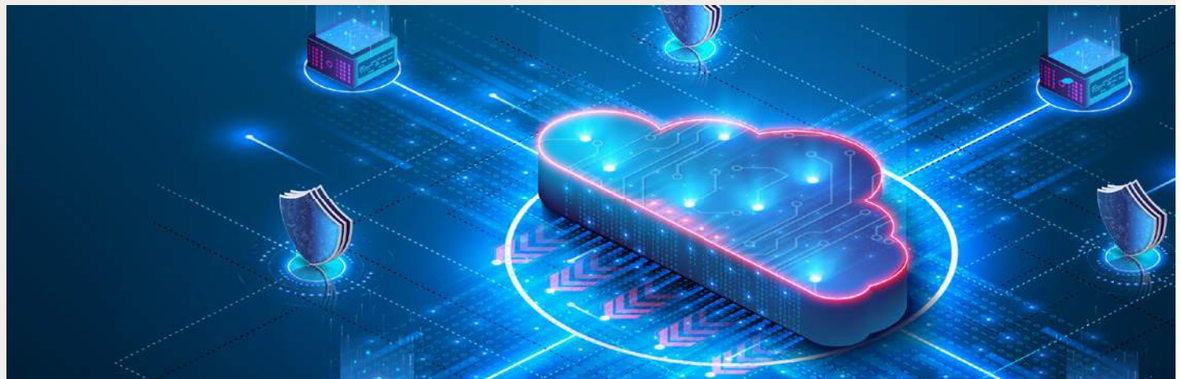
Em qual etapa de adequação à LGPD sua organização se encontra?



QUESTÃO

Em uma escala de 1 a 10 (sendo 10 a maior), como você avalia o comprometimento da alta gestão para com o atendimento à LGPD?

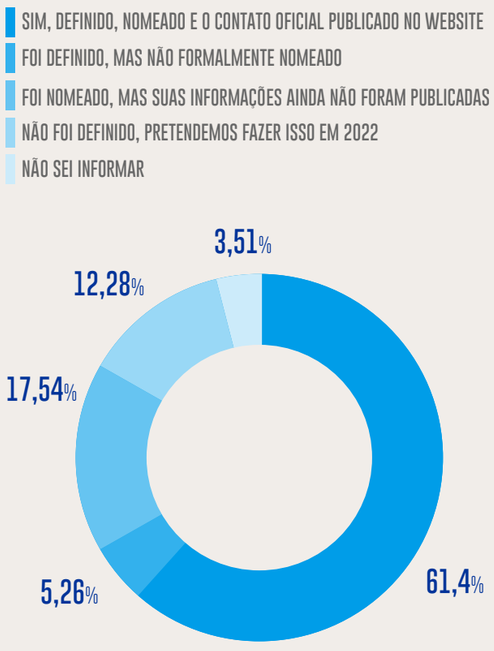




O Encarregado pelo tratamento de dados pessoais, também conhecido como Data Protection Officer (DPO), possui a função de atuar como canal de comunicação entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). Além disso, o Encarregado tem como atribuição monitorar o cumprimento da LGPD, buscando garantir que o tratamento de dados ocorra em conformidade com a lei. A sua nomeação é exigida em lei. Um número relevante de organizações (61,45%) disse já ter definido, nomeado e divulgado publicamente o Encarregado. Outras 22,80%, embora já tenham definido esta figura, disseram que o Encarregado ocupa cargo em áreas diretamente ligadas à alta gestão – destacadamente Ouvidorias – e um grupo menor em áreas de TI (8,77%) e Segurança (1,75%).

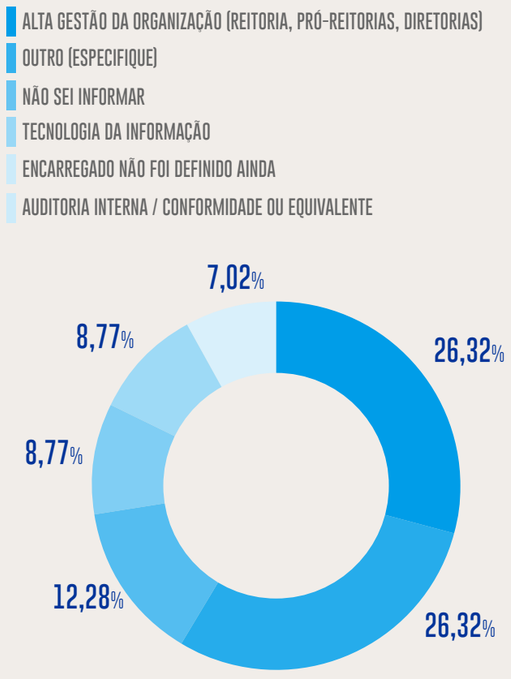
QUESTÃO

O Encarregado pelo tratamento de dados pessoais (DPO) foi definido, nomeado e as informações de contato divulgadas no website da organização?



QUESTÃO

Se já tiver sido definido, qual a área de atuação do Encarregado?

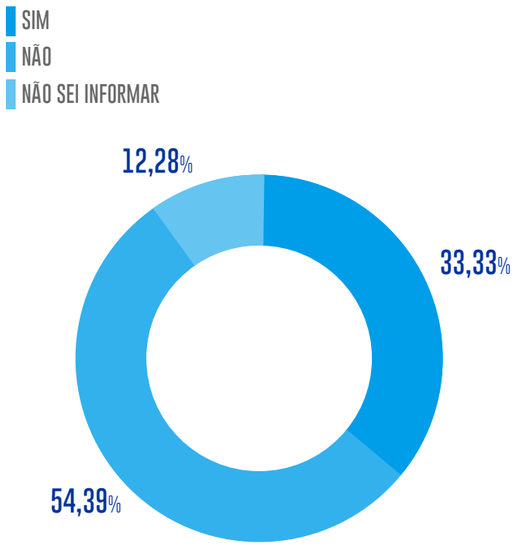


A criação de um comitê multidisciplinar de privacidade e proteção de dados pessoais não é uma obrigação legal, porém uma boa prática recomendada. Atua como facilitador e instância de apoio no processo de adequação à lei e na eventual implantação de um programa de governança de dados. Os membros do comitê poderão ser verdadeiros aliados à proteção de dados pessoais dentro das organizações.

Quanto à formação do comitê multidisciplinar, um terço (33,33%) das instituições respondentes indicaram possuir esta instância, porém um número elevado (54,39%) de organizações ainda não o fez. Na composição dos comitês já constituídos, há uma forte presença de áreas como Tecnologia da Informação (90,48%), Processos (85,71%), Jurídico (71,43%), Auditoria e Controle (42,86%) e envolvimento da Alta gestão (pró-reitorias, diretores etc. - 71,43%).

QUESTÃO

Sua organização tem Comitê Multidisciplinar de Proteção de Dados Pessoais?



QUESTÃO

Se o comitê multidisciplinar tiver sido constituído, indique de quais áreas são os seus membros (indique todas as áreas, se possível). Caso o comitê não exista, deixe em branco.

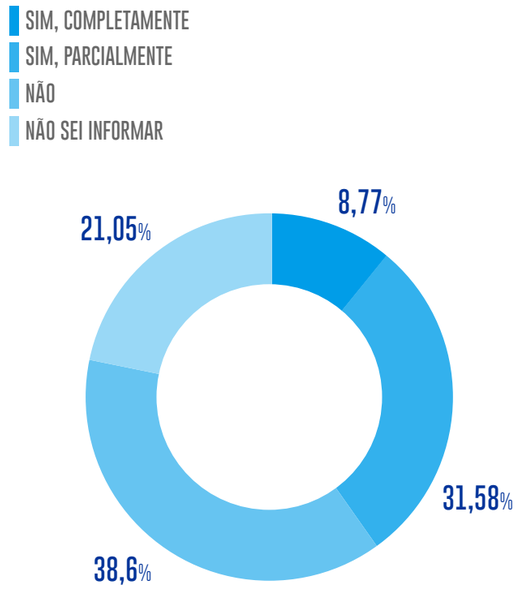
OPÇÕES DE RESPOSTA	RESPOSTA (%)
Jurídico ou Procuradoria da organização	71,43
Tecnologia da Informação	90,48
Administrativo (processos)	85,71
Marketing/Comunicações	33,33
Financeiro	23,81
Alta gestão (reitoria, pró-reitorias, diretores)	71,43
Recursos Humanos	47,62
Auditoria interna ou Controladoria ou Compliance	42,86
Outro (especifique)	28,57

São diversos os atores citados na LGPD, destacadamente encarregado de dados, ANPD (Autoridade Nacional de Proteção de Dados) e os diferentes agentes de tratamentos de dados (titular, controlador, operador, dentre outros). De uma maneira simplificada, a figura abaixo mostra como se dá a interação entre eles.

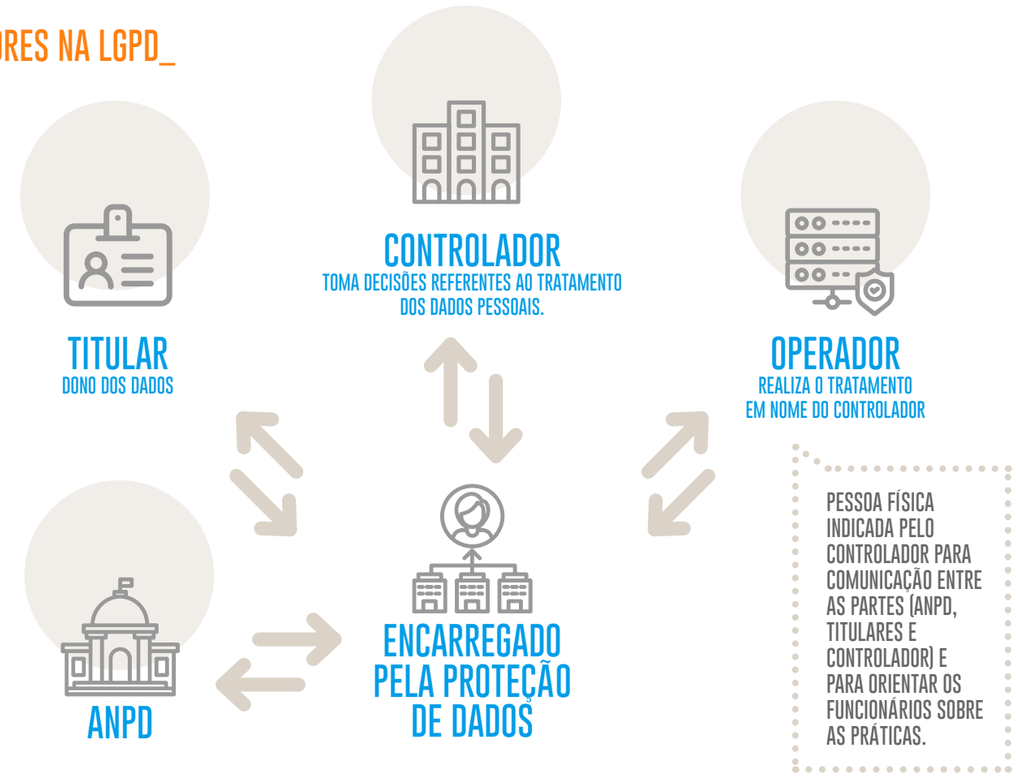
Quanto ao mapeamento dos operadores de dados pessoais, apenas 8,77% das organizações já concluíram essa etapa na sua totalidade, e 31,58% o fizeram parcialmente. Um volume expressivo (38,6%) de instituições ainda não o iniciou.

QUESTÃO

Sua organização mapeou quem são os chamados "operadores" de dados pessoais?



ATORES NA LGPD_



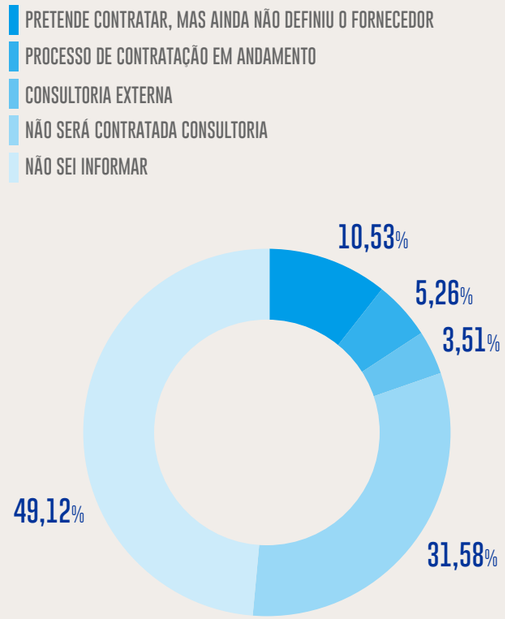
A maioria das organizações do Sistema RNP ainda sofre com a falta de recursos humanos qualificados dedicados na área de segurança e privacidade. Sendo assim, uma parcela apoia-se em consultorias externas – 3,51% delas contam com este apoio, outras pretendem contratar (5,26%) – porém, quando o assunto é adequação à LGPD, a maioria opta por arregaçar as mangas e topar o desafio!

A RNP oferece o serviço de consultoria especializada em LGPD para as organizações que compõem o Sistema RNP.

Com esse serviço, é possível contar com uma solução customizada conforme as necessidades de adequação da instituição. As atividades vão desde o apoio no desenvolvimento de um plano de adequação até a adoção de Privacy by Design na instituição. Constata-se que 40,35% não conhecia os serviços consultivos de privacidade da RNP, apenas uma parcela mínima (7,02%) conhecia e fazia uso, sendo que 14,04% manifestou interesse e pretende contratar.

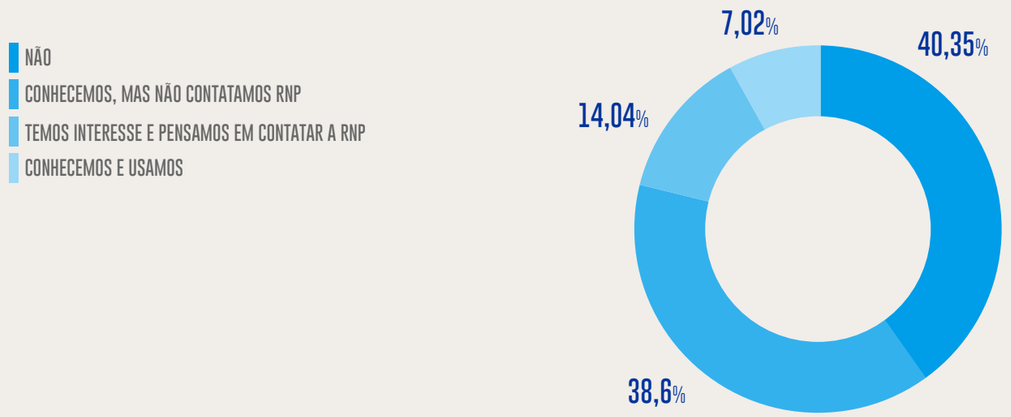
QUESTÃO

Sua organização contratou ou pretende contratar uma consultoria especializada para contribuir com a adequação à LGPD?



QUESTÃO

A sua organização conhece e usa os serviços consultivos de privacidade (adequação à LGPD) da RNP?

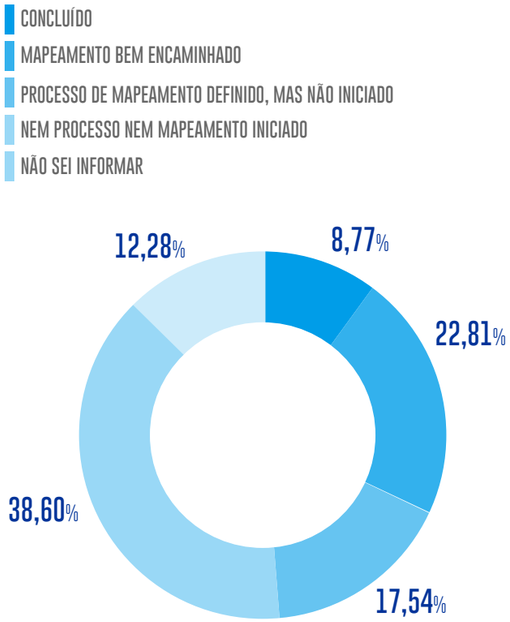


Fazer um correto mapeamento de dados e análise do fluxo e ciclo de vida dos mesmos é crucial para o sucesso de qualquer projeto de adequação. O mapeamento é o processo pelo qual é possível conhecer de maneira aprofundada as atividades de tratamento de dados pessoais na organização.

No que diz respeito ao mapeamento dos fluxos de dados pessoais, somente 8,77% das organizações concluíram este processo. A maioria das instituições (78,95%) expressou tratar e manipular dados pessoais sensíveis. Igualmente expressiva (66,77%) foi a parcela de instituições que lida com dados pessoais de crianças e/ou adolescentes.

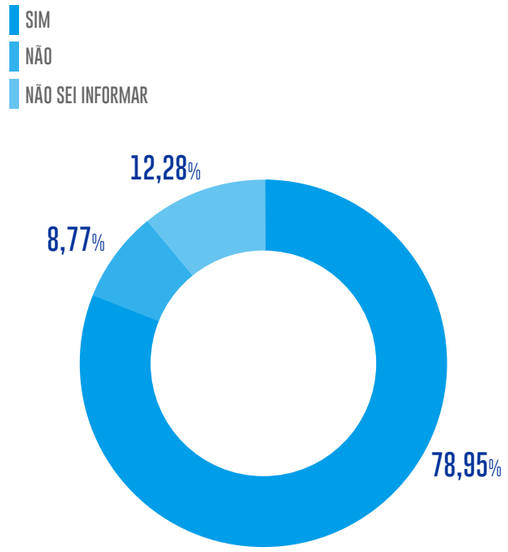
QUESTÃO

Em relação ao processo de mapeamento dos fluxos de dados pessoais, em que etapa sua organização se encontra?



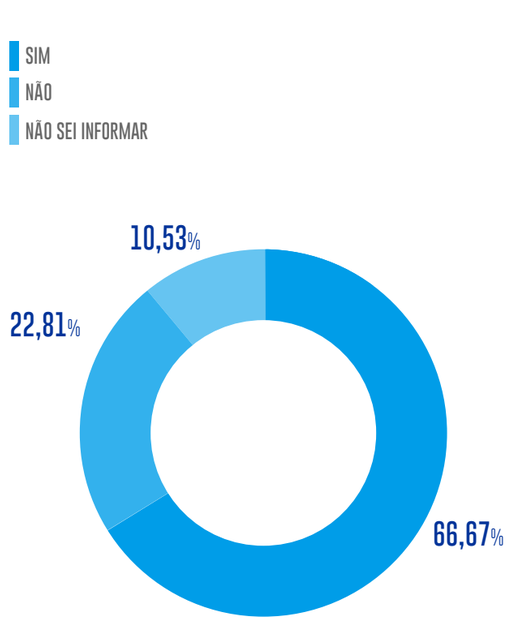
QUESTÃO

Sua organização trata/manipula dados sensíveis?



QUESTÃO

Sua organização trata/manipula dados pessoais de crianças e/ou adolescentes?

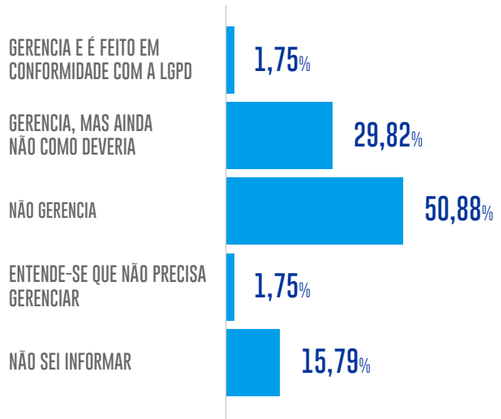


A LGPD determina que o titular tem direito ao acesso facilitado a informações sobre o tratamento dos seus dados. Neste quesito, foram constataram diferentes níveis de maturidade dentre as organizações respondentes – enquanto algumas já implantaram um processo de atendimento aos titulares (12,28%) conforme orientado em lei, um expressivo número de instituições não dispõe sequer de um canal para a gestão dos direitos dos titulares (43,96%).

Ainda em relação aos direitos dos titulares, é crucial que a instituição conte com um processo de gestão do consentimento dos usuários para tratamento dos seus dados pessoais. Metade (50,88%) das organizações não faz esta gestão, apenas 1,75% o faz de forma plena, e uma parcela significativa (29,82%) o faz de forma parcial.

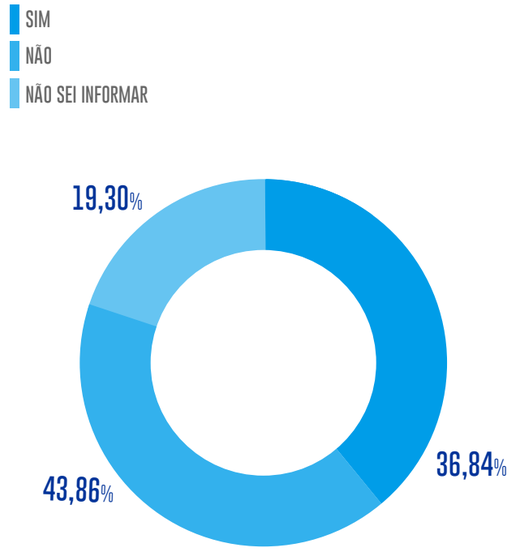
QUESTÃO

Sua organização gerencia o consentimento dos usuários para tratamento de seus dados pessoais (por exemplo, para envio de newsletter ou propaganda)?



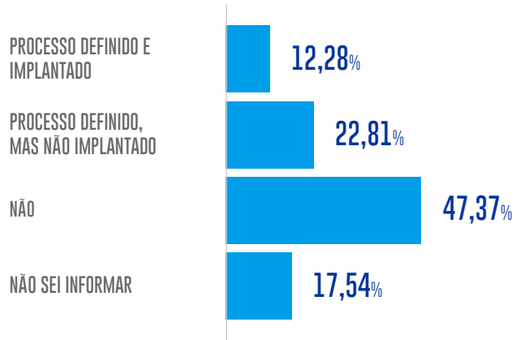
QUESTÃO

Sua organização possui um canal (telefone, e-mail, site) para a gestão dos direitos dos titulares?



QUESTÃO

Sua organização já definiu e implantou um processo para responder a solicitações dos titulares dos dados pessoais?



Existem outras três importantes atividades na jornada de adequação: Assesment (Diagnóstico), Relatório de Impacto à Proteção de Dados Pessoais (RIPD) e Plano de Ação para adequação.

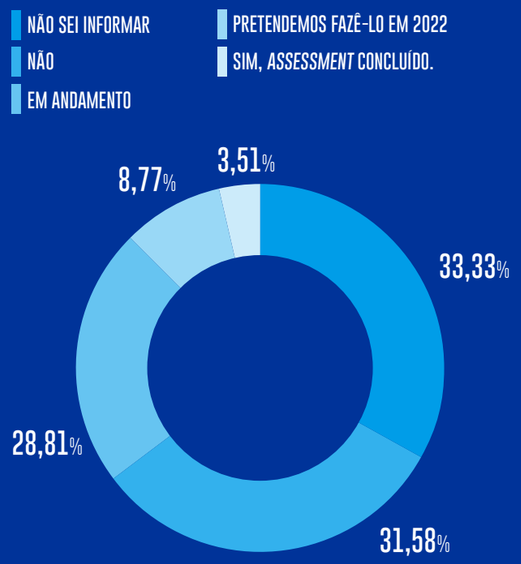
O Assessment é um procedimento inicial que visa o diagnóstico do cenário atual da organização em relação ao tratamento de dados pessoais que esta realiza. A pesquisa apontou que apenas 3,51% das organizações finalizou esta etapa, outros 22,81% o tem em andamento e, aproximadamente um terço (31,58%) sequer iniciou o processo.

O RIPD visa demonstrar quais os dados pessoais que são coletados, tratados, usados, compartilhados e quais as medidas para mitigação dos riscos que possam afetar as liberdades e os direitos dos titulares são usados. Foi constatado que 10,53% das organizações concluíram sua elaboração, em outras 12,53%, a elaboração do RIPD encontra-se em andamento e mais da metade (57,89%) sequer a iniciaram.

Já o Plano de Ação estabelece diretrizes e necessidades imprescindíveis à adequação à LGPD. Por meio dele, é possível vislumbrar projetos estruturantes que possibilitarão o reforço da privacidade dos dados pessoais, verificar condutas que necessitam ser melhoradas e otimizar os processos como um todo. Um quarto das organizações (25%) disseram ter desenvolvido este plano, outras 7,02% não concluíram e 35,09% informou não ter iniciado esta etapa.

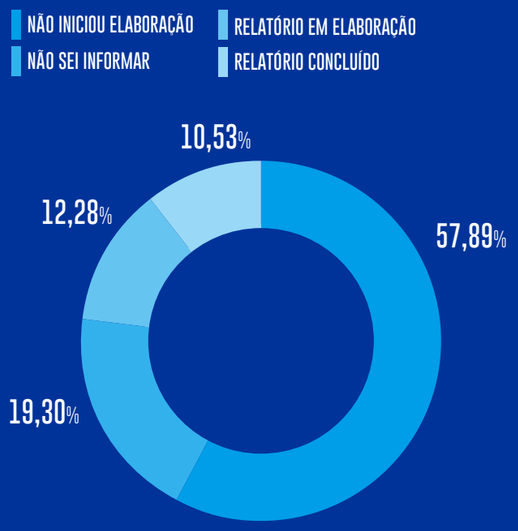
QUESTÃO

Sua organização fez um *assessment* para entendimento do cenário interno para direcionar a adequação?



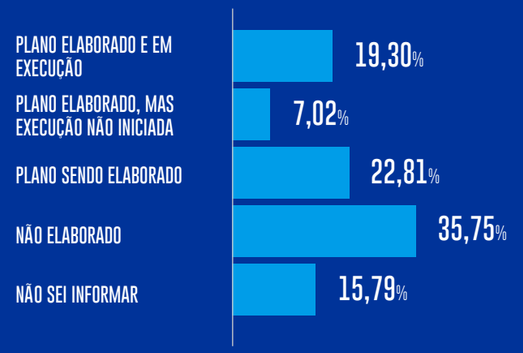
QUESTÃO

Sua organização já elaborou o relatório de impacto à proteção de dados pessoais (RIPD)?



QUESTÃO

Sua organização elaborou um plano de ação para adequação?



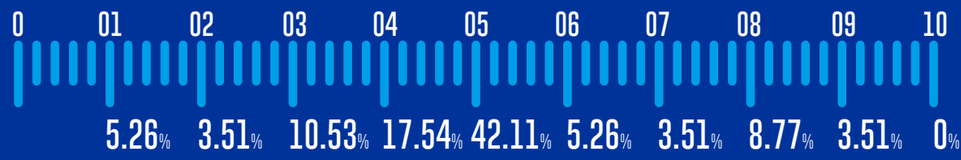
Ainda em relação ao processo de adequação à LGPD e à implantação de um programa de governança de dados, há dois temas importantes aos quais as organizações precisam dedicar esforços: a promoção da cultura de proteção de dados pessoais e a implementação de controles de segurança dos dados - dados devem ser protegidos!

A pesquisa constata que a cultura de proteção de dados pessoais é ainda um aspecto desafiador para as organizações. Na maioria delas (70,18%), a avaliação deste quesito ficou entre 3 e 5, numa escala de 1 a 10.

No que diz respeito ao nível de maturidade da organização em relação à implementação de controles de segurança visando evitar vazamentos de dados pessoais, a opinião está dividida. Enquanto uma parcela expressiva (56,15%) faz uma avaliação entre 3-5, um outro grupo avalia este quesito com pontuação 7, numa escala de 1 a 10.

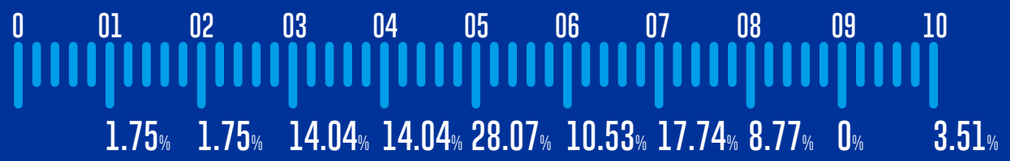
QUESTÃO

Em uma escala de 1 a 10 (sendo 10 a maior), como você avalia a cultura de proteção de dados pessoais de sua organização?



QUESTÃO

Em uma escala de 1 a 10 (sendo 10 a maior), como você avalia o atual conjunto de controles de segurança para evitar/tratar vazamentos de dados pessoais de sua organização?



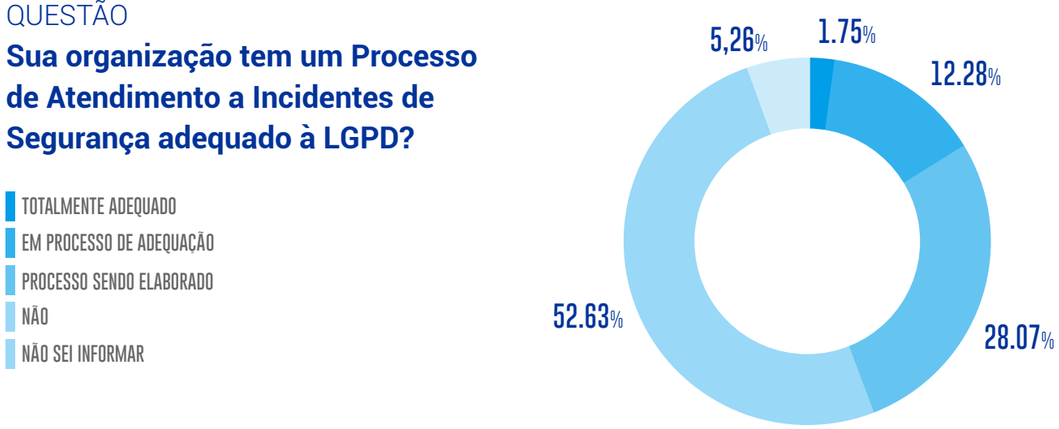
Assim como o processo de gestão do consentimento, a elaboração do aviso de privacidade, bem como a adequação do processo de tratamento de incidentes fazem parte das entregas "mais urgentes" na jornada de adequação de uma organização à LGPD. A lei já está em vigor, incidentes envolvendo dados dos seus usuários podem ser comprometidos, usuários já podem fazer uso dos seus direitos, sem contar que há prazos e penalidades previstos.

O Aviso de Privacidade é uma comunicação direcionada aos indivíduos externos à organização na condição de titulares de dados pessoais informando e descrevendo as operações de tratamento de dados realizadas pela organização. A pesquisa apontou que quase metade (47,37%) das instituições respondentes não elaboraram esta comunicação ainda. Apenas 14,04% delas o fizeram e outras (24,56%) encontram-se no meio do caminho.

Em relação à adequação do processo de tratamento de incidentes à lei, nenhuma das instituições respondentes realizou esta adequação – mesmo as que já têm o processo em si implementado (12,28%). Mais de 80% das instituições participantes sequer possuem um processo de tratamento de incidentes.

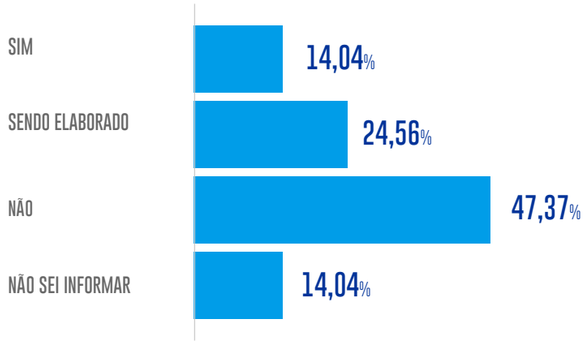
QUESTÃO

Sua organização tem um Processo de Atendimento a Incidentes de Segurança adequado à LGPD?



QUESTÃO

Sua organização já tem uma Política/Aviso de Privacidade (externa)?



Dentre os três principais desafios encontrados neste processo de adequação, certamente a realização do mapeamento e fluxo de dados pessoais em todos os processos da organização (80,70%) tem sido apontado como a fase mais onerosa. Seguido pela promoção da cultura de privacidade e proteção de dados pessoais (50,88%), bem como a implantação dos controles de segurança (50,88%).

QUESTÃO

Quais os três (3) principais desafios para sua organização estar em conformidade com a LGPD?

Mapear todas as formas de tratamento de dados pessoais em todos os processos da organização (inventário e fluxo de dados)	80,70%
Criar processos para atender aos pedidos dos titulares dos dados (direitos de acesso, portabilidade, remoção, notificação etc.)	33,33%
Promover a cultura da proteção de dados pessoais na organização	50,88%
Engajamento da alta gestão	19,30%
Contratar/capacitar consultoria jurídica especializada para verificação de conformidade	8,77%
Implantação de controles de segurança para proteção de dados pessoais (suporte físico e/ou eletrônico)	50,88%
Criar e atualizar contratos/acordos com clientes, fornecedores e parceiros em conformidade com a lei	10,53%
Gestão do consentimento dos usuários	12,28%
Orçamento para colocar em prática o plano de ação	17,54%

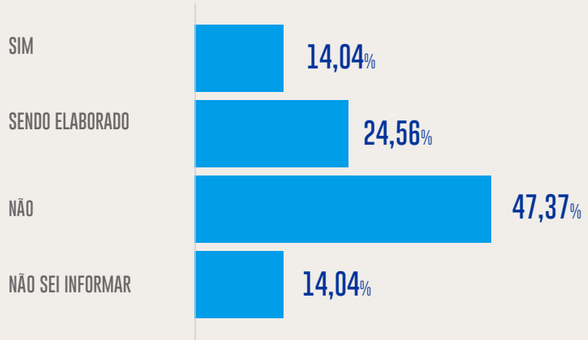
Dentre as ações que fazem parte do “Programa LGPD da RNP” anteriormente citado, em particular no âmbito do apoio metodológico, duas iniciativas ganham destaque: o “Método RNP para adequação à LGPD”, que objetiva auxiliar as organizações em seus processos de adequação e na construção dos seus programas de governança em privacidade; e o SIG-LGPD@RNP, fórum restrito que visa oferecer um espaço para interação e troca de conhecimento e experiências sobre o tema privacidade e proteção de dados pessoais e, a cada ciclo, oferece apoio a um grupo de instituições nos seus processos de adequação, escolhidas por de um processo de seleção.

Dentre o grupo de respondentes, apenas 7,02% participaram da primeira edição do SIG e 22,81% vem participando do segundo. No entanto, aproximadamente 80% delas dizem conhecer a iniciativa, inclusive a maioria (35,09%) indicou ter interesse em participar ativamente.

Quanto ao Método, apenas uma tímida parcela (14,04%) indicou conhecê-lo, a maioria não tinha conhecimento desta iniciativa - ações de divulgação se fazem necessárias.

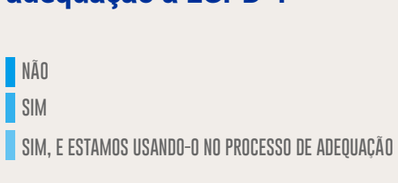
QUESTÃO

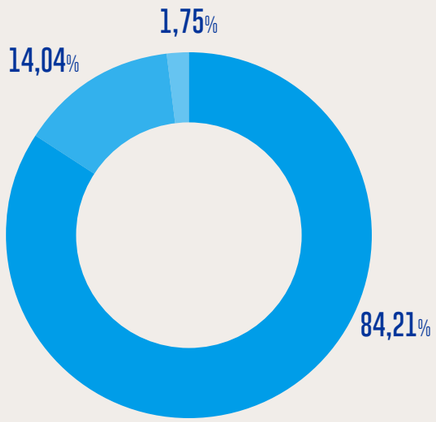
Você conhece o fórum de apoio “SIG-LGPD@RNP”?



QUESTÃO

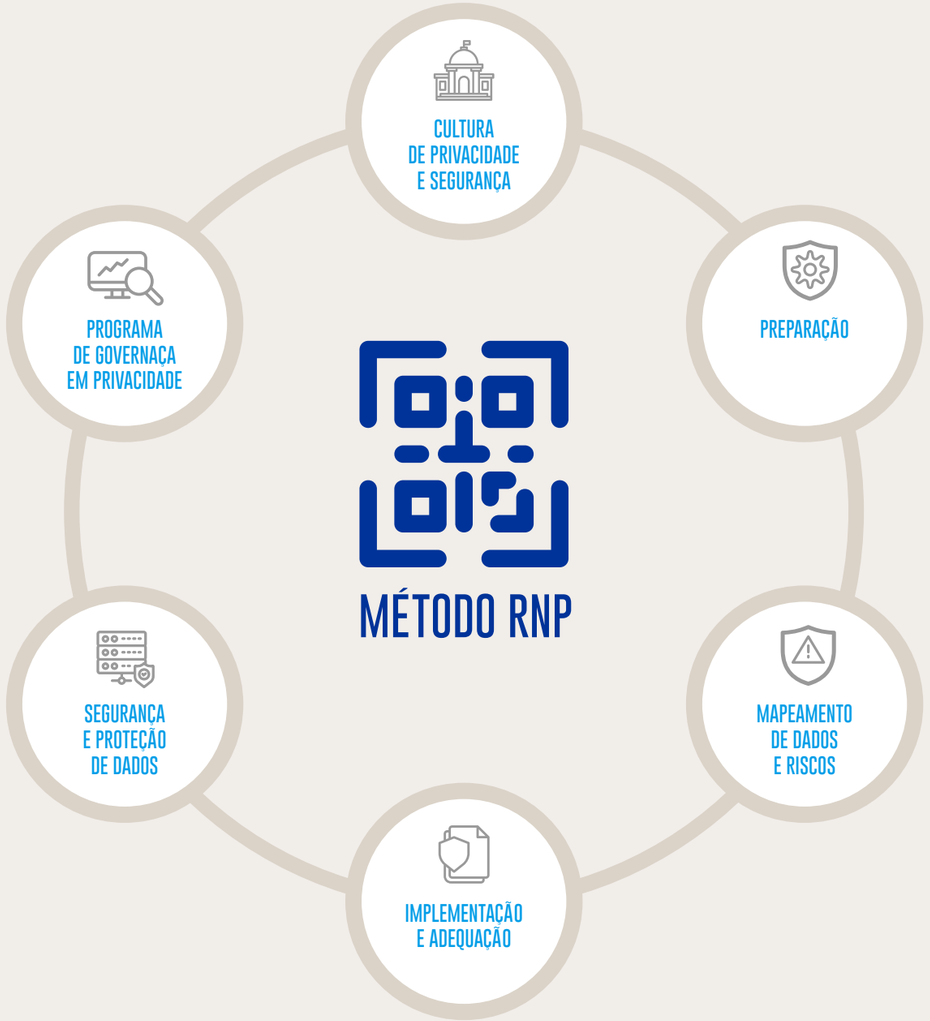
Você conhece o “Método RNP para adequação à LGPD”?





QUESTÃO

Você conhece o “Método RNP para adequação à LGPD”?



HTTPS://PRIVACIDADE.RNP.BR

HTTPS://WWW.RNP.BR/PRIVACIDADE

Se a Lei de Acesso à Informação (LAI) enfatizou o desenvolvimento da transparência na Administração Pública, a Lei Geral de Proteção de Dados Pessoais (LGPD), por sua vez, propõe-se a fortalecer a privacidade, a autodeterminação informativa e os direitos dos titulares de dados pessoais.

Pode parecer impossível conciliar transparência pública com privacidade e proteção de dados pessoais, mas ambas as leis são compatíveis, e não há prevalência entre elas, devendo elas caminharem em um espaço harmônico.

Em comparação à LGPD – uma lei relativamente nova –, a LAI cumpriu 12 anos de existência, portanto, não surpreende que 87,72% das organizações já tenham um responsável para receber e atender solicitações fundamentadas na LAI e que 73,68% já possui um processo estruturado de Serviço de Informação ao Cidadão (SIC), requisitos contemplados na lei. Assim, também metade (50,88%) das instituições dispõe de um espaço de transparência ativa para acesso aos documentos corporativos produzidos.

QUESTÃO

LAI: Lei de Acesso à Informação

QUESTÕES	SIM	NÃO	EM DESENVOLVIMENTO	PLANEJAMOS TER EM 2022	NÃO SEI INFORMAR
A SUA ORGANIZAÇÃO POSSUI UMA POLÍTICA DE TRANSPARÊNCIA DE DADOS?	40,35%	19,3%	10,53%	1,75%	28,07%
A SUA ORGANIZAÇÃO POSSUI UM RESPONSÁVEL POR RECEBER E ATENDER AOS PEDIDOS DE INFORMAÇÃO VIA LEI DE ACESSO À INFORMAÇÃO (LAI)?	87,72%	3,51%	1,75%	1,75%	5,26%
A SUA ORGANIZAÇÃO POSSUI UM PROCESSO ESTRUTURADO DE SIC (SERVIÇO DE INFORMAÇÃO AO CIDADÃO)?	73,68%	8,77%	1,75%	0,00%	15,79%
A SUA ORGANIZAÇÃO POSSUI UM ESPAÇO DE TRANSPARÊNCIA ATIVA PARA ACESSO AOS PRINCIPAIS DOCUMENTOS PRODUZIDOS PELA ORGANIZAÇÃO?	50,88%	8,77%	12,28%	3,51%	24,56%

DESENVOLVIMENTO DE COMPETÊNCIAS_

Foi mencionado anteriormente como o fenômeno de transformação digital e a pandemia de Covid-19 acelerou muitas mudanças no mundo todo, em todas as esferas e em todas as dimensões (governos, diferentes setores econômicos, sociedade, cidadãos), e como aspectos envolvendo segurança e privacidade se tornaram tão críticos.

Este cenário leva à necessidade de profissionais qualificados para tratar das principais funções da segurança cibernética, isto é, identificação, proteção, detecção, resposta e recuperação.

A complexidade existente nas funções de cibersegurança aumenta com a multidisciplinaridade do tema, que envolve aspectos tecnológicos, humanos e processuais, que se somam à multidimensionalidade que envolve diferentes camadas tecnológicas. Urgem novas propostas e adequações no currículo dos programas de formação profissional.

O reflexo mais evidente da relevância do mercado de cibersegurança é o aumento do número de incidentes cibernéticos e a falta de profissionais qualificados em cibersegurança. De acordo com o estudo da força de trabalho em cibersegurança da (ISC)2, em 2021 – Cybersecurity Workforce Study 2021 – o número de vagas não preenchidas no Brasil era de mais de 441 mil profissionais, sendo 2,7 milhões em todo o mundo . Ao mesmo tempo, o número de *startups* de segurança cibernética que recebem investimentos no mundo, e as que se tornam unicórnios, é alto se comparado com outros setores, o que evidencia a preocupação de desenvolvimento tecnológico na área.

(ISC)2 CYBERSECURITY WORKFORCE STUDY 2021

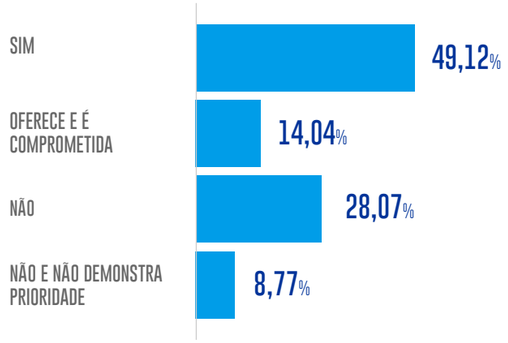
NESTE CONTEXTO, A RNP RECONHECE A IMPORTÂNCIA DE CONTRIBUIR COM O SISTEMA RNP E O PAÍS NO DESENVOLVIMENTO DE COMPETÊNCIAS NA ÁREA, E EM CRIAR SINERGIAS ENTRE GOVERNO, INDÚSTRIA, EMPRESA E ACADEMIA COM ESTE FIM.

Com a transformação digital e a consequente influência da tecnologia no meio corporativo, a capacitação da equipe de TI traz aumento do desempenho dos profissionais, o que faz que a atividade da organização atinja patamares superiores. A capacitação das equipes é um dos requisitos mais importantes neste processo e precisa ser realizada periodicamente.

De acordo com os respondentes da pesquisa, 63,16% das instituições oferecem regularmente oportunidades de capacitação e treinamento para as equipes técnicas, 14,04% destacam ainda o comprometimento da instituição. Apenas 8,77% não prioriza esta necessidade. Administração segura, resposta a incidentes e gestão de identidade são apontados como principais competências que a maioria possui. Já em análise forense e gestão de vulnerabilidades parece existir *gap*.

QUESTÃO

Sua organização oferece periodicamente oportunidades de capacitação e treinamento às equipes técnicas?



QUESTÃO

Indique quais das seguintes competências técnicas a sua instituição possui e quais precisa desenvolver:

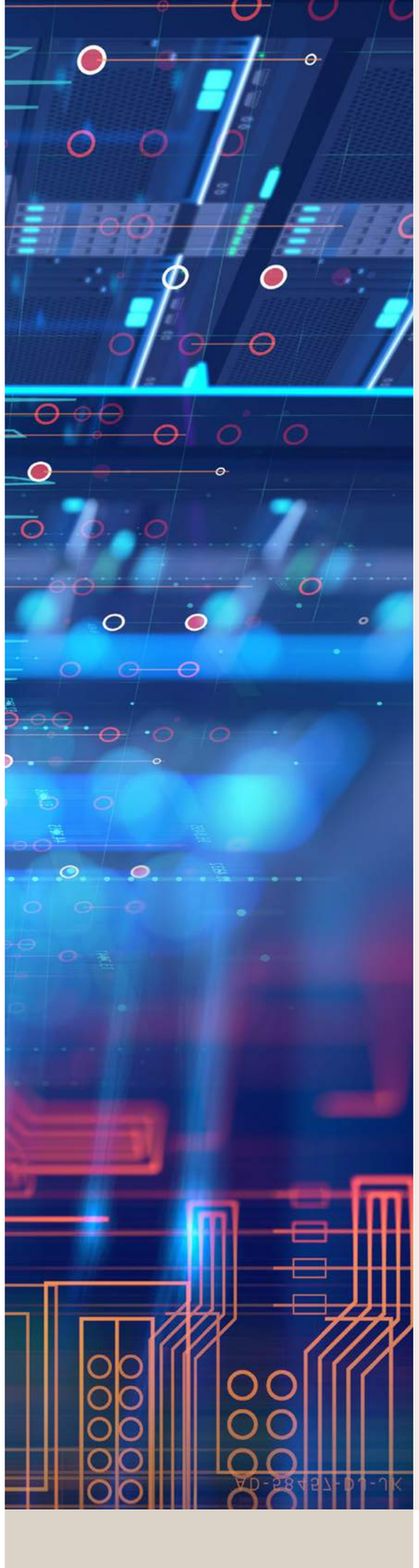
QUESTÕES	POSSUI	POSSUI PARCIALMENTE	PRECISA DESENVOLVER
Administração segura/controle tecnológico de segurança (firewall, IDS/IPS, antimalware etc.)	40,35%	45,61%	14,04%
Resposta a incidentes	22,81%	45,61%	31,58%
Pentest/Ethical hacking/gestão de vulnerabilidades	7,02%	35,09%	57,89%
Política de segurança/gestão de riscos/ gestão de segurança da informação/ privacidade	12,28%	52,63%	35,09%
Gestão de identidades	22,81%	33,33%	43,86%
Desenvolvimento seguro	7,02%	45,61%	47,37%
Forense digital/Análise de malware	5,26%	22,81%	71,93%
Educação e conscientização	10,53%	52,63%	36,84%

A Escola Superior de Redes (ESR) é a unidade de serviço da RNP criada para promover a capacitação, o desenvolvimento profissional e a disseminação de conhecimento em Tecnologias da Informação. Ao todo são 15 anos de mercado e mais de 30 mil alunos capacitados.

A cada ano, a ESR, no âmbito do Contrato de Gestão, oferece gratuitamente um número de vagas de capacitação às organizações usuárias que compõem o Sistema RNP, em diversas trilhas e modalidades, em temas estruturantes de TI. Em particular, as trilhas de "Segurança" e "Governança de TI" incluem cursos em temas de Segurança e Privacidade, respectivamente. Confiram!

CLIQUE AQUI PARA MAIS INFORMAÇÕES SOBRE A ESR

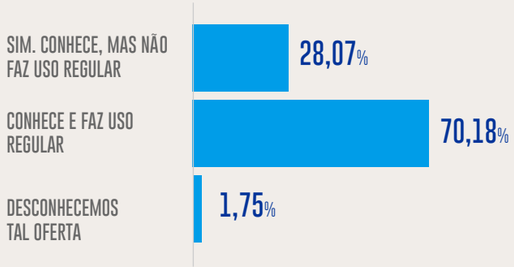
A ESR OFERTA CURSOS ESPECÍFICOS SOBRE PRIVACIDADE DE DADOS E LGPD, TANTO PARA LEIGOS QUANTO PARA QUEM TEM O DESAFIO DE ADEQUAR A SUA ORGANIZAÇÃO À LGPD.



Visando ao melhor aproveitamento desta oferta por parte da nossa comunidade, a pesquisa incluiu questões que permitisse mais divulgação deste serviço. Quase todas elas disseram ter conhecimento da oferta de vagas na ESR, porém não todas fazem uso regular da mesma. Dentre estas últimas, 31,58% indicaram que gostariam que a ESR entrassem em contato com elas.

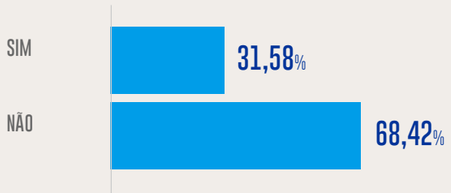
QUESTÃO

Sua organização conhece e faz uso da oferta de vagas disponíveis na Escola Superior de Redes (ESR/ RNP) para instituições usuárias do Sistema RNP?



QUESTÃO

Caso não use as vagas, gostaria que algum representante da ESR entrasse em contato para explicar o funcionamento?

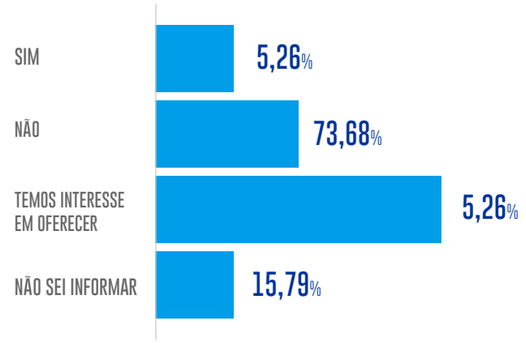


No mapeamento de ofertas de cursos de formação a nível de graduação e pós-graduação, foi constatado que a maioria das organizações respondentes indicou não possuir nenhuma oferta de formação em segurança cibernética a nível de graduação, apenas uma informou ter o curso de graduação em segurança da informação, trata-se da Universidade Federal de Ceará. Apenas algumas poucas (3,51%) manifestaram interesse em oferecer.

O cenário não foi muito diferente para o caso de pós-graduação. A maioria (73,68%) disse não possuir e novamente poucas manifestaram interesse em prover. Foram duas as organizações que informaram ter ofertas em nível de pós-graduação, são elas: Universidade Federal de Rio de Janeiro (UFRJ) e Universidade Tecnológica Federal de Paraná (UTFPR).

QUESTÃO

A sua organização tem atualmente uma oferta de formação em segurança cibernética a nível de graduação?



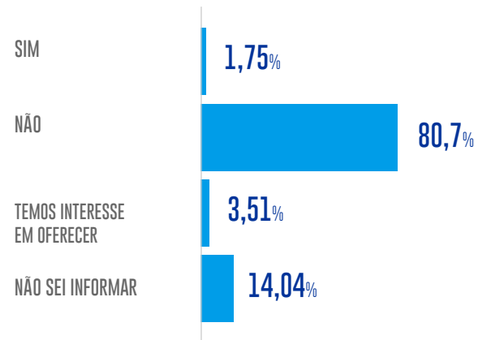
QUESTÃO

Se a sua resposta for SIM para alguma das duas perguntas anteriores, por favor especifique o tipo de oferta.

UFRJ	PÓS-GRADUAÇÃO EM GESTÃO DE SEGURANÇA DA INFORMAÇÃO
UTFPR	CURSO LATU SENSU – ESPECIALIZAÇÃO EM SEGURANÇA CIBERNÉTICA
UFC	GRADUAÇÃO EM SEGURANÇA DA INFORMAÇÃO PELO CAMPUS DE ITAPAJE

QUESTÃO

A sua organização tem atualmente uma oferta de formação em segurança cibernética a nível de pós-graduação?

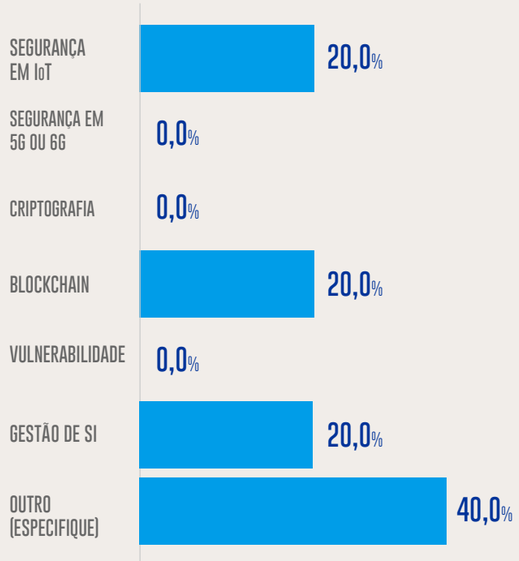


Visando ao fortalecimento do ecossistema de segurança e privacidade no Sistema RNP por meio da cooperação entre academia, governo, mercado e indústria, a pesquisa buscou mapear eventuais grupos de pesquisa e *startups* existentes nas organizações. Apenas 8,77% delas indicaram que contavam com algum grupo específico de pesquisa em segurança na sua organização, a maioria (47,37%) disse não possuir. Uma parcela bastante significativa não soube informar a respeito desse quesito.

Aquelas que afirmaram contar com o grupo de pesquisa, indicaram os temas Segurança em IoT (20%), Blockchain (20%) e Gestão de Segurança como sendo os principais temas-alvo de pesquisa (20%). O restante (40%) indicou fazer pesquisa em outros assuntos fora as opções apresentadas. Ainda neste grupo, todas indicaram não ter criado nenhuma *startup* em decorrência do grupo de pesquisa.

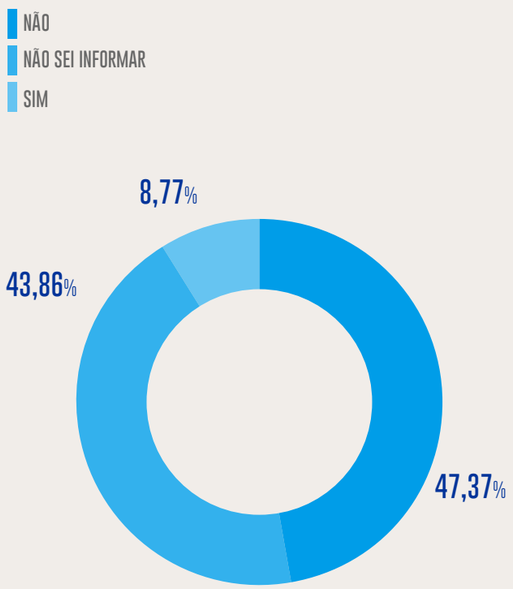
QUESTÃO

Se a resposta for positiva para a pergunta anterior, por favor indique se alguns destes temas são alvo de pesquisa desse(s) grupo(s):



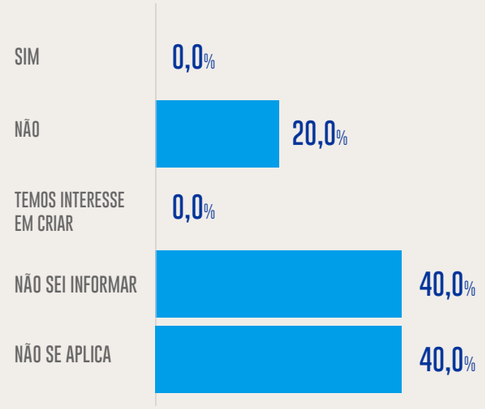
QUESTÃO

Existe algum grupo específico de pesquisa em segurança na sua organização?



QUESTÃO

Se a resposta for positiva para a pergunta anterior, por favor indique se alguma *startup* em segurança já foi criada.



CONCLUSÕES_

Os Resultados da Pesquisa de Segurança e Privacidade do Sistema RNP 2021 nos levou a algumas descobertas nos três pilares avaliados:

SEGURANÇA DA INFORMAÇÃO_

70,69% Não possuem um planejamento orçamentário em segurança. No entanto, comparado com o ano de 2020, evidencia-se uma melhora de quase 10% neste quesito.

43,10% dispõem de um Gestor de Segurança da Informação, muitos deles ocupando cargos na área de TI. Um aumento de 3,81% em relação ao ano de 2020.

50,00% instituíram formalmente um comitê multidisciplinar de Segurança da Informação.

65,52% possuem uma Política de Segurança da Informação, porém em diferentes estágios: 32,76% devidamente aprovada e divulgada, 20,69% em processo de divulgação e 12,07% aguardando aprovação.

34,48% já estabeleceram uma ETIR (ou CSIRT) – Equipe de Tratamento a Incidentes de Segurança, porém alguns ainda com uma atuação mais tímida. Prevalecem equipes com 4 ou mais membros, vários com dedicação parcial.

98,27% das organizações afirmaram conhecer o CAIS, um terço delas com uma relação muito próxima inclusive.

5,17% apenas têm o processo de Gestão de Riscos devidamente implantado. Porém, mais de um terço das respondentes o estão desenvolvendo.

20,69% oferecem periodicamente programas de conscientização e treinamento em segurança da informação aos usuários finais.

34,48% das instituições que participaram da pesquisa disseram não conhecer ainda os serviços consultivos em segurança da informação – uma divulgação maior se faz necessária.

PRIVACIDADE E TRANSPARÊNCIA_

84,22% indicaram ter iniciado o processo de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD), seja por esforço institucional ou esforço individual isolado. Um aumento de 9,22% em relação a 2020.

58,32% contam com uma alta gestão sensibilizada e comprometida – considerando uma nota 7/10 como "comprometido".

61,40% nomearam e divulgaram publicamente o seu Encarregado de Dados Pessoais. Um aumento de 3,37% em relação ao ano anterior.

54,39% não contam ainda com um comitê multidisciplinar de privacidade e proteção de dados pessoais. Em 2020, este número chegou a 62,50%.

8,77% das organizações concluíram o mapeamento dos fluxos de dados pessoais. Em 2020, este número era de apenas 3,57%.

47,37% ainda não implantaram um processo de atendimento aos titulares conforme orientado em lei.

36,84% das instituições dispõem de um canal para a gestão dos direitos dos titulares.

1,75% apenas fazem a gestão do consentimento dos usuários para tratamento dos seus dados pessoais em conformidade com a LGPD. Outro grupo (19,64%) o faz de forma parcial.

34,48% das instituições que participaram da pesquisa disseram não conhecer ainda os serviços consultivos em segurança da informação – uma divulgação maior se faz necessária.

57,89% não iniciaram a elaboração do Relatório de Impacto à Proteção de Dados Pessoais (RIPD).

47,37% das instituições respondentes ainda não elaboraram o Aviso de Privacidade.

80,70% das instituições apontam o Mapeamento dos fluxos de dados pessoais como o maior desafio na jornada de adequação.

80,00% das instituições indicaram conhecer o SIG-LGPD@RNP, iniciativa do Programa LGPD da RNP.

14,04% das instituições disseram conhecer o Método RNP para adequação à LGPD, iniciativa do Programa LGPD da RNP.

73,68% possuem um processo estruturado de Serviço de Informação ao Cidadão (SIC), para atender demandas relacionadas à Lei de Acesso à Informação (LAI).

DESENVOLVIMENTO DE COMPETÊNCIAS_

63,16% oferecem regularmente oportunidades de capacitação e treinamento para as equipes técnicas.

80,70% não possuem oferta de formação em cibersegurança em nível de graduação. Porcentagem similar à do ano de 2020.

73,68% não possuem oferta de formação em cibersegurança em nível de pós-graduação. Foram mantidos os níveis do ano de 2020.

8,77% contam com algum grupo específico de pesquisa em segurança na sua organização. Nestas organizações, os temas IoT, Blockchain e Gestão de Segurança foram indicados como sendo seus principais alvos de pesquisa.

REALIZAÇÃO_
Projetos Especiais em Segurança da Informação (PESI)
Liliana Velásquez Solha
Gerente

REDAÇÃO/EDIÇÃO_
PESI/RNP
DACS/RNP

DIAGRAMAÇÃO_
Flavia da Matta Design

REVISÃO DO PROJETO GRÁFICO
Gerência de Comunicação Corporativa/RNP

PUBLICADO PELA RNP_
Emilio Tissato Nakamura
Diretor Adjunto de Cibersegurança
Eduardo Grizendi
Diretor de Engenharia e Operações
Nelson Simões
Diretor-geral