RESULTADOS DA PESQUISA DE SEGURANÇA E PRIVACIDADE DO SISTEMA RNP

2022

RNP

RESUMO EXECUTIVO_

Em sua terceira edição, a Pesquisa de Segurança e Privacidade 2022 tem o objetivo de mapear as dificuldades e o tratamento dado a tais temas pelas instituições integrantes do Sistema RNP. Graças às 113 organizações que responderam ao questionário, a pesquisa alcançou seu maior número de respondentes até hoje.

A pesquisa é realizada pela área de Inteligência em Cibersegurança (CAIS) da Rede Nacional de Ensino e Pesquisa (RNP). Embora as instituições participem da pesquisa a convite, o preenchimento do questionário online é feito de forma voluntária por cada instituição. Este relatório consolida os resultados e, embora toda a sociedade deva se interessar pelos desafios enfrentados por suas instituições, esta análise também permite que elas mesmas se enxerguem dentro do universo ao qual pertencem.

A seção “Sobre a pesquisa” traz informações sobre o perfil dos participantes, que incluem instituições de ensino superior estaduais, federais e privadas, bem como instituições de saúde, institutos federais e institutos de pesquisa.

Com uma participação mais robusta das organizações e um histórico dos três últimos anos, a pesquisa já viabiliza uma análise inicial das mudanças na relação do Sistema RNP com o tema da segurança da informação. Pela primeira vez, por exemplo, a pesquisa revelou que há instituições no Sistema RNP em estágios avançados de conformidade com a Lei Geral de Proteção de Dados (LGPD).

De fato, a LGPD tem sido dos tópicos mais importantes para a segurança da informação e a privacidade no Brasil. Por essa razão, as organizações foram sondadas sobre o tema em vários ângulos – se já foi nomeado algum encarregado de proteção de dados, se existe um processo de tratamento de incidentes, como elas enxergam a qualidade dos controles de segurança de dados, entre outros.

A segurança da informação permanece sendo um dos pilares desta pesquisa e é também por onde começaremos a análise dos resultados. Nesse campo, é conferida a existência de processos de segurança, da política e o arcabouço normativo, bem como a postura da instituição em relação ao tema.

Por fim, olhamos para o a questão do desenvolvimento de competências e capacitação. No caso das instituições de ensino, há um panorama interno – se elas oferecem capacitação regularmente para seus próprios colaboradores – e um panorama externo, ou seja, se existe uma oferta de cursos ou programas de pesquisa. Ambos os ângulos fazem parte da pesquisa.

Com exceção das perguntas de resposta livre, que não permitem categorização, todo o questionário de 64 perguntas está exposto nos gráficos e explicado pelo conteúdo deste relatório. Boa leitura!

EDIÇÕES ANTERIORES

ACESSE AS PESQUISAS DE SEGURANÇA E PRIVACIDADE DA RNP AQUI.

A SEGURANÇA DA INFORMAÇÃO PERMANECE SENDO UM DOS PILARES DESTA PESQUISA E É TAMBÉM POR ONDE COMEÇAREMOS A ANÁLISE DOS RESULTADOS.

A RNP_

Somos a rede brasileira para educação e pesquisa. Disponibilizamos internet segura e de alta capacidade, serviços personalizados e promovemos projetos de inovação. Fomos os pioneiros, ao trazer a internet para o Brasil e hoje nossa rede chega a todas as unidades da federação. Somos qualificados como uma organização social vinculada ao Ministério da Ciência, Tecnologia e Inovação (MCTI) e mantida por esse, em conjunto com os ministérios da Educação (MEC), das Comunicações (MCom), Cultura, Saúde (MS) e 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.

CAIS_

A área de inteligência em cibersegurança da RNP, o CAIS, é responsável pela proteção das redes acadêmicas ligadas ao Sistema RNP. Em atuação desde 1997, o CAIS tem por missão promover e impulsionar o desenvolvimento e uso seguro de CT&I (Ciência, Tecnologia e Inovação).

SUMÁRIO_

RESUMO EXECUTIVO _3

SOBRE A PESQUISA _6

SEGURANÇA DA INFORMAÇÃO _8

PRIVACIDADE E TRANSPARÊNCIA _24

PRINCIPAIS FATORES NO PROCESSO DE ADEQUAÇÃO _28

DIAGNÓSTICO E MAPEAMENTO DE DADOS E RISCOS _31

ATENDIMENTO AOS TITULARES _36

INCIDENTES, CULTURA E CONTROLES DE SEGURANÇA _38

PROGRAMA LGPD E RNP _40

LAI – LEI DE ACESSO À INFORMAÇÃO _42

DESENVOLVIMENTO DE COMPETÊNCIAS _44

CONCLUSÕES _52

SOBRE A PESQUISA_

PÚBLICO-ALVO

26

ESTADOS
DA FEDERAÇÃO
E O DISTRITO FEDERAL

AUMENTO DE
88%
INSTITUIÇÕES
PARTICIPANTES

113
INSTITUIÇÕES
RESPONDENTES

Esta Pesquisa de Segurança e Privacidade tem o objetivo de mapear a situação de segurança e privacidade das instituições integrantes do Sistema RNP. O levantamento é realizado anualmente desde 2020 e utiliza um questionário online enviado diretamente às instituições por meio de seus gestores de TI, de segurança da informação ou outro representante apto a atuar como ponto focal para os temas abordados: segurança da informação, privacidade e desenvolvimento de competências (capacitação e inovação).

Sabemos, contudo, que a complexidade das organizações muitas vezes exige que as respostas sejam compiladas a partir de informações obtidas de diversos colaboradores e setores da instituição. Embora cada instituição esteja representada por um único respondente, a RNP agradece a todos que colaboraram para tornar esta pesquisa possível.

Graças a esse esforço, o número de instituições participantes teve um aumento de 88% — de 60 respondentes em 2021 para 113 em 2022. Entre universidades estaduais e federais, polos tecnológicos, instituições privadas e institutos de pesquisa, tivemos respondentes de todos os 26 estados da federação e do Distrito Federal.

Esse aumento da participação ocorreu apesar do questionário estar mais denso: foram 64 perguntas, 12 a mais que na edição anterior.

Quanto ao perfil das instituições que responderam, temos mais uma novidade no relatório deste ano: a dimensão de usuários atendidos. Praticamente metade das instituições (56) informou ter entre 10 e 50 mil usuários, seis disseram atender mais de 50 mil usuários e as demais atendem menos de 10 mil usuários.

Embora a RNP produza este relatório com as informações agregadas da pesquisa, as respostas individuais não são disponibilizadas. O nome das instituições respondentes também é resguardado pela RNP.

Para divulgação da pesquisa, assim como em 2021, 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).

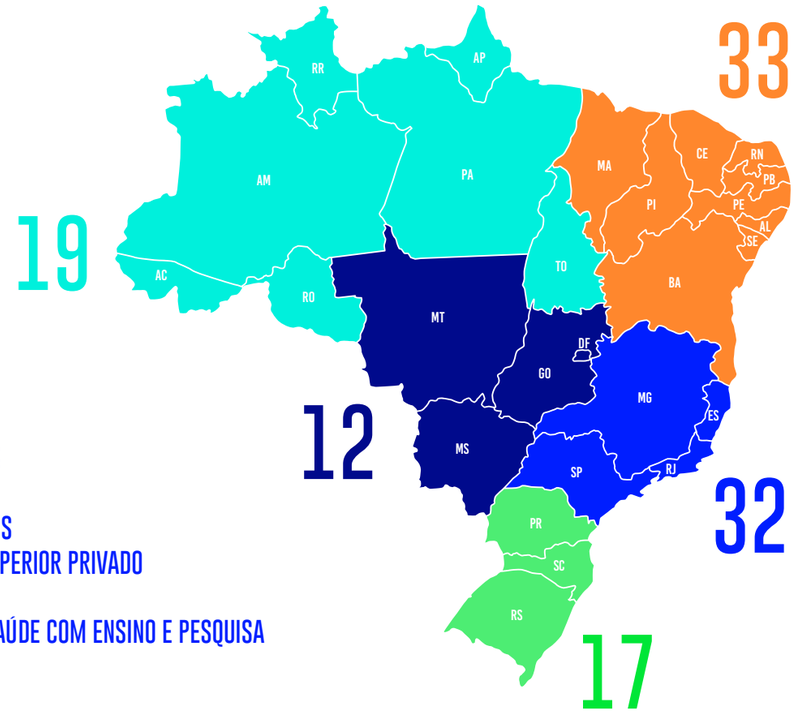
QUESTIONÁRIO

64
PERGUNTAS
EM 4 SEÇÕES:

01 IDENTIFICAÇÃO DA ORGANIZAÇÃO [02]
02 SEGURANÇA DA INFORMAÇÃO [18]
03 PRIVACIDADE E TRANSPARÊNCIA [28]
04 DESENVOLVIMENTO DE COMPETÊNCIAS [16]

RESPONDENTES

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



TIPO DE ORGANIZAÇÃO
37 UNIVERSIDADES FEDERAIS
20 INSTITUTOS FEDERAIS
24 UNIVERSIDADES ESTADUAIS
05 INSTITUTOS DE ENSINO SUPERIOR PRIVADO
19 INSTITUTOS DE PESQUISA
04 ESTABELECIMENTOS DE SAÚDE COM ENSINO E PESQUISA
04 POLO TÉCNOLÓGICO
01 AGÊNCIA DE FOMENTO

SEGURANÇA DA INFORMAÇÃO_

Estão cada vez mais raras as tarefas e processos de trabalho que não contam com algum suporte direto ou indireto das tecnologias de informação e comunicação. Do vendedor autônomo que atende clientes por aplicativos de mensagens às organizações multinacionais que estabelecem ambientes de trabalho remoto, quase sempre é possível encontrar um dispositivo processando e transmitindo informações pelas redes de comunicação digital.

Na prática, os riscos associados a esses dispositivos acabam se alastrando para toda a organização. Em muitos casos, é arriscado supor que falhas e irregularidades na operação da plataforma tecnológica ficarão isoladas à própria infraestrutura de tecnologia da informação.

Dito de outro modo, é importante considerar os possíveis impactos das interrupções, violações e outros incidentes ligados à tecnologia na realização de todas as atividades de uma empresa ou instituição. Embora ainda seja comum que o gestor ou coordenador de tecnologia fique também encarregado das atribuições ligadas à segurança, muitas organizações vêm sentindo as limitações dessa abordagem.

Hoje é possível encontrar nas melhores práticas da área a adoção de modelos de gestão mais robustos, com executivos que respondem diretamente à alta gestão (na figura do CISO, o Chief Information Security Officer) ou comitês com integrantes de diferentes departamentos da instituição formados para o aprimoramento de processos, regras de contratação, aquisição de sistemas, entre outros.

Uma evidência disso consta no relatório “2023 Global Cybersecurity Outlook” do World Economic Forum, o qual revela que 56% dos líderes de segurança hoje se reúnem ao menos uma vez por mês com o conselho administrativo de suas organizações. O relatório explica que essa prática vem contribuindo para que executivos tenham uma percepção de riscos mais alinhada. Em outras palavras, os líderes de segurança compreendem melhor a realidade da organização, e os líderes da organização compreendem melhor os riscos a que ela está exposta.

Além dessas tendências gerais, há também desafios que aparecem mais em determinados setores. As instituições integrantes do Sistema RNP são em maioria instituições de ensino superior e pesquisa, mas há também as instituições de saúde responsáveis pelos hospitais vinculados às universidades – uma área que tem o desafio constante de incorporar as inovações do setor sem que haja prejuízo para a segurança dos pacientes.

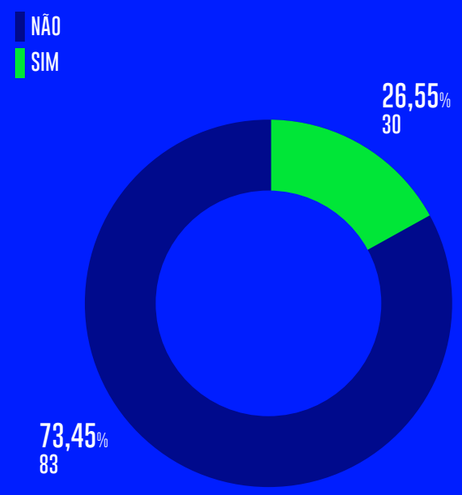
Com 18 perguntas em 2022, a seção do questionário referente à segurança da informação buscou levantar dados relevantes para uma visão geral sobre a abordagem de cada instituição neste tema. Sendo assim, as perguntas tratam da forma como a instituição lida com a gestão da segurança da informação, quais processos foram estabelecidos e se há uma equipe dedicada para o tratamento de incidentes.

WEF GLOBAL CYBERSECURITY OUTLOOK 2023 ACESSE O RELATÓRIO AQUI

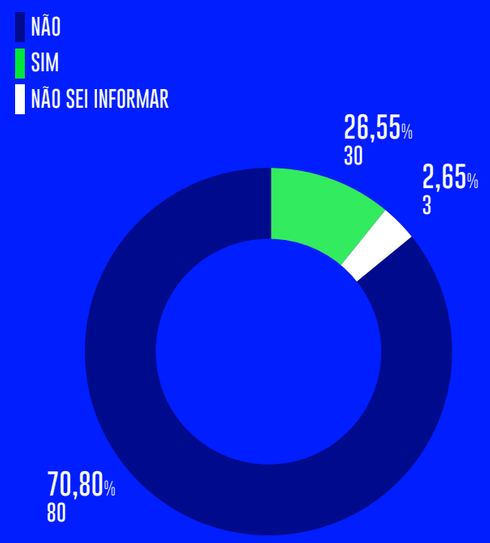
Como a prática da segurança da informação deve buscar um alinhamento com as atividades da instituição, priorizando tarefas conforme uma visão de riscos organizacionais, é fundamental que as ações sejam previstas, orçadas e planejadas. Em 2022, 26,5% das instituições disseram que possuem um planejamento anual e formal para a área.

Quando o tema abordado é o orçamento, novamente 26,5% das instituições informaram que possuem um orçamento dedicado à segurança. Contudo, é importante esclarecer que não são as mesmas 26,5% que responderam “Sim” à questão sobre o planejamento. Desse modo, algumas instituições possuem orçamento e outras possuem um plano formal, mas apenas 14,1% possuem ambos.

Sua organização possui planejamento formal anual em segurança?

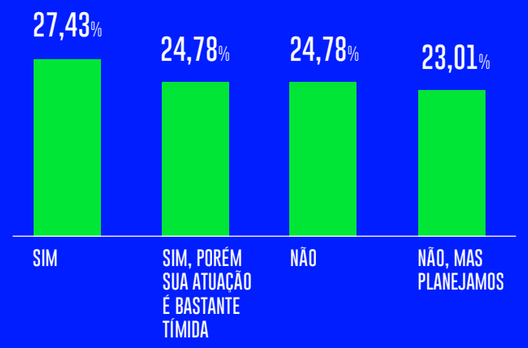


A sua organização possui destinação orçamentária interna para assuntos de segurança da informação?



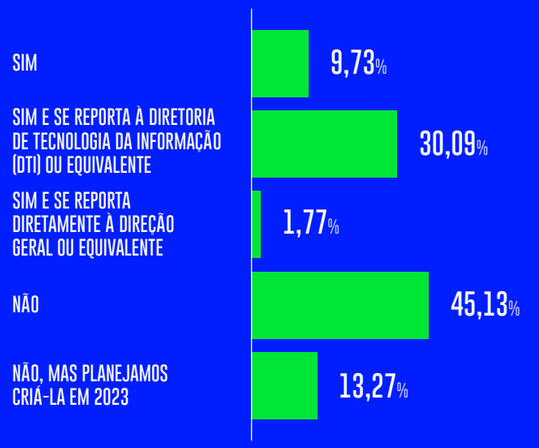
Em termos de mecanismos e hierarquia na gestão de segurança das instituições, praticamente metade (47,7%) não possui um comitê multidisciplinar estabelecido. Entre aquelas que o possuem, o comitê ainda tem atuação tímida em metade dos casos. Idealmente, esse comitê deve assessorar a alta gestão e fornecer uma visão ampla dos riscos ligados à segurança da informação – não apenas na área de TI, mas em todos os processos e atividades desempenhados.

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



Uma das novas perguntas desta edição da pesquisa revela que quase metade dos participantes (45%) também não possui uma coordenação específica para a segurança da informação e, mesmo naquelas que possuem essa coordenação, ela costuma estar subordinada ao departamento de TI, o que pode limitar o escopo das ações e a visão da segurança como parte de toda a organização. Apenas 2 instituições (1,7%) relataram a existência de uma coordenação subordinada diretamente à diretoria-geral.

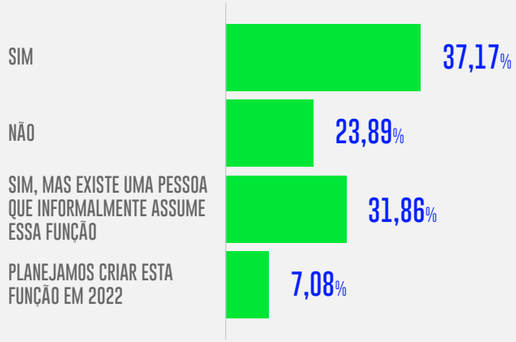
Existe uma área ou coordenação específica de Segurança da Informação formalmente estabelecida?



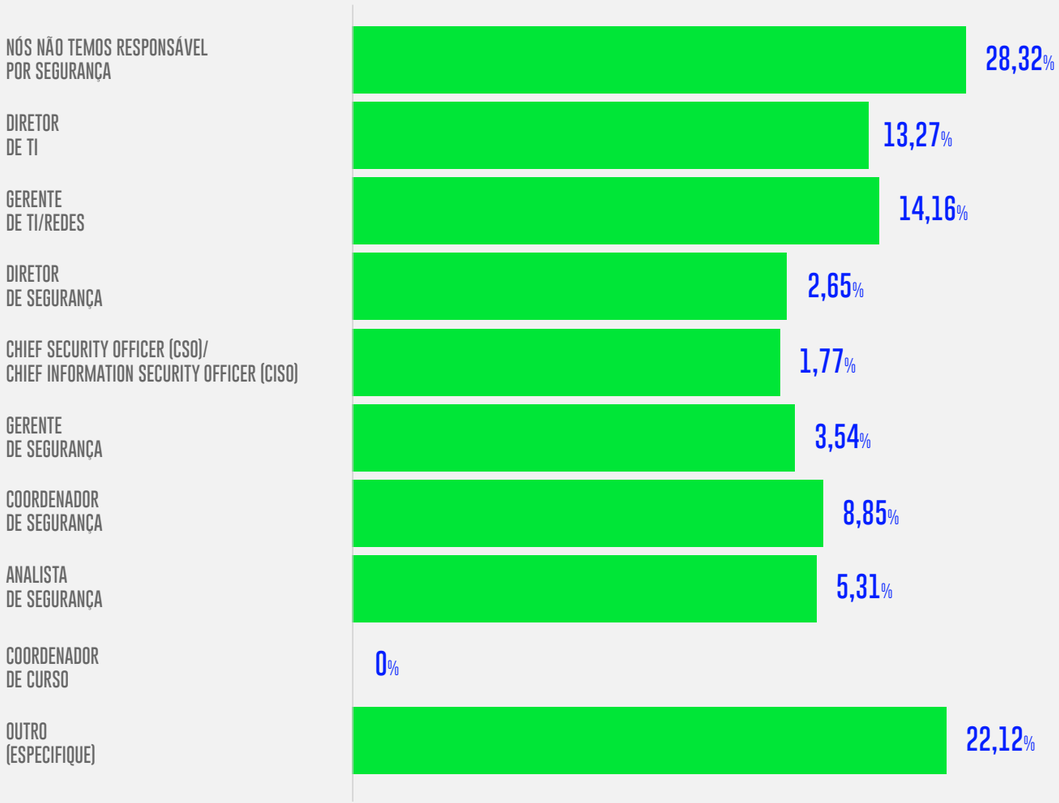
De fato, 62,7% das instituições disseram não ter um gestor de segurança indicado diretamente pela alta gestão, o que resulta em uma certa variação no tipo de colaborador que assume as responsabilidades por esta área – embora o responsável seja da equipe de TI em muitos casos. Alguns respondentes especificaram o responsável como sendo analista de suporte ou técnico de TI, possivelmente sem poderes de tomada de decisão.

Embora tenham sido observadas mudanças de ano para ano nestes números, a variação não tem sido significativa.

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



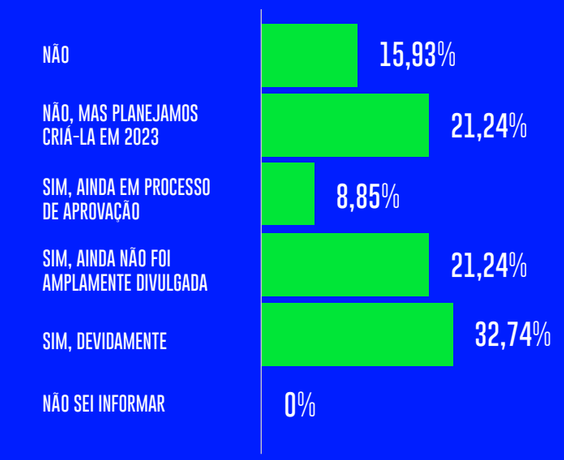
Caso exista esta figura, qual cargo que ele ocupa?



Após serem abordados aspectos da estrutura organizacional, foram sondados os elementos da segurança da informação que cada instituição coloca em prática. O alicerce costuma ser a Política de Segurança da Informação (PSI), um documento contendo as diretrizes gerais sobre o entendimento e os objetivos da aplicação da segurança para toda a organização. Assim como nos anteriores, mais da metade das instituições já possui uma política, mas muitas carecem de divulgação adequada.

Como a política de segurança trata do tema na esfera institucional e estratégica, ela deve se aplicar a todos os colaboradores e outros interessados (incluindo fornecedores e alunos, no caso de instituições de ensino). Embora seja possível que todos tenham conhecimento de ações específicas de segurança (como os requisitos mínimos para criar uma senha), a divulgação da política integra-se aos esforços de conscientização em segurança para aprimorar a sensibilidade acerca do tema.

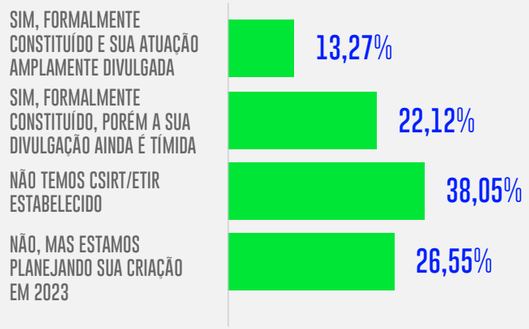
Sua organização possui uma Política de Segurança da Informação (PSI/POSIC) devidamente aprovada pela alta gestão e divulgada a todos (professores, alunos, funcionários técnico-administrativos), além de parceiros e fornecedores?



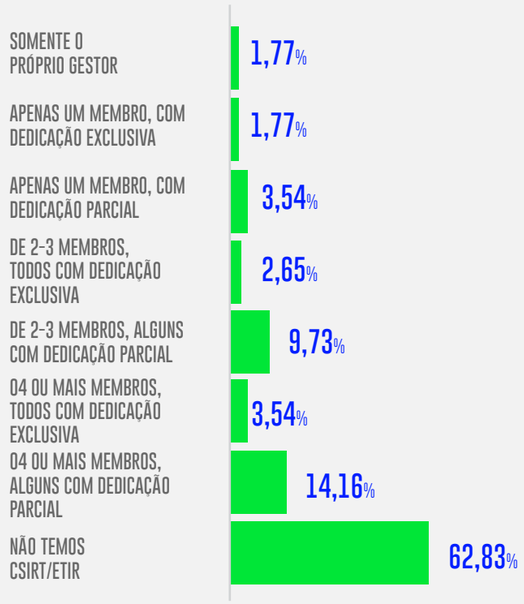
Outro elemento importante é a existência da equipe de resposta a incidentes (CSIRT, na sigla em inglês, ou ETIR, em português, para “equipe de tratamento de incidentes em redes”). Nos processos de segurança da informação, a “resposta” (ou “reação”) é tão relevante quanto a prevenção, pois tende a diminuir o tempo necessário para recuperar sistemas e retomar as atividades em casos de violações, além de munir a instituição dos recursos necessários para cumprir obrigações legais e oferecer uma resposta à sociedade em caso de violações ou uso indevido de sua infraestrutura tecnológica.

Assim como nas edições anteriores da pesquisa, a maior parte das instituições não dispõem de uma equipe especializada para essa tarefa, o que significa que a resposta a incidentes tende a ser feita de maneira informal pela equipe de TI. Felizmente, quando essa equipe existe, 80% das instituições informaram que ela conta com mais de 2 membros, muitas vezes com dedicação exclusiva.

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?



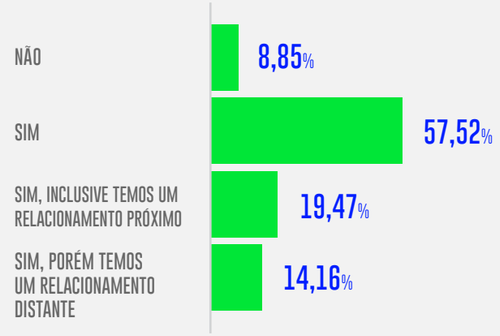
Se a resposta for positiva para a pergunta anterior, quantos membros compõem o CSIRT/ETIR?



A RNP estabeleceu um dos primeiros CSIRTs do Brasil, o Centro de Atendimento a Incidentes de Segurança (CAIS). Em 2022, o CAIS completou seu aniversário de 25 anos, atuando como CSIRT de coordenação de toda a rede acadêmica.

O resultado dessa história e deste trabalho aparece na pesquisa, em que 91% das instituições informaram conhecer o CAIS, muitas delas indicando ter inclusive um relacionamento próximo com a equipe da RNP. Em outras palavras, mesmo instituições que não possuem seu próprio CSIRT afirmam conhecer o CAIS.

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



CAIS_

CENTRO
DE ATENDIMENTO
A INCIDENTES
DE SEGURANÇA

O CAIS/RNP atua como CSIRT de coordenação da rede acadêmica brasileira.

25
ANOS DO CAIS

CONHEÇA
NOSSA HISTÓRIA

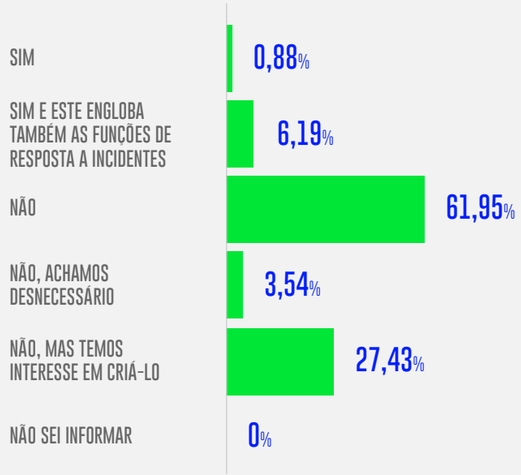
APOIANDO
DIVERSOS CSIRTS ACADÊMICOS

CONFIRA
A LISTA

As instituições também foram indagadas se possuem um Security Operations Center (SOC – Centro de Operações de Segurança). É a primeira vez que esta pergunta aparece na pesquisa, pois havia um entendimento de que apenas grandes provedores necessitavam de uma central dedicada à segurança da informação no mesmo molde das redes (que são monitoradas pelo NOC – Network Operations Center). De fato, 3,5% das instituições acham a criação do SOC desnecessário.

Hoje, contudo, o SOC é visto como um benefício para organizações de médio e grande porte de qualquer setor. Na pesquisa, cerca de 7% relataram possuir um SOC, e 27% têm interesse em cria-lo. Em quase todos os casos em que ele existe, o SOC está integrado com a resposta a incidentes.

Sua organização possui um centro de operações de segurança (SOC - Security Operation Center)?



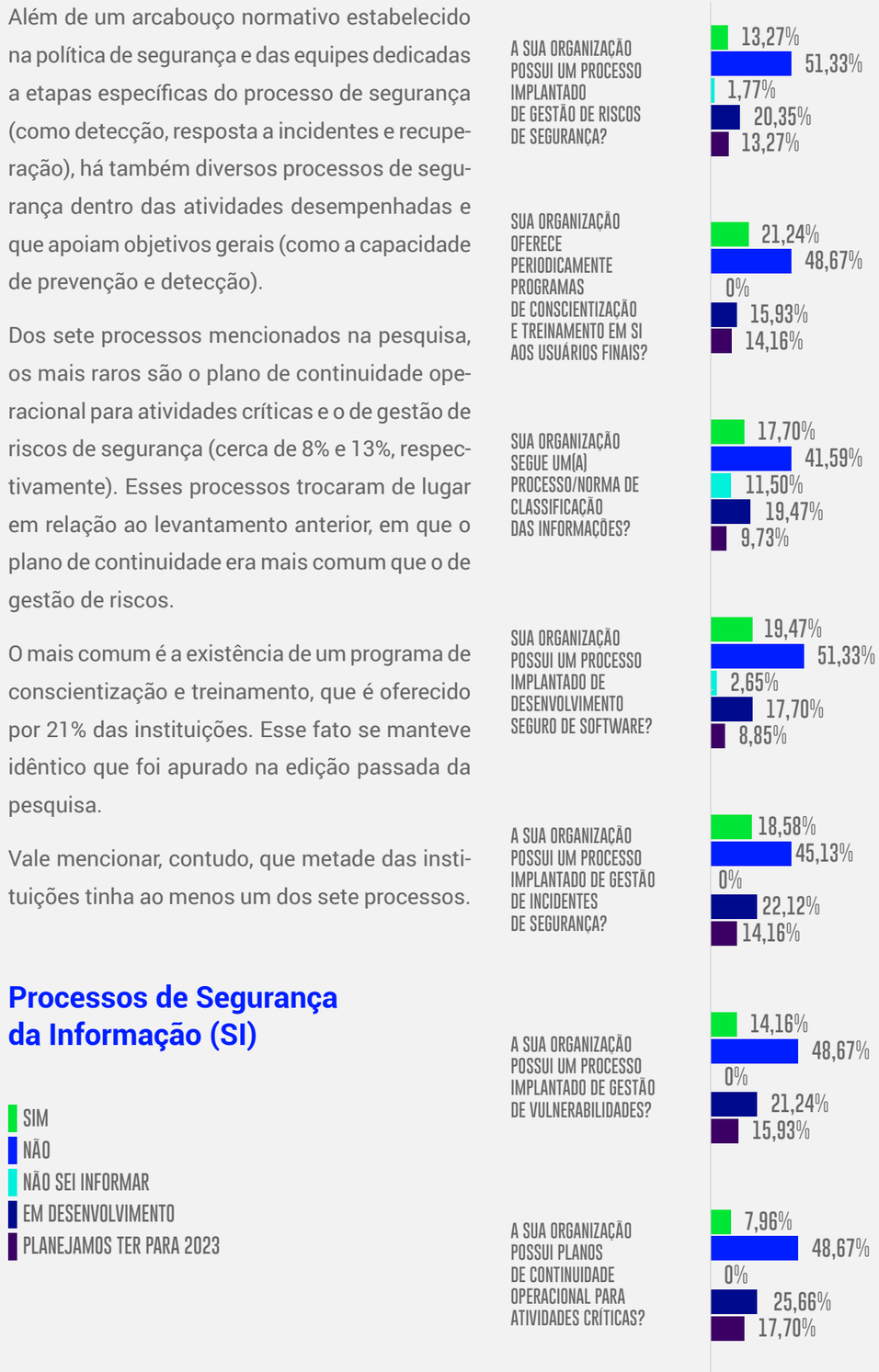
Além de um arcabouço normativo estabelecido na política de segurança e das equipes dedicadas a etapas específicas do processo de segurança (como detecção, resposta a incidentes e recuperação), há também diversos processos de segurança dentro das atividades desempenhadas e que apoiam objetivos gerais (como a capacidade de prevenção e detecção).

Dos sete processos mencionados na pesquisa, os mais raros são o plano de continuidade operacional para atividades críticas e o de gestão de riscos de segurança (cerca de 8% e 13%, respectivamente). Esses processos trocaram de lugar em relação ao levantamento anterior, em que o plano de continuidade era mais comum que o de gestão de riscos.

O mais comum é a existência de um programa de conscientização e treinamento, que é oferecido por 21% das instituições. Esse fato se manteve idêntico que foi apurado na edição passada da pesquisa.

Vale mencionar, contudo, que metade das instituições tinha ao menos um dos sete processos.

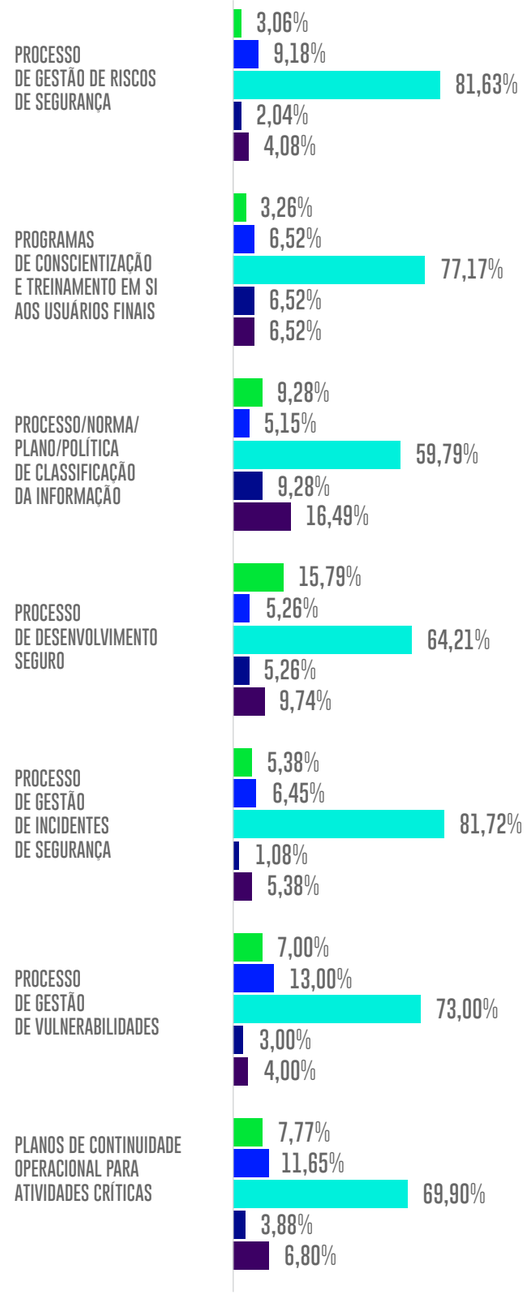
Processos de Segurança da Informação (SI)



Assim como a pesquisa já havia apontado em anos anteriores, o maior impedimento citado pelas instituições para a criação desses processos é a falta de recursos humanos. Cabe observar que esses recursos humanos nem sempre estariam apenas na equipe de segurança, pois alguns processos (como a classificação de informação e a gestão de riscos) impactam equipes administrativas ou até departamentos diversos.

De fato, estudos apontam uma falta de profissionais de segurança no mercado. O um gap mundial chega a 3,4 milhões de profissionais, de acordo com o estudo de Cybersecurity Workforce da (ISC)². No Brasil, o mesmo estudo aponta que a força de trabalho do setor cresceu 18,3% em 2022. Embora essas contratações tenham diminuído o gap, ele ainda é 312 mil profissionais no país.

Se alguma das suas respostas no gráfico anterior foi diferente de SIM, indique quais as principais dificuldades enfrentadas para não ter implantado cada um desses processos

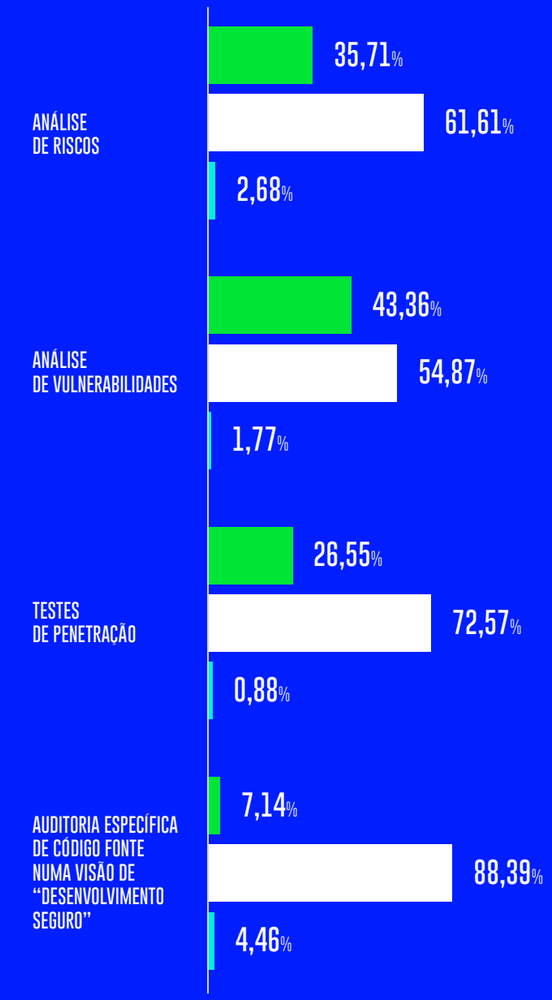


- NÃO SEI INFORMAR/NÃO SE APLICA
- NÃO É PRIORIDADE PARA A ORGANIZAÇÃO
- FALTA DE RECURSOS HUMANOS
- FALTA DE RECURSOS FINANCEIROS
- FALTA DE CONHECIMENTO TÉCNICO

Outro processo importante para a segurança da informação é a realização periódica de análises e testes de segurança. É a primeira vez que apuramos este número, e foi verificado que, embora análise de vulnerabilidades seja o teste mais comum, nenhum deles é realizado por mais da metade das instituições.

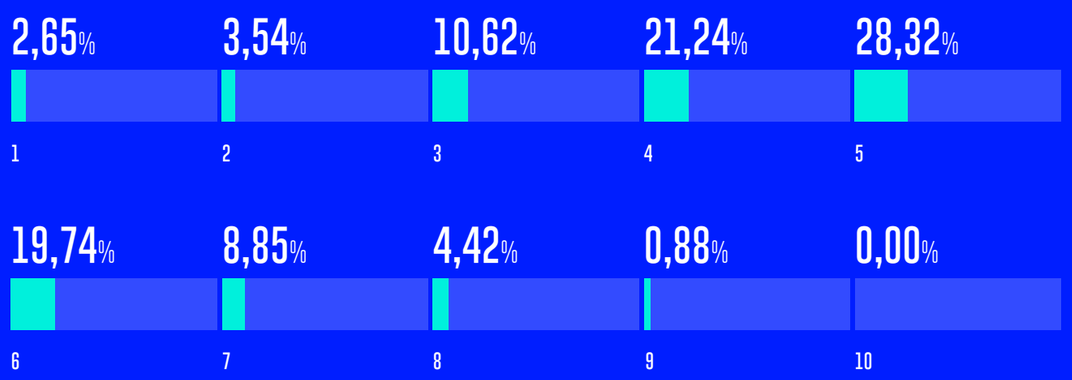
A sua instituição realiza análises ou testes de forma regular (minimamente, uma vez por ano)?

- SIM
- NÃO
- NÃO SEI INFORMAR



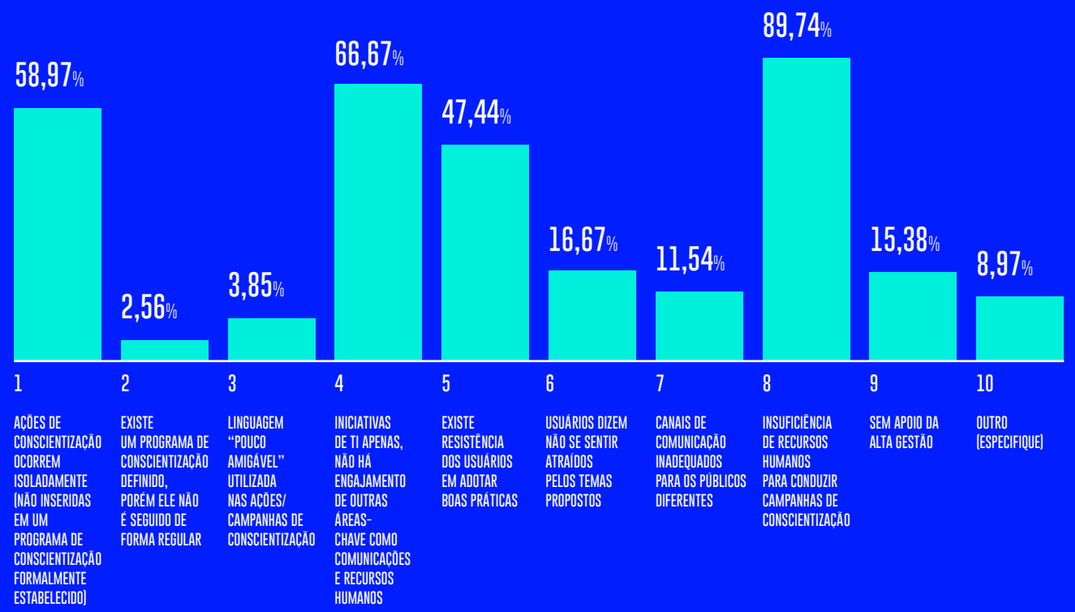
Em termos de maturidade da organização como um todo diante do tema de segurança da informação, os respondentes deram uma nota média de 4,9 em 2022, levemente acima da média de 4,6 de 2021. O aumento é possível com mais avaliações de maturidade na faixa entre 4 e 6. Cabe especificar que esta pergunta está ligada aos esforços de conscientização dos usuários, introduzindo hábitos seguros no dia a dia dos colaboradores e nas práticas e processos de trabalho.

Em uma escala de 1 a 10 (sendo 10 a maior), como você avalia a maturidade da cultura de segurança em sua organização (o quanto os temas de segurança estão presentes no dia a dia dos colaboradores)?



Em mais uma pergunta nova desta edição, os respondentes indicaram as possíveis causas (inclusive mais de uma) para maturidades com nota 5 ou inferior. Novamente, o principal fator apontado é a escassez de recursos humanos para conduzir um programa de conscientização (quase 90% selecionaram esta alternativa como uma das causas), mas a falta de engajamento das áreas de comunicação e recursos humanos também foi um fator bastante mencionado (66%).

Caso você tenha dado uma nota menor ou igual a 5, por favor indique as possíveis causas disso:



2022 (ISC)² CYBERSECURITY WORKFORCE

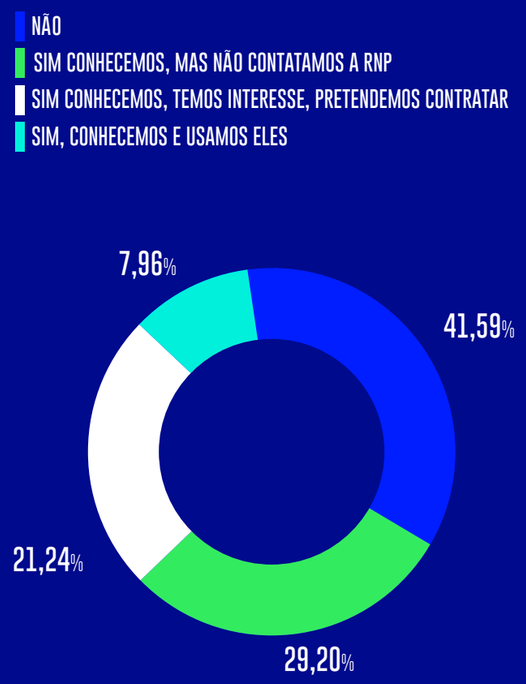
ACESSE O ESTUDO AQUI

Os avanços na área de segurança da informação dependem de um processo de melhoria contínua sustentado em iniciativas que já demonstraram resultados positivos em outras organizações que compartilham características como tamanho e área de atuação. Em alguns casos, especialmente quando se trata da conscientização sobre o tema, até a formação cultural dos colaboradores pode influenciar a estratégia.

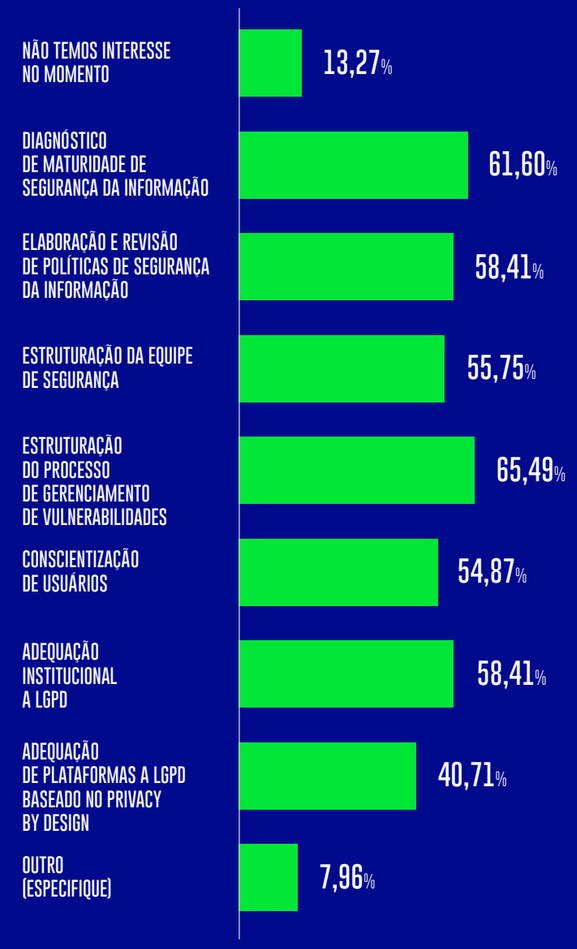
É por isso que a RNP apoia as organizações integrantes do Sistema RNP oferecendo serviços consultivos na área de segurança da informação, ajudando as instituições a superar os desafios da área com embasamento em experiências de sucesso. Contudo, 41% dos respondentes disseram não ter conhecimento dos serviços oferecidos.

Por outro lado, a maioria dos respondentes se interessou por alguns dos serviços oferecidos, principalmente a Estruturação do Processo de Gerenciamento de Vulnerabilidades e o Diagnóstico de Maturidade de Segurança da Informação.

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



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



PRIVACIDADE E TRANSPARÊNCIA_

A segurança da informação e a privacidade são assuntos coligados no mundo digital. É inclusive pertinente observar que as preocupações com privacidade foram a grande força motriz de regulamentações que impactaram as práticas de segurança em diversas organizações. Mesmo quando não existem exigências de segurança da informação em si, os requisitos de privacidade impõem obrigações que só serão cumpridas mediante ações de segurança de segurança.

A Lei Geral de Proteção de Dados (LGPD) no Brasil e o Regulamento Geral de Proteção e Dados (GDPR) são dois exemplos significativos desse movimento. Embora os Estados Unidos ainda não tenham aprovado uma lei federal sobre o tema, ele está amplamente coberto por leis estaduais que obrigam empresas e entidades governamentais a tratar dados pessoais de forma segura e a notificar os titulares em caso de vazamentos – exatamente como a lei brasileira e a europeia.

Em diversas situações, contudo, as leis de privacidade impactam também os processos de trabalho, limitando quais dados podem ser acessados e impondo restrições e requisitos que exigem uma nova forma de pensar a respeito dos dados, reformulando as atividades da organização em conformidade com as regras estabelecidas.

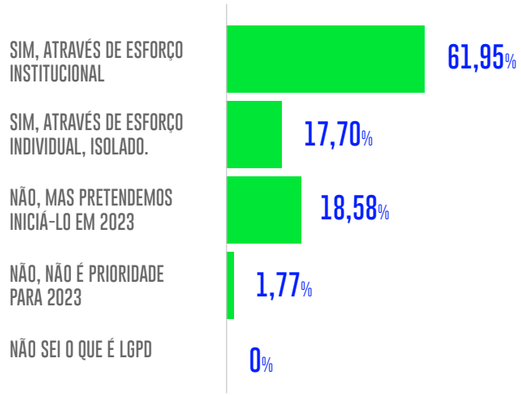
Além de aperfeiçoamentos tecnológicos, a proteção adequada dos dados e dos direitos dos titulares costuma exigir também controles de governança – outro assunto inseparável da segurança da informação. As mudanças culturais, por outro lado, exigem programas de conscientização para que os colaboradores compreendam a nova realidade e porque nem tudo que antes era permitido ainda pode ser feito da mesma forma.

A seção sobre privacidade e transparência é a maior do questionário, com 28 perguntas. Praticamente todas, porém, tratam de pontos associados à legislação brasileira ou de etapas do processo de adequação à LGPD.

A SEGURANÇA DA INFORMAÇÃO E A PRIVACIDADE SÃO ASSUNTOS COLIGADOS NO MUNDO DIGITAL.

A pesquisa apontou que a maioria das instituições já começou o processo de adequação à LGPD, em geral com apoio institucional para o tema. Contudo, cerca de 20% dos participantes disseram que o processo não foi iniciado, alguns inclusive informando que o tema não é prioridade nem para 2023.

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

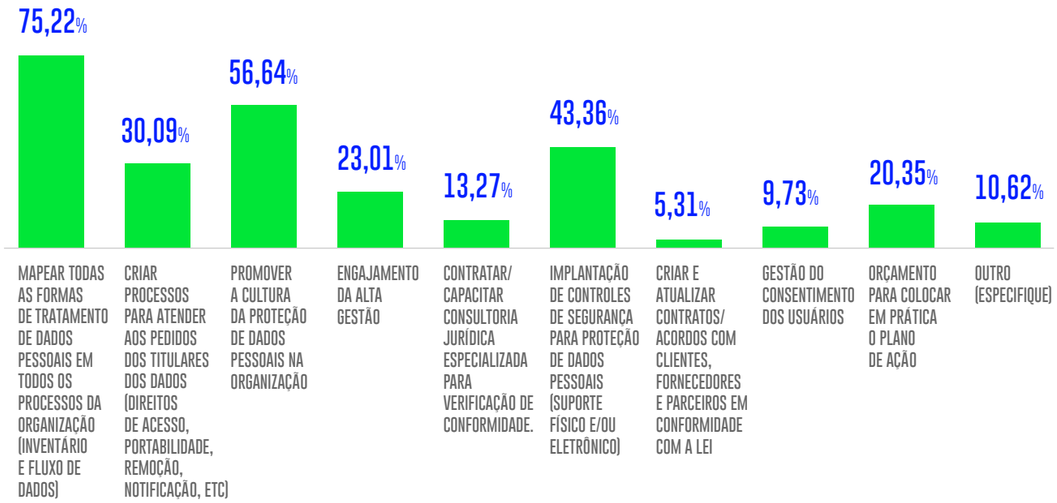


O levantamento mostra, porém, que há uma proporção maior de organizações em estágios avançados da LGPD, como a governança e a melhoria contínua. De fato, além de termos três vezes mais instituições no estágio de governança, é a primeira vez que a pesquisa registra respostas no estágio de melhoria contínua.

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

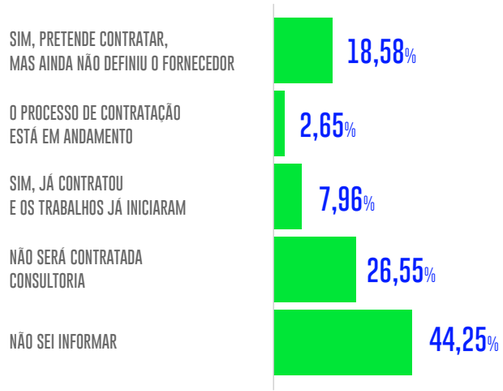
Os participantes da pesquisa foram convidados a elencar os três principais desafios da conformidade com a LGPD em suas instituições. As respostas mostram que há problemas bastante práticos: as três dificuldades mais comuns foram o mapeamento dos processos de tratamento e fluxos, a promoção de uma cultura que sustente a proteção de dados pessoais e a implantação de controles de segurança.

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



Apesar dessas dificuldades, muitos respondentes (44%) disseram não saber informar se suas instituições contrataram alguma consultoria externa para contribuir com a adequação à LGPD, enquanto 26,5% afirmaram que não haverá qualquer contratação para essa finalidade. Apenas 29% dos respondentes disseram que um fornecedor foi contratado ou que uma contratação está em andamento.

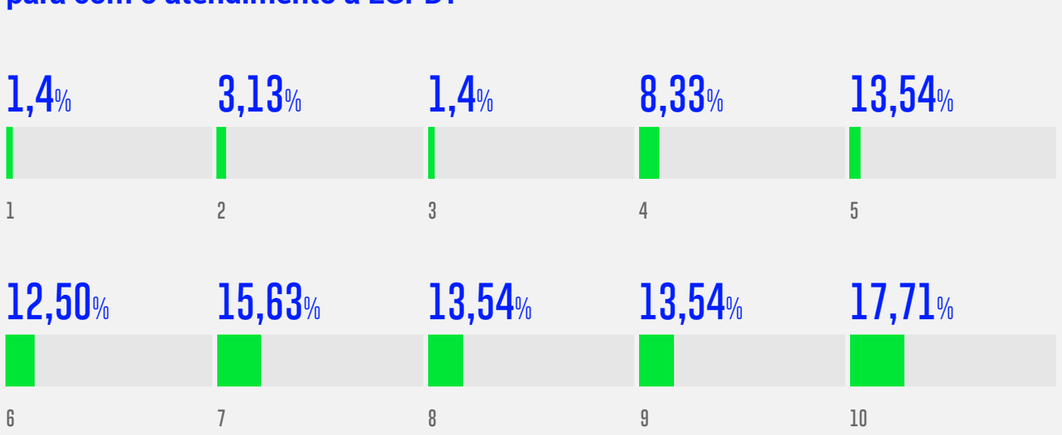
Sua organização contratou ou pretende contratar uma consultoria para contribuir com a adequação à LGPD?



PRINCIPAIS FATORES NO PROCESSO DE ADEQUAÇÃO

Os respondentes também foram convidados a avaliar o comprometimento da alta gestão com esse processo de adequação. Cerca de 20% decidiram não responder, mas a média das notas permanece estável desde a pesquisa de 2020 em cerca de 7 pontos em uma escala de 1 a 10.

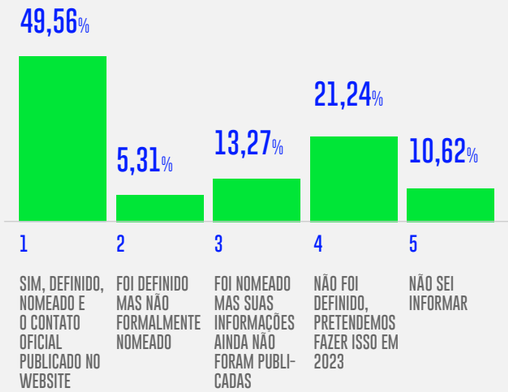
Em uma escala de 1 a 10 (sendo 10 a maior), como você avalia o comprometimento da alta gestão para com o atendimento à LGPD?



Em 2022, foi observado um aumento de 65% nas instituições que disseram que ainda não definiram o encarregado de proteção de dados (ou "DPO", da sigla em inglês para Data Protection Officer). Esse tipo de variação pode ser atribuído a uma mudança no perfil das instituições sondadas pela pesquisa e não indica que houve um retrocesso no Sistema RNP – os dados devem ser analisados em conjunto e, como vimos, há mais organizações em estágios avançados de conformidade do que em anos anteriores

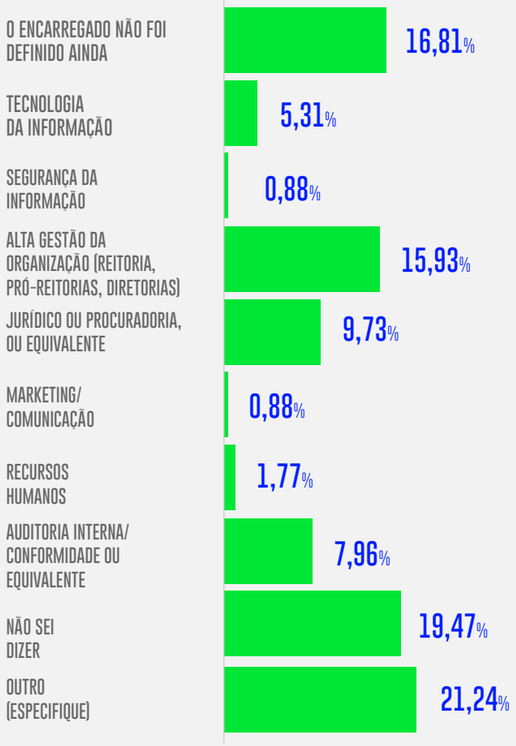
Seja como for, é evidente que muitas instituições ainda precisam definir seus encarregados ou divulgá-los, pois trata-se de uma exigência da LGPD.

O Encarregado de Proteção de Dados (DPO) foi definido, nomeado e as informações de contato divulgadas no website da organização?



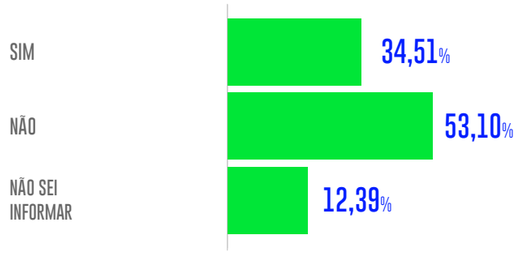
Se já tiver sido definido, qual a área de atuação do(a) Encarregado (a)?

Nas instituições em que o encarregado já foi indicado, o mais comum é que ele seja integrante da alta gestão, da ouvidoria, do jurídico ou da auditoria interna da organização Embora não estivesse nas opções originais, a "ouvidoria" foi especificada por 12,4% do total de respondentes por meio da opção "outro".



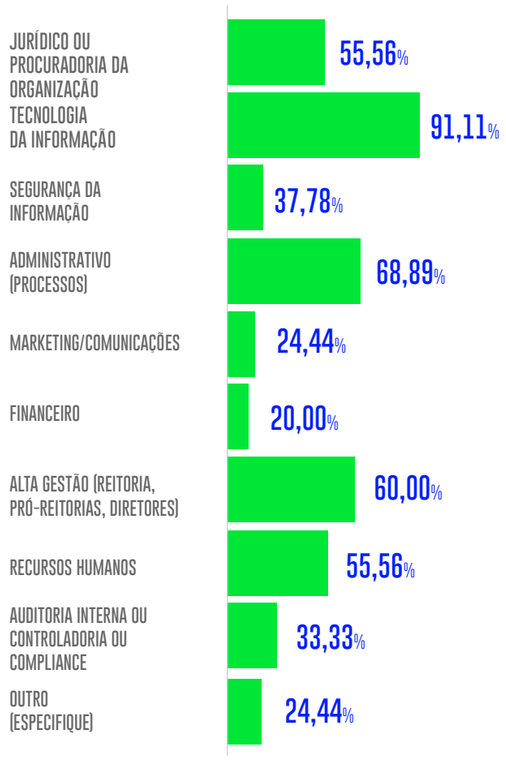
A formação de comitês multidisciplinares para a proteção de dados tende a contribuir com as organizações ao avaliar as políticas de tratamento de dados a partir de ângulos diversos. A maioria das instituições (53%) não dispõe deste comitê, mas ele é empregado por 34% dos respondentes. A variação nestes números foi de apenas um ponto percentual na comparação com 2021.

Sua organização tem Comitê Multidisciplinar de Proteção de Dados Pessoais?



Quanto aos integrantes destes comitês nas instituições participantes da pesquisa que o possuem, eles são em geral compostos de colaboradores das equipes de tecnologia, do jurídico e do administrativo, inclusive da alta gestão.

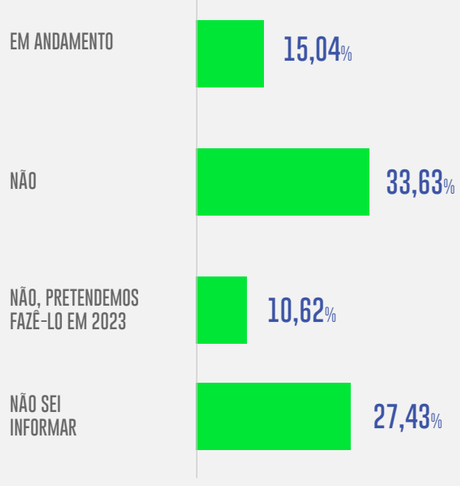
Se o comitê multidisciplinar tiver sido constituído, indique de quais áreas são os seus membros (indique todas as áreas, se possível). Caso o comitê não exista, deixe em branco.



DIAGNÓSTICO E MAPEAMENTO DE DADOS E RISCOS

Quanto ao diagnóstico geral (assessment), uma etapa inicial que avalia o cenário interno da organização, 13,27% das instituições disseram que ele já foi concluído, mas 27,4% dos respondentes não sabiam informar em que estágio ele se encontrava. Em relação ao ano anterior, registrou-se um aumento no número de diagnósticos concluídos, mas o número geral de diagnósticos continua praticamente o mesmo, tendo em vista que a queda foi compensada por uma diminuição no número de diagnósticos “em andamento”.

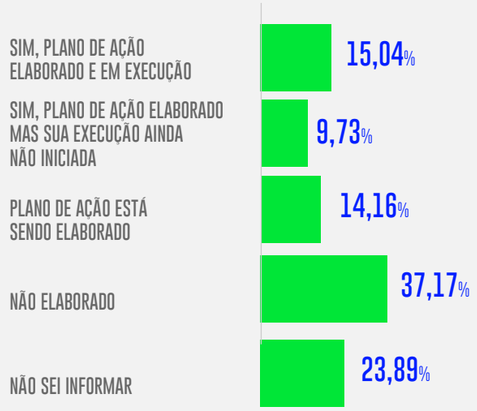
Sua organização fez um Diagnóstico (Assessment) para entendimento do cenário interno para direcionar a adequação?



Finalizada a etapa de diagnóstico, cabe elaborar um Plano de Ação que descreva o escopo e as etapas de adequação com a lei, já levando em conta a situação concreta que foi encontrada.

Embora 41% dos participantes tenham informado que este plano estava em execução ou em elaboração, essa proporção é menor que a do ano passado (49,13%).

Sua organização elaborou um Plano de Ação para adequação?



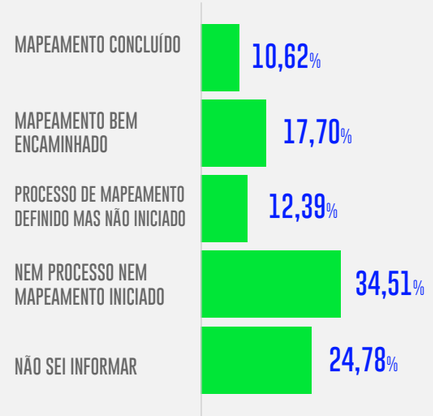
Assim como em uma análise de risco em segurança da informação, a proteção de dados exige um mapeamento adequado do cenário da organização sobre o tema. Antes de saber como dados serão protegidos e de que forma eles poderão ser usados durante as atividades (com qual autorização ou finalidade, por exemplo), é preciso saber qual é a natureza e a origem desses dados e quem são seus titulares.

Nem todas as informações são consideradas "dados pessoais", e a algumas atividades podem apresentar mais risco do que outras, por exemplo. É o processo de adequação e conformidade que vai orientar o que fazer em cada caso, mas isso só será possível se cada um desses contextos for mapeado da forma correta.

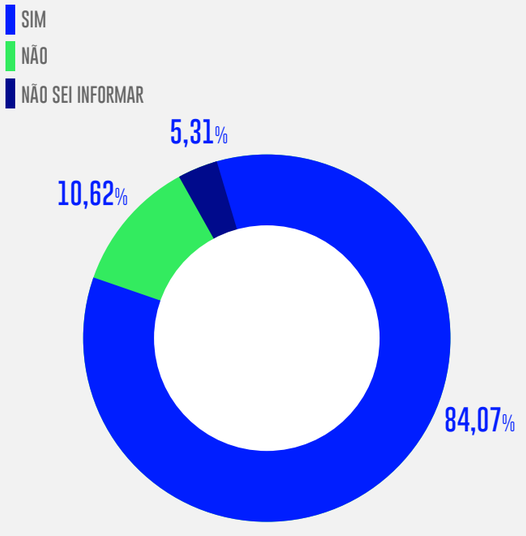
Nesse sentido, é importante que a organização realize um mapeamento dos fluxos se dados, identificando também aqueles que podem estar sujeitos a regras específicas (como dados pessoais sensíveis e os de crianças e adolescentes).

Já quanto ao mapeamento específico de fluxo de dados, um em cada quatro participantes da pesquisa também disse não saber informar se um mapeamento existia ou em qual etapa ele estava; 17,7% disseram que o mapeamento estava bem-encaminhado 10,6% informaram que ele já tinha sido concluído. Em 12,4% das instituições o mapeamento tinha sido estruturado, mas ainda estava para começar.

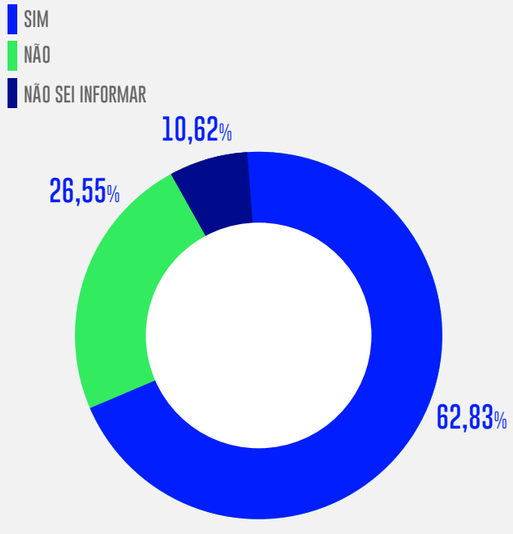
Em relação ao processo de mapeamento dos fluxos de dados pessoais, em que fase sua organização se encontra?



Sua organização trata/manipula dados pessoais sensíveis?

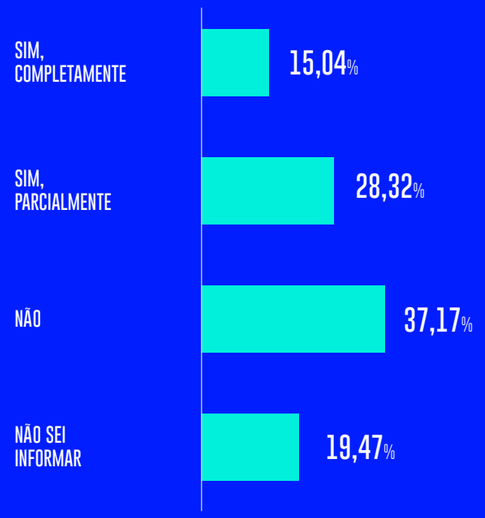


Sua organização trata/manipula dados pessoais de crianças e/ou adolescentes?



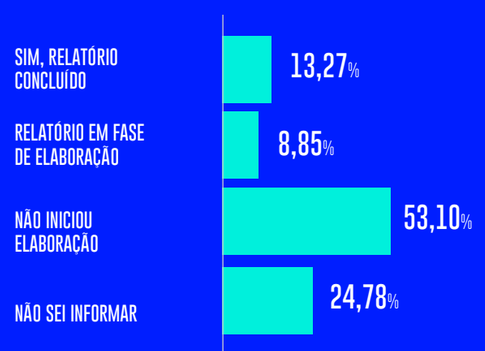
Seguindo nessa linha, após identificar os tipos de dados tratados e seu fluxo, há a necessidade de apontar os “operadores” dos dados. Dito de forma simples, o operador é quem de fato faz o tratamento da informação em nome do “controlador” (que normalmente é a própria instituição à qual titular cedeu seus dados). Houve um crescimento no número de instituições que mapearam completamente seus operadores – de 8,77% para 15,04%. Observa-se que esse aumento parece decorrer da conclusão dos mapeamentos que já tinham sido iniciados, tendo em vista que a proporção de instituições que não iniciaram o mapeamento continuou semelhante.

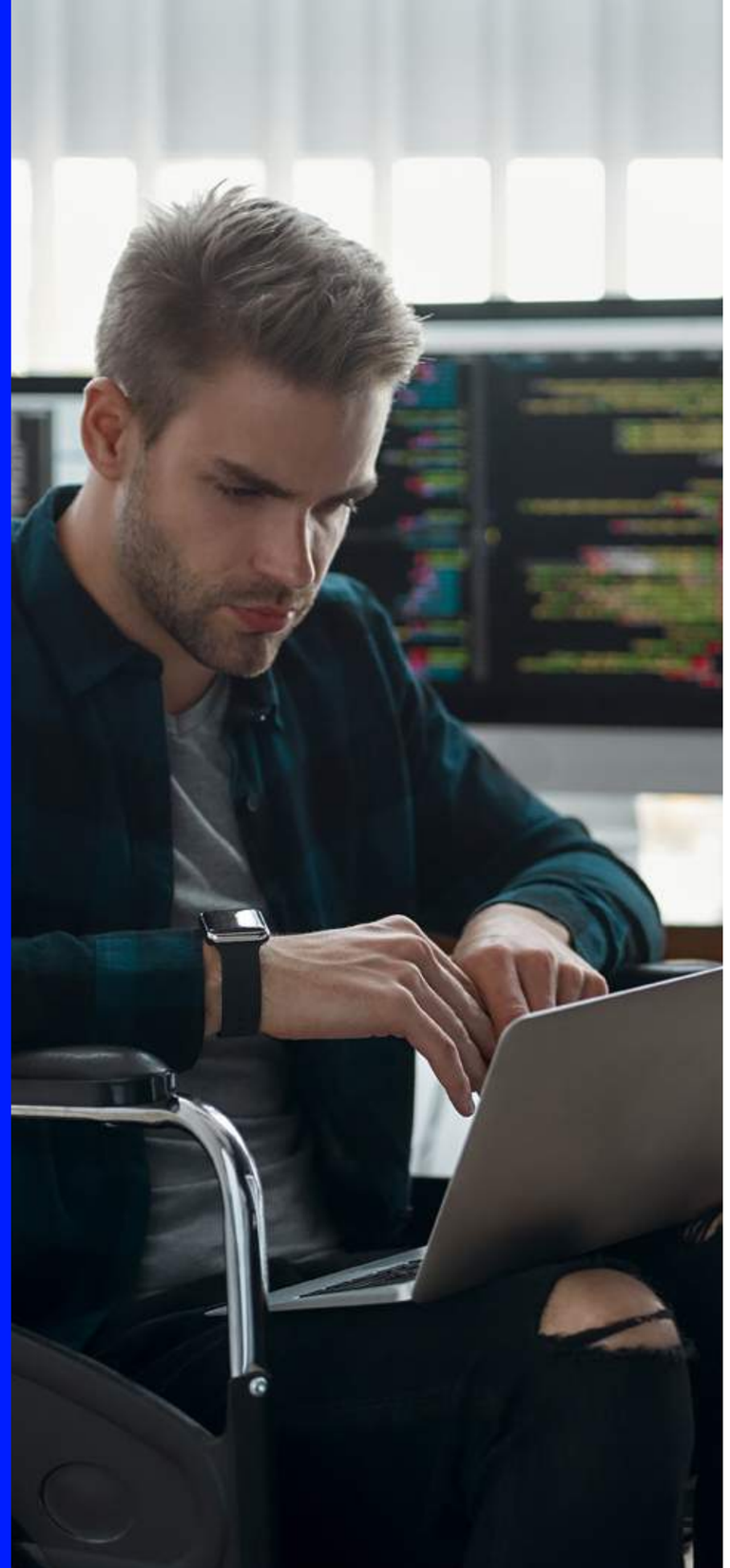
Sua organização mapeou quem são os chamados “operadores” de dados pessoais?



O Relatório de Impacto à Proteção de Dados Pessoais, por sua vez, tende a representar um estágio mais avançado na conformidade com a legislação. Trata-se de um documento obrigatório em contextos que representem alto risco à garantia dos princípios gerais de proteção de dados pessoais, inclusive aqueles em que há tratamento de dados sensíveis. Este documento foi elaborado ou está em elaboração em 22,12% das instituições, número consideravelmente inferior (84,07%) ao de instituições que reconhecem tratar de dados sensíveis.

Sua organização já elaborou o Relatório de Impacto à Proteção de Dados pessoais (RIPD)?





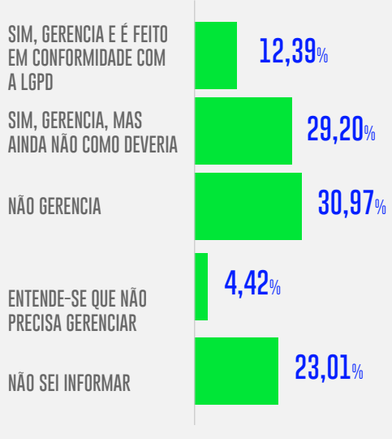
ATENDIMENTO AOS TITULARES

Um dos pilares da LGPD é a proteção dos direitos dos titulares de dados. A lei estabelece que as organizações devem sempre permitir que o titular mantenha o controle seus dados, saiba como são usados e possa fornecer (ou negar) seu consentimento quanto ao uso das informações.

O cumprimento dessas regras passa pela criação de processos e mecanismos que possam receber as solicitações dos titulares e tratá-las de forma adequada. Também é preciso que haja um sistema que faça a gestão do consentimento para o uso de dados ou vincule certas informações à finalidade para a qual foram eles foram coletados.

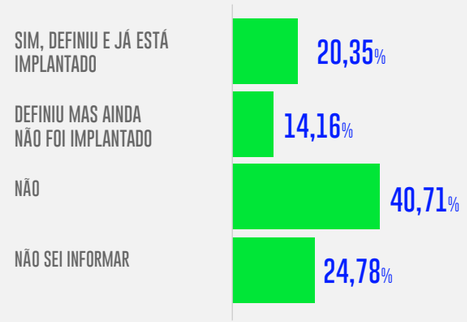
A pesquisa apurou um avanço nessa área: 12,4% das instituições fazem a gestão do consentimento em conformidade com a LGPD – um percentual bem maior que a das edições anteriores, quando este número ficava abaixo dos 2%. A proporção de instituições que fazem uma gestão parcial ficou estável, mas o número de instituições que afirmaram não fazer a gestão do consentimento caiu de 50,88% para 30,97%.

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



Quanto à existência de canais de contato para receber as solicitações dos titulares, 41,59% das instituições informaram que esse canal já existe. Porém, apenas 20,35% das organizações sondadas já possui um processo formalizado para atender às demandas.

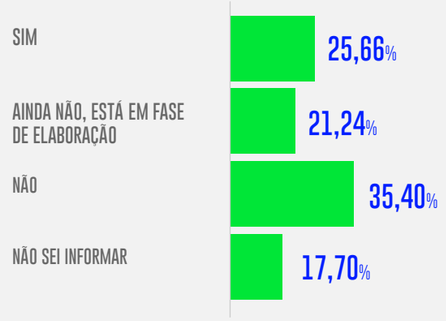
Sua organização já definiu e implantou um processo para responder a solicitações dos titulares dos dados pessoais?



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

Os titulares são informados sobre seus direitos e sobre as regras que a organização segue no tratamento de dados por meio de um documento de acesso externo chamado Aviso de Privacidade. Um em cada quatro respondentes disseram que esse documento já existe em suas instituições, observando-se uma melhora em relação ao número de 2021 (14,04%).

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



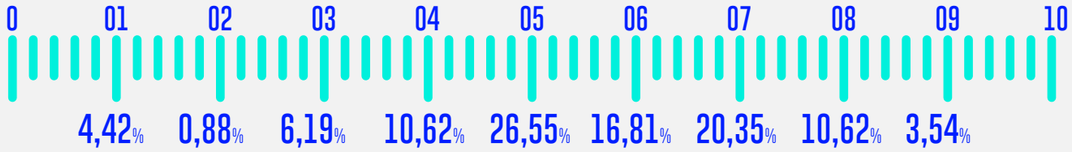
INCIDENTES, CULTURA E CONTROLES DE SEGURANÇA

A conformidade com a LGPD dentro da uma organização é apoiada por controles de segurança, por uma cultura de proteção de dados e pela capacidade de resposta a incidentes – ou seja, como será a reação quando alguma violação for detectada.

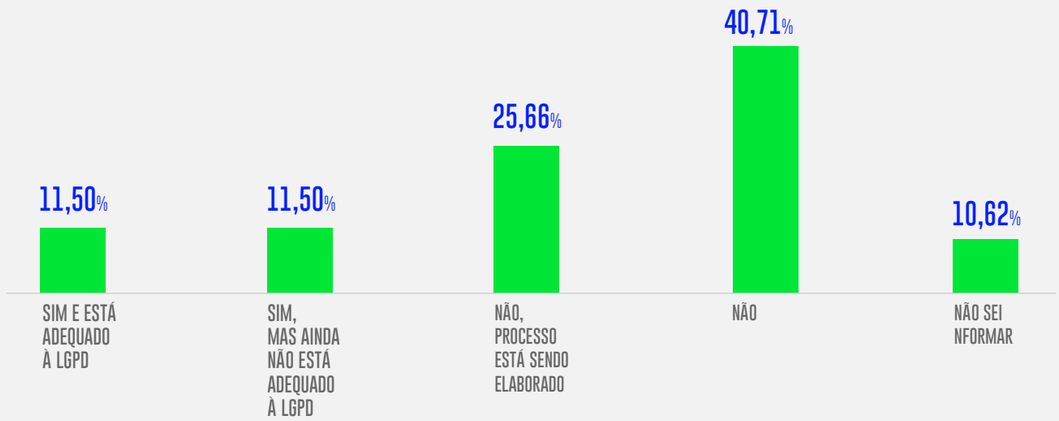
Quanto aos controles de segurança, os respondentes avaliaram suas organizações em uma escala de 1 a 10. Os valores se mantêm estáveis desde 2020, com uma média entre 5,6 e a maioria das notas concentradas entre 4 e 7. Na cultura de proteção de dados, registrou-se uma pequena melhora – a média subiu para 5,23, acima dos 4,8 registrados tanto em 2021 como em 2020.

Houve também uma melhora no tratamento de incidentes. Entre os participantes, 23% disseram que existe um processo de resposta a incidentes de dados pessoais – metade deles já em conformidade com a legislação. É a primeira vez que este número fica acima dos 20%. Mesmo assim, 40,71% das instituições não contam com esse processo estabelecido.

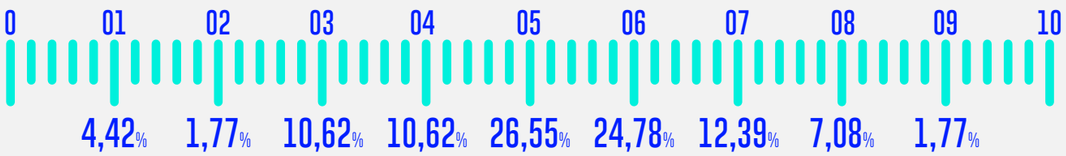
Em uma escala de 1 a 10 (sendo 10 a maior), como você avalia o atual conjunto de controles de segurança para evitar/tratar vazamentos de dados pessoais de sua organização?



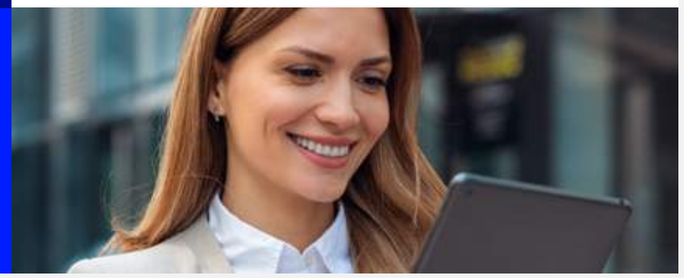
Sua organização tem um Processo de Tratamento de Incidentes da Segurança adequado à LGPD?



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



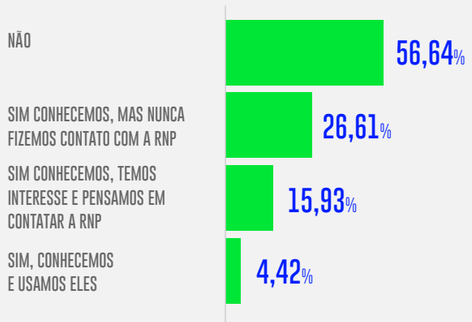
PROGRAMA LGPD NA RNP



A adequação à LGPD precisa passar por diversas etapas de acordo com as atividades desempenhadas pela instituição e a natureza dos dados obtidos, produzidos e armazenados no decorrer da rotina diária. Muitas vezes, uma consultoria externa consegue alavancar esse processo por meio de experiências similares em outras instituições, resolvendo impasses que são comuns a várias organizações do mesmo ramo de atuação.

A RNP oferece esse serviço às organizações integrantes do Sistema, facilitando e acelerando a adequação. Contudo, 56,6% dos respondentes disseram não conhecer esse serviço, que é de conhecimento de apenas 4,4% dos respondentes.

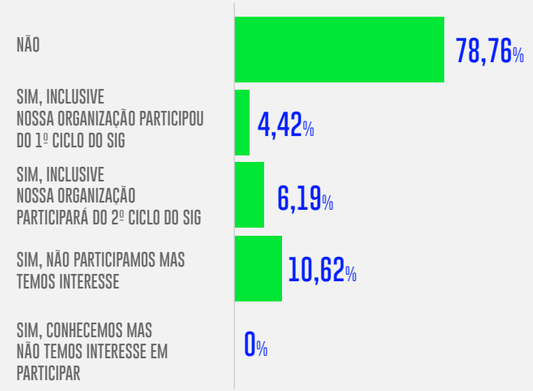
A sua organização conhece e usa os serviços consultivos de privacidade (Adequação à LGPD) da RNP?



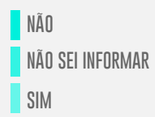
A RNP também apoia o Sistema RNP por meio do SIG-LGPD@RNP – um fórum restrito que oferece um espaço para interação e troca de conhecimento e experiências sobre o tema, renovando seus participantes a cada ciclo – e do Método RNP para adequação à LGPD, que estrutura um processo flexível e completo de conformidade voltado à comunidade de ensino. Essas iniciativas fazem parte do Programa LGPD na RNP, estabelecido para munir as instituições de tudo que é necessário para fazer frente aos desafios e transformações institucionais impostas pelo novo cenário regulatório.

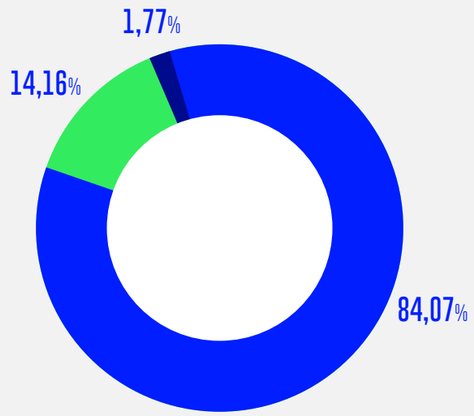
Muitos respondentes afirmaram não conhecer o SIG-LGPD (78,7%) e o método RNP para adequação (84%). É possível supor que haja mais espaço para cooperação, a qual pode ser um caminho para diminuir as dificuldades que as instituições enfrentam na jornada de adequação.

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



Você conhece o "Método RNP para adequação à LGPD"?





LAI – LEI DE ACESSO À INFORMAÇÃO

A Lei de Acesso à Informação (LAI) é uma legislação semelhante à LGPD em alguns sentidos. Por exemplo, ela exige a guarda de informações específicas e, ao mesmo tempo, esses dados precisam estar disponíveis para quem os solicitar sem que isso comprometa a segurança da instituição ou dados confidenciais.

Ao mesmo tempo, como ambas ditam regras sobre a utilização de dados coletados pelas organizações e entidades públicas, é preciso que a conformidade com a LGPD ocorra em harmonia com a LAI. Em outras palavras, é preciso conciliar a privacidade dos titulares de dados com a transparência que a sociedade espera do setor público.

Uma diferença, contudo, é que a LAI é mais antiga que a LGPD. Ela existe em sua forma atual desde 2011. Isso é visível nos números apurados pela pesquisa: a maioria das instituições consultadas estão em conformidade com todos os principais processos exigidos pela LAI, e 76,9% delas possui um responsável nomeado para o atendimento das demandas.

LAI: Lei de acesso à informação. A sua organização possui...

	SIM	NÃO	EM DESENVOLVIMENTO	PLANEJAMOS TER PARA 2023	NÃO SEI INFORMAR
A sua organização possui uma Política de transparência de dados?	52,21	15,93	4,42	6,19	21,24
A sua organização possui um responsável por receber e atender os pedidos de informação via Lei de Acesso à Informação (LAI)?	76,99	8,85	0,88	4,42	8,85
A sua organização possui um processo estruturado de SIC (Serviço de Informação ao Cidadão)?	68,14	18,58	0,88	3,54	8,85
A sua organização possui um espaço de transparência ativa para acesso aos principais documentos produzidos pela organização?	69,91	9,73	3,54	3,54	13,27

Sendo assim, é visível que a conformidade com a LAI se encontra em um estágio muito mais robusto do que o observado nos tópicos vinculados à LGPD.

DESENVOLVIMENTO DE COMPETÊNCIAS

GARTNER
ACESSE A MATÉRIA AQUI

2022 (ISC)² CYBERSECURITY WORKFORCE
ACESSE O ESTUDO AQUI

A capitação dos profissionais de segurança tende a somar os desafios da área de tecnologia com as complexidades da gestão da organização.

Da ala da tecnologia, há uma necessidade de evolução constante e de reciclagem das habilidades e conhecimentos. Um exemplo recente disso foi o aumento do uso da computação em nuvem, que acelerou em decorrência da sobrecarga enfrentada pelas cadeias de fornecimento de hardware. Segundo o Gartner, o uso de infraestrutura em nuvem superou expectativas e aumentou 99,1% nos dois primeiros anos da pandemia (2020 e 2021).

Esse tipo de evolução depende de profissionais qualificados, que compreendam e saibam contornar os desafios e perigos que acompanham o emprego de uma nova tecnologia. São cenários como este que acabam colaborando para o gap de profissionais do ramo, hoje estimado em 3,4 milhões pelo (ISC)².

O ângulo da gestão é ainda mais específico para a área de segurança. O mercado hoje entende que a segurança é inseparável da governança institucional e das próprias necessidades do negócio e do ramo de atuação. Portanto, cabe ao profissional de segurança desenvolver uma visão ampla da organização para saber os riscos e ameaças que devem ser priorizados.

As regulamentações como a Lei Geral de Proteção de Dados adicionam mais uma variável nesse cálculo. A organização não pode ignorar a lei nem descuidar de sua segurança e, ao mesmo tempo, o cumprimento dessas obrigações não pode inviabilizar as atividades.

As instituições de ensino superior têm um papel importante nesse cenário, já que são capazes de prover essa visão ampla em suas ofertas de capacitação. Partindo desse pressuposto, a pesquisa convidou as instituições a informar como lidam com a capacitação seus próprios colaboradores e quais programas de ensino e pesquisa em segurança elas oferecem à sociedade.

ESSE TIPO DE EVOLUÇÃO DEPENDE DE PROFISSIONAIS QUALIFICADOS, QUE COMPREENDAM E SAIBAM CONTORNAR OS DESAFIOS E PERIGOS QUE ACOMPANHAM O EMPREGO DE UMA NOVA TECNOLOGIA.

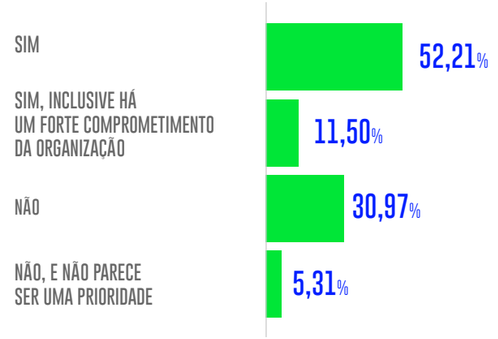
Os profissionais que atuam na área de cibersegurança contam com alguma das seguintes certificações?

ISACA CISA (Certified InformationSystems Auditor)	0,88%
ISACA CISM (Certified Information Security Management)	0,88%
(ISC)2 CISSP (Certified Information Systems Security Professional)	0,00%
EC-Council CCISO (Certified Chief Information Security Officer)	0,88%
EC-Council CEH (Certified Ethical Hacker)	0,88%
EC-Council CHFI (Computer Hacking Forensic Investigator)	0,00%
ECSS (EC-Council Certified Security Specialist)	0,00%
ECIH (EC-Council Certified Incident Handler)	0,88%
EC-Council CND (Certified Network Defender)	0,00%
EC-Council CPENT (Certified Penetration Testing Professional)	0,00%
CASP+ (CompTIA Advanced Security Practitioner)	0,00%
CompTIA Security+	2,65%
ISO 27001 Auditor Lider	1,77%
IAPP certificações (CIPP, CIPM, CIPT)	0,88%
Nenhuma até o momento, mas gostaríamos de obter alguma(s) das citadas	49,56%
Certificação não é prioridade para nós	15,04%
Não sei informar	27,43%
Outro (especifique)	8,85%

Mais de 60% das instituições que participaram da pesquisa afirmaram oferecer oportunidades de capacitação periódicas às equipes técnicas, e apenas 5,3% disseram que não há um interesse prioritário nessas iniciativas. Contudo, uma pergunta nova no questionário mostrou que metade das organizações ainda carece de profissionais com certificações consagradas no mercado.

Em termos de capacidades técnicas, a maior lacuna está em forense digital e análise de malware. Cabe destacar que a aprovação de novas regulamentações, como a LGPD, aumenta a relevância destas habilidades. Além de solucionar um incidente restabelecendo um sistema atacado, faz-se necessária uma perícia que determine se houve algum acesso indevido a dados pessoais, garantindo os direitos dos titulares na forma da lei.

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



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

	POSSUI	POSSUI PARCIALMENTE	NÃO POSSUI, PRECISA DESENVOLVER
Administração segura/controle tecnológico de segurança (firewall, IDS/IPS, anti-malware, etc)	51,33%	41,59%	7,08%
Resposta a incidentes	23,01%	49,56%	27,43%
Pentest/Ethical hacking/gestão de vulnerabilidades	6,19%	40,71%	53,10%
Política de segurança/gestão de riscos/gestão de segurança da informação/privacidade	18,58%	51,33%	30,09%
Gestão de identidades	17,70%	40,71%	41,59%
Desenvolvimento seguro	7,96%	41,59%	50,44%
Forense digital/Análise de malware	2,65%	17,70%	79,65%
Educação e conscientização	11,50%	55,75%	32,74%

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 17 anos de mercado e aproximadamente 40 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.

A maioria das instituições (58,41%) afirmou conhecer e fazer uso regular das vagas, mas 11,5% dos respondentes ainda disseram não ter conhecimento desta oportunidade.

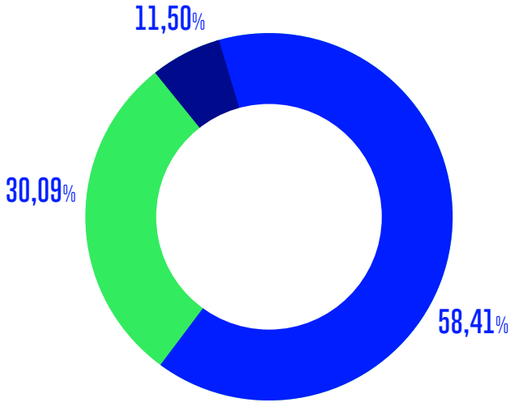
Quanto às ofertas de formação em cibersegurança, a pesquisa apurou a existência de cursos de graduação, pós-graduação, bolsas de estudo, laboratórios, grupos de pesquisa e o número de pesquisadores associados.

Observou-se um considerável volume de respostas como "não sei informar", inclusive entre respondentes de universidades federais e estaduais. Isso pode indicar que não há uma certeza a respeito da oferta destas pesquisas e iniciativas de formação, e que as instituições poderiam se beneficiar de uma melhor coordenação e comunicação nessa seara.

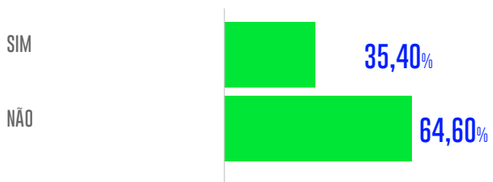
No geral, também vemos que as ofertas são bastante tímidas. O número mais expressivo foi obtido pela oferta de pós-graduação em universidades federais – 10,8%. Todos os demais números ficaram abaixo de 10%. Como há poucas ofertas de formação em cibersegurança, a existência de laboratórios dedicados também não é comum.

Muitas destas questões foram integradas ao questionário pela primeira vez em 2022 e, por este motivo, não há base de comparação com o ano anterior.

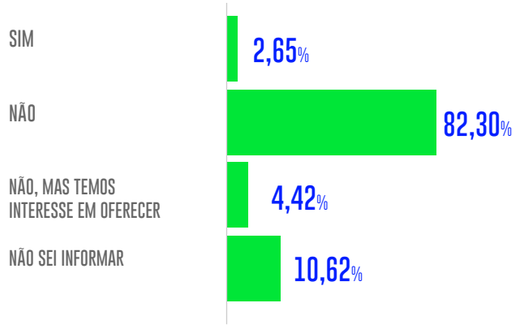
Sua organização conhece e faz uso da oferta de vagas disponíveis na Escola Superior de Redes da RNP (ESR/RNP) para instituições usuárias do Sistema RNP?



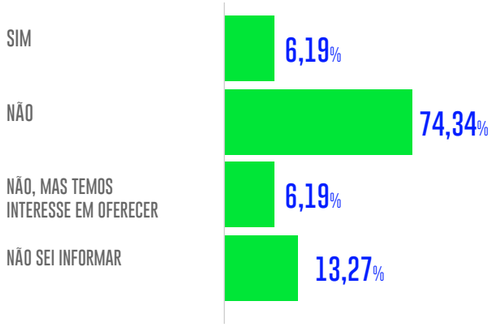
Caso não use as vagas, gostaria que algum representante da ESR entre em contato para explicar o funcionamento?



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

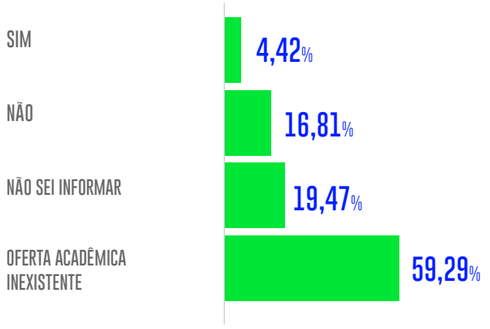


A sua organização tem atualmente uma oferta de formação em segurança cibernética a nível de Pós Graduação?



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

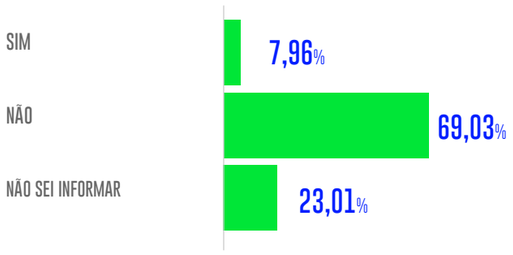
Caso as ofertas de formação acadêmicas existam, alguma delas oferece oportunidades de bolsas de estudo?



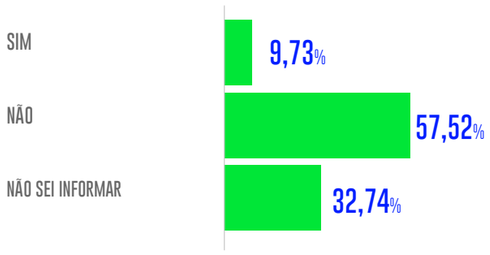
Por fim, a pesquisa também apurou se alguma startup já foi criada com base nas pesquisas e se há colaboração internacional. Entre as instituições que pesquisam o tema de segurança, uma em cada quatro disseram contar com colaboração internacional, mas apenas uma única instituição informou já ter colaborado com a criação de uma startup.

A criação de startups com base em pesquisas de segurança é uma maneira eficiente de transformar as inovações produzidas no mundo acadêmico em soluções para o mercado. Além disso, a existência de oportunidades para criar uma startup também ajuda a direcionar o esforço de pesquisa às áreas que podem tirar proveito da inovação desenvolvida na pesquisa.

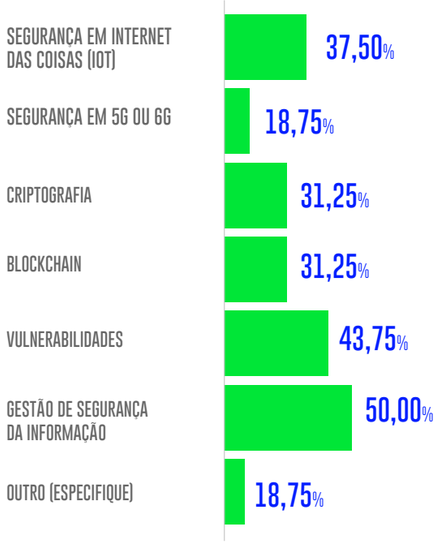
A sua instituição conta com algum laboratório para fins de ensino em segurança da informação/cibersegurança?



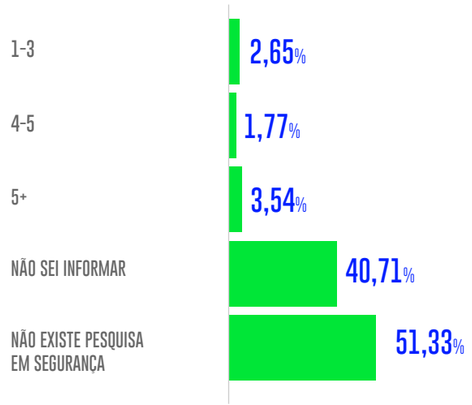
Existe algum grupo específico de pesquisa em segurança da informação/cibersegurança na sua organização?



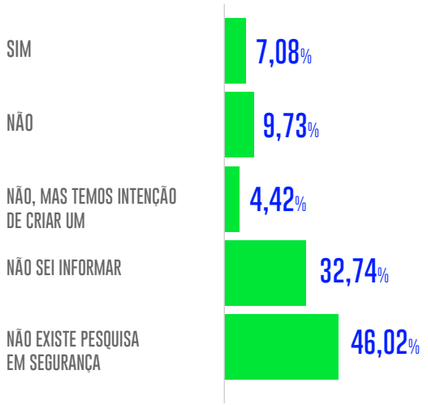
Se a resposta for positiva para a pergunta anterior, por favor indique se alguns destes temas são alvo de pesquisa desse(s) grupo(s):



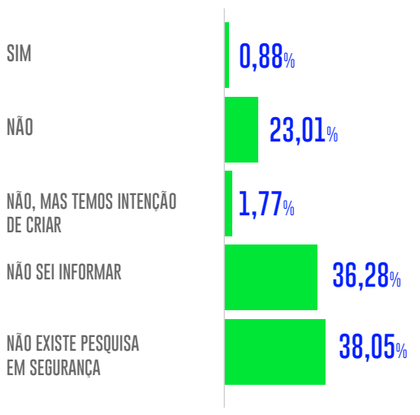
Se existir pesquisa em segurança, quantos pesquisadores estão associados às linhas de pesquisa apontadas?



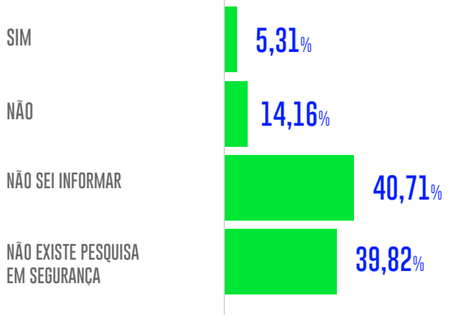
Se existirem iniciativas de pesquisa em segurança, a sua instituição dispõe de laboratórios específicos para este fim?



Se existirem iniciativas de pesquisa em segurança, por favor indique se alguma startup em segurança já foi criada.



Se existirem iniciativas de pesquisa no tema, estas contam com colaboração internacional?



CONCLUSÕES

Interpretar uma realidade em segurança da informação não é uma tarefa fácil. Mesmo quando podemos comparar com outros cenários, a comparação raramente é justa ou exata. Portanto, temos que ter certo cuidado com generalizações, especialmente quando levamos em conta o aumento significativo no número de organizações participantes nesta edição.

O que podemos enxergar em linhas gerais são os pontos onde há maior oportunidade para melhorias. Pelo terceiro ano consecutivo, vemos que a falta de recursos humanos é a dificuldade mais presente no dia a dia das instituições.

Mais especificamente, o problema pode ser resumido à contratação, pois constatamos que 63,7% das instituições oferecem oportunidades regulares de capacitação às suas equipes técnicas, demonstrando um comprometimento com a evolução contínua do quadro de colaboradores já existente. Ao que tudo indica, é um ponto forte das instituições.

Em termos de comparações, esta pesquisa guarda semelhanças com uma auditoria publicada em junho de 2022 pelo Tribunal de Contas da União (TCU). O levantamento do tribunal considerou as organizações públicas federais como um todo – um universo maior que o das instituições de ensino federais, mas que exclui as universidades estaduais sondadas nesta pesquisa.

Mesmo assim, há alguns paralelos. Destacamos os números referentes ao Plano de Ação para a LGPD: 49% não possuíam o plano na auditoria do TCU, enquanto esta pesquisa apurou um valor de 37,17%, embora muitos respondentes também não souberam informar.

As estatísticas sobre a Política de Segurança da Informação também permitem uma comparação válida: 24% das organizações não tinham uma política no levantamento do TCU, enquanto o mesmo número nesta pesquisa foi de 37,17%.

Embora seja inegável que há muito trabalho a ser feito – seja na administração pública ou nas instituições de ensino e pesquisa que compõem o Sistema RNP –, é essencial manter a perspectiva de que a segurança é um processo de melhoria contínua. Não existe uma vitória permanente, mas sim uma postura de comprometimento – e isso foi demonstrado por todos aqueles que fizeram questão de responder a esta pesquisa.

AUDITORIA DE PRIVACIDADE DO TRIBUNAL DE CONTAS DA UNIÃO_

ACESSO A PESQUISA

88% Foi o crescimento do número de participantes na pesquisa de 2021 para 2022

37,17% Das instituições não possuem Política de Segurança da Informação

63,7% É a proporção de instituições que oferecem oportunidades de capacitação às suas equipes técnicas

49,56% Das entidades respondentes definiram e nomearam um Encarregado de Proteção de Dados

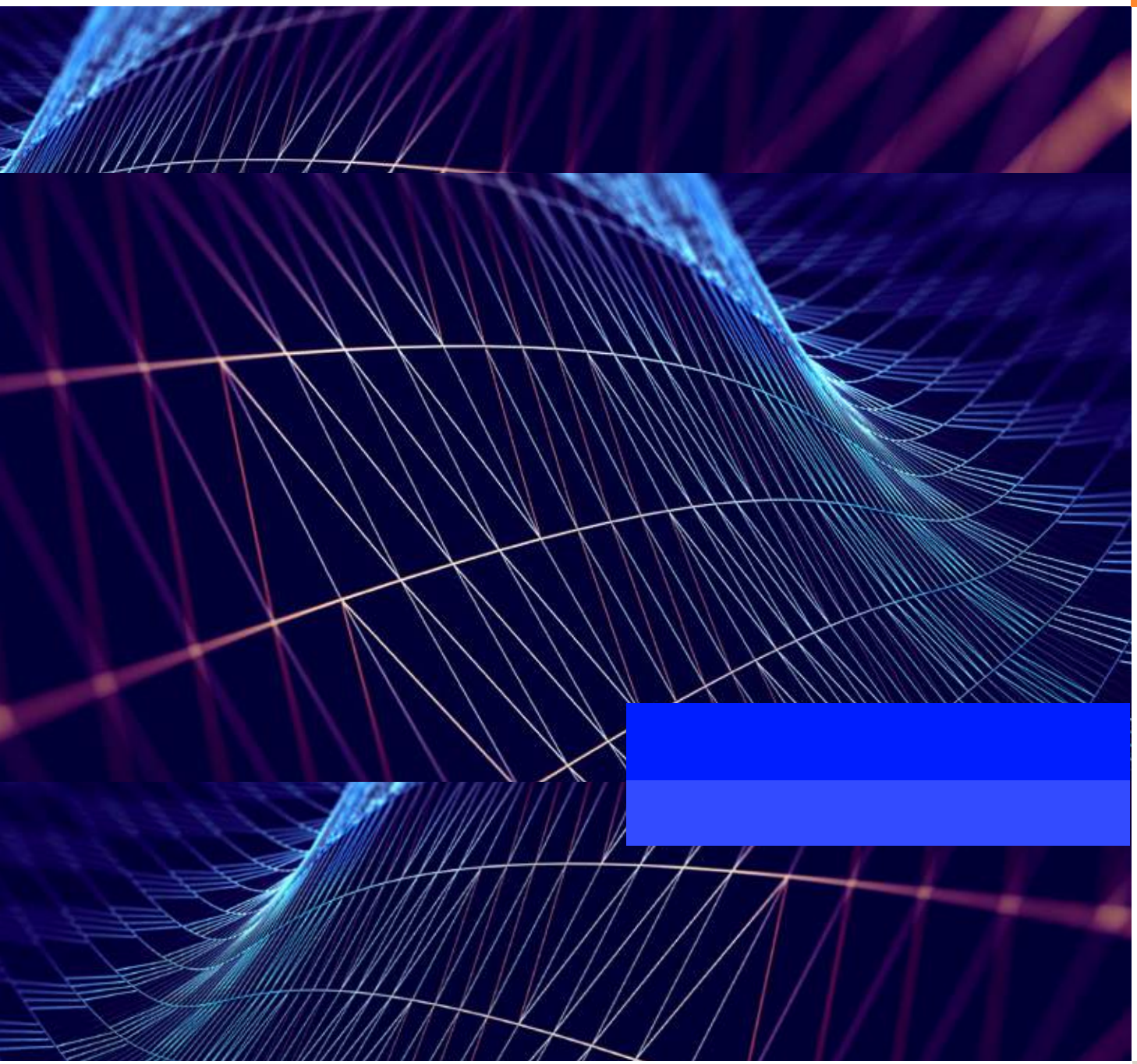
45% Das instituições não possui uma coordenaria específica para segurança da informação

10,61% É a proporção de instituições que se encontra em um estágio avançado de conformidade com a LGPD (Governança ou Melhoria Contínua)

65,4% Das instituições disseram possuir uma equipe de tratamento de incidentes (CSIRT ou ETIR)

11,5% É o número de instituições com processos de tratamentos de incidentes adequados à LGPD

4,9% Foi a autoavaliação das instituições para sua maturidade em segurança, em uma escala de 1 a 10



REALIZAÇÃO_
Gerência de Projetos Especiais em Segurança (GPES)
Liliana Velásquez Solha
Gerente

REDAÇÃO/EDIÇÃO_
GPES/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