Export these responses as PDF: Exportar para PDF

Export these responses as queXML PDF: Exportar para queXML PDF

Nome do questionário (ID): Diagnóstico e Índice de Maturidade de Segurança para adequação à Lei Geral de Proteção de Dados - LGPD (71975)

Identificação (216)

Por favor, informe o seu órgão: (1170)
Tipo: (!/list-dropdown)
A127 - Instituto Nacional da Propriedade Industrial – INPI

Por favor, insira as informações: (1169)
Tipo: (Q/multiple-short-txt)
Walace de Aguiar Ferreira
Nome Completo do Respondente (1171)

walace.ferreira@inpi.gov.br
E-mail do Respondente (1172)

Dimensão 1 - Estruturação e Organização (208)

1.1 Existe um planejamento de segurança da informação estabelecido na instituição com ações, metas e indicadores, contemplando as orientações previstas pela IN GSI nº 1/2020?

(1126)
Tipo: (L/list-radio)

Iniciou plano para adotar

20

1.2 A instituição designou formalmente um gestor de SI como responsável pela segurança da informação com capacitação técnica compatível às suas atribuições?

(1127)

Tipo: (L/list-radio)

Adota integralmente

100

1.3 A instituição estabeleceu um Comitê de Segurança da Informação ou estrutura equivalente com a finalidade de definir e conduzir diretrizes para a segurança da informação, composto por representantes das áreas de negócio?

(1129)

Tipo: (L/list-radio)

Adota integralmente

100

1.4 A instituição dispõe de uma Política de Segurança da Informação publicada e amplamente divulgada a todas as partes que se relacionam com a organização?

(1130)

Tipo: (L/list-radio)

Adota integralmente

100

1.5 A política de Segurança da Informação contempla os itens indiciados pelo art. 12 da IN GSI nº 1/2020?

(1131)

Tipo: (L/list-radio)

Adota integralmente

100

1.6 Os papéis e responsabilidades relacionadas com a Segurança da Informação e Privacidade estão descritos em normativos de cumprimento obrigatório, de forma a evidenciar a segregação de funções e assegurar que colaboradores e partes externas entendam suas responsabilidades?

(1132)

Tipo: (L/list-radio)

Adota parcialmente

50

1.7 A instituição definiu diretrizes e implementa o uso de criptografia para a proteção dos dados sensíveis ou críticos trafegados na rede e armazenados em dispositivos móveis, mídias removíveis ou em banco de dados?

(1133)
Tipo: (L/list-radio)

Não adota

0

1.8 O órgão ou entidade instituiu um sistema de gestão de segurança da informação?

(1134)
Tipo: (L/list-radio)

Não adota

0

Dimensão 2 – Gestão de Riscos e de Vulnerabilidades (209)

2.1 A instituição definiu diretrizes e executa processo de gestão de riscos de segurança da informação?

(1137)
Tipo: (L/list-radio)

Iniciou plano para adotar

20

2.2 A instituição dispõe de processo de análise e monitoramento de vulnerabilidades?

(1138)
Tipo: (L/list-radio)

Adota parcialmente

50

2.3 Existe um prazo formalmente definido para o tratamento de vulnerabilidades técnicas relevantes identificadas?

(1139)
Tipo: (L/list-radio)

Não adota

0

2.4 Os recursos de segurança da informação e de tecnologia da informação encontram-se em versões seguras, estáveis e atualizadas?

(1140)

Tipo: (L/list-radio)

Adota integralmente

100

2.5 A instituição identificou quais são os sistemas de informação críticos para os serviços ofertados à sociedade e para as atividades administrativas internas?

(1141)

Tipo: (L/list-radio)

Adota parcialmente

50

2.6 A instituição formalizou documentação relativa aos procedimentos de *hardening* do sistema operacional de equipamentos que atuam como servidores no ambiente tecnológico contemplando ações como: desabilitar *logins* e senhas de fábrica, desabilitar serviços desnecessários, ativar somente os protocolos necessários e desabilitar outras configurações de fábrica de acordo com a tecnologia a ser instalada nos ambientes tecnológicos da instituição?

(1142)

Tipo: (L/list-radio)

Adota parcialmente

50

2.7 A instituição realiza varreduras nos ambientes tecnológicos a fim de identificar e mitigar as vulnerabilidades cibernéticas?

(1143)

Tipo: (L/list-radio)

Adota integralmente

100

2.8 A instituição adota a prática de testes de penetração (*pentest*) para descobrir e mitigar vulnerabilidades de segurança da informação em redes, em sistemas operacionais e em aplicações?

(1173)

Tipo: (L/list-radio)

Iniciou plano para adotar

20

2.9 A instituição realizada monitoramento da *Dark Web* com a finalidade de rastrear salas, blogs, fóruns e sites no mercado negro para identificar credenciais roubadas e outros vazamentos de dados pessoais tratados pelo órgão ou entidade?

(1174)
Tipo: (L/list-radio)

Iniciou plano para adotar

20

Dimensão 3 – Gestão de Configuração e Mudanças (210)

3.1 Há um inventário completo (software e hardware) e atualizado dos ativos de informação, contendo o fornecedor, o número da versão, os dados pessoais processados, a classificação dos dados pessoais (sensíveis ou apenas dados pessoais), quais softwares estão instalados e em quais equipamentos, e a(s) pessoa(s) na organização responsável(s) pelos ativos?

(1145)
Tipo: (L/list-radio)

Iniciou plano para adotar

20

3.2. A instituição realizada controle de mudanças em atualizações de software e outros componentes das soluções de TIC?

(1146)
Tipo: (L/list-radio)

Adota parcialmente

50

3.3. As mudanças realizadas no ambientes tecnológicos são planejadas e testadas?

(1147)
Tipo: (L/list-radio)

Adota parcialmente

50

3.4 Há uma avaliação de impactos potenciais, riscos e consequências, incluindo impactos de segurança da informação, quando da identificação de necessidade de mudanças?

(1148)
Tipo: (L/list-radio)

Adota integralmente

100

3.5. As mudanças são comunicadas para todas as partes interessadas?

(1175)
Tipo: (L/list-radio)

Adota integralmente

100

Dimensão 4 – Gestão de Incidentes (211)

4.1 A instituição formalizou e executa procedimentos específicos para gestão e resposta aos incidentes, contemplando: a definição de incidente; o escopo da resposta; quando e por quem as autoridades devem ser contatadas; papéis, responsabilidades e autoridades; avaliação de impacto do incidente; medidas para reduzir a probabilidade e mitigar o impacto do incidente; descrição da natureza dos dados pessoais afetados; as informações sobre os titulares envolvidos; procedimentos para determinar se um aviso para indivíduos afetados e outras entidades designadas (por exemplo, órgãos reguladores) é necessário?

(1150)
Tipo: (L/list-radio)

Adota parcialmente

50

4.2 Existe uma equipe de detecção, tratamento e resposta a incidentes de segurança cibernética (CSIRT)?

(1151)
Tipo: (L/list-radio)

Adota integralmente

100

4.3 A CSIRT é composta por pessoal com dedicação exclusiva?

(1152)

Tipo: (L/list-radio)

Não adota

0

4.4 Existe um canal apropriado para notificar os incidentes de segurança da informação de forma rápida?

(1176)

Tipo: (L/list-radio)

Adota integralmente

100

4.5 Os arquivos coletados como evidências são gravados em conjunto com o arquivo com a lista dos resumos criptográficos?

(1177)

Tipo: (L/list-radio)

Não adota

0

4.6 Nos casos em que seja inviável preservar as mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, o agente responsável pelo CSIRT coleta e armazena cópia dos arquivos afetados pelo incidente, tais como: logs, configurações do sistema operacional, arquivos do sistema de informação, e outros julgados necessários, mantendo-se a estrutura de diretórios original, bem como os "metadados" desses arquivos, como data, hora de criação e permissões; registrando em relatório a impossibilidade de preservar as mídias afetadas e listando todos os procedimentos adotados?

(1178)

Tipo: (L/list-radio)

Adota parcialmente

50

4.7 A instituição mantém um SOC *(Security Operations Center)* a fim monitorar eventos e detectar incidentes de segurança da informação?

(1179)

Tipo: (L/list-radio)

Não adota

0

4.8 O SOC *(Security Operations Center)* atua no regime de 24x7 (24 horas x 7 dias da semana)?

(1180)
Tipo: (L/list-radio)

Não adota

0

Dimensão 5 – Desenvolvimento Seguro (212)

5.1 A instituição definiu formalmente e executa processo formal de desenvolvimento seguro de sistemas construídos/mantidos por equipe própria ou por terceiros?

(1154)
Tipo: (L/list-radio)

Adota parcialmente

50

5.2 Os ambientes tecnológicos de desenvolvimento, teste, homologação e produção são segregados a fim de reduzir as possibilidades de modificação ou uso indevido dos recursos de processamento da informação, com controles de segurança adequados para cada ambiente?

(1155)
Tipo: (L/list-radio)

Iniciou plano para adotar

20

5.3 Quando há a cópia dos dados de produção para os ambientes de desenvolvimento, teste e homologação, há autorização do proprietário do ativo de informação

(1181)
Tipo: (L/list-radio)

Adota parcialmente

50

5.4 É realizada análise estática (SAST) e/ou análise dinâmica (DAST) dos requisitos de segurança cibernética dos sistemas de informação?

(1182)
Tipo: (L/list-radio)

Não adota

0

Dimensão 6 – Capacidade, Redundância e Continuidade (213)

6.1 A instituição utiliza mecanismos para monitoramento do uso dos recursos de TI, de forma a atender as necessidades de capacidade futura e garantir o desempenho requerido das aplicações?

(1156)

Tipo: (L/list-radio)

Adota parcialmente

50

6.2 Há redundância dos recursos de processamento da informação suficiente para atender aos requisitos de disponibilidade previstos em contratos, acordos ou convênios?

(1157)

Tipo: (L/list-radio)

Adota parcialmente

50

6.3 A instituição conta com um Plano de Continuidade de Negócio, que garanta o nível adequado de continuidade dos serviços e da segurança da informação durante uma situação adversa?

(1158)

Tipo: (L/list-radio)

Iniciou plano para adotar

20

6.4 São realizados, em intervalos de tempo predefinidos, simulações e/ou testes planejados, levando-se em consideração as menores indisponibilidades e impactos possíveis nos processos de negócio, de forma que seja possível identificar falhas que venham a comprometer qualquer parte do processo de continuidade, com vistas a promover revisões e atualizações periódicas dos Planos relacionados?

(1159)

Tipo: (L/list-radio)

Não adota

0

6.5 Há uma política ou norma de backup que aborde os procedimentos operacionais que padronizam os processos de geração de cópias de segurança e recuperação de arquivos, assim como os processos de controle de acesso, armazenamento, movimentação e descarte das mídias que contêm cópias de segurança?

(1184)

Tipo: (L/list-radio)

Adota integralmente

100

6.6 É definida a abrangência dos testes de backup e sua periodicidade, de forma que os testes sejam planejados observando as dependências e relacionamentos entre sistemas, considerando inclusive os ambientes de continuidade de negócios, com o objetivo de minimizar a possibilidade de que a ausência de sincronismo entre os dados inviabilize ou dificulte sua recuperação?

(1185)

Tipo: (L/list-radio)

Não adota

0

6.7 As mídias que contêm cópias de segurança são armazenadas em uma localidade remota *("offsite")*, a uma distância suficiente que garanta sua integridade e disponibilidade contra possíveis danos advindos de um desastre ocorrido no sítio primário?

(1186)

Tipo: (L/list-radio)

Adota integralmente

100

Dimensão 7 – Capacitação, Conscientização e Sensibilização (214)

7.1 A instituição definiu e implementa programa de educação e conscientização em segurança da informação com o objetivo de tornar conscientes os servidores, empregados públicos, colaboradores, estagiários e, onde relevante, partes externas, dos normativos e das suas responsabilidades relativas a segurança da informação dos recursos de TI, serviços e informações do órgão ou entidade?

(1160)

Tipo: (L/list-radio)

Não adota

0

7.2 A instituição realiza campanhas de sensibilização sobre segurança da informação como por exemplo: divulgação de boletins e folders, promover o dia da segurança da informação, etc.?

(1162)
Tipo: (L/list-radio)

Iniciou plano para adotar

20

7.3 Após a realização de ações de conscientização ou capacitação em segurança da informação promovidas pela instituição, os servidores, empregados públicos, colaboradores, estagiários e terceirados são avaliados a fim de verificar a assimilação dos conhecimentos dos temas de segurança da informação?

(1161)
Tipo: (L/list-radio)

Não adota

0

7.4 As equipes técnicas que atuam diretamente com segurança da informação são treinadas regularmente?

(1187)
Tipo: (L/list-radio)

Iniciou plano para adotar

20

Dimensão 8 – Controles de Acesso Lógico (217)

8.1 A instituição formalizou e implementa política de controle de acesso à informação e aos recursos de TI?

(1188)
Tipo: (L/list-radio)

Adota parcialmente

50

8.2 A criação de contas de acesso de usuários ao ambiente tecnológico da instituição somente ocorre mediante assinatura de Termo de Responsabilidade?

(1189)

Tipo: (L/list-radio)

Adota integralmente

100

8.3 No caso das contratações, o representante legal e o(s) empregado(s) da Contratada assinam, respectivamente, o Termo de Compromisso e Termo(s) de Ciência?

(1190)

Tipo: (L/list-radio)

Adota integralmente

100

8.4 A criação e manutenção de contas de acesso são embasadas do princípio da necessidade de conhecer?

(1191)

Tipo: (L/list-radio)

Adota integralmente

100

8.5 Uma análise crítica de direitos de acesso é realizada em um período de tempo previamente definido ou a qualquer momento depois de qualquer mudança nos direitos de usuários ou para verificação de incidentes de segurança?

(1192)

Tipo: (L/list-radio)

Iniciou plano para adotar

20

8.6 A instituição adota para suas contas de acesso à rede e sistemas de informação uma política de senha com definição de tamanho mínimo e formato?

(1193)

Tipo: (L/list-radio)

Adota integralmente

100

8.7 Um mecanismo de recuperação de senha está implementado de forma a assegurar a recuperação da senha de maneira segura, sem fornecimento de senha por parte da aplicação, e que obrigue a alteração de senha do usuário no primeiro acesso?

(1194)

Tipo: (L/list-radio)

Não adota

0

Dimensão 9 – Privacidade (218)

9.1 O desenvolvimento dos sistemas tem como base os riscos e as medidas de segurança identificadas no RIPD (Relatório de Impacto de Proteção à Dados Pessoais)?

(1196)

Tipo: (L/list-radio)

Não adota

0

9.2 A instituição formalizou uma política ou norma de proteção de dados pessoais que aborde a finalidade da instituição perante o tratamento de dados; a transparência com relação à coleta e tratamento de dados pessoais; a estrutura estabelecida para a proteção de dados pessoais; regras para tomar decisões em questões de proteção de dados pessoais; critérios de aceitação de risco de privacidade; compromisso de satisfazer os requisitos aplicáveis de proteção à privacidade?

(1197)

Tipo: (L/list-radio)

Adota parcialmente

50

9.3 Os dados pessoais utilizados em ambiente de TDH (Teste, Desenvolvimento e Homologação) passaram por um processo de anonimização?

(1198)

Tipo: (L/list-radio)

Não adota

0

9.4 A instituição implementou um canal de comunicação ativo, seguro e autenticado para o recebimento de reclamações e manter um ponto de contato para receber e responder a reclamações, preocupações ou perguntas dos titulares sobre o tratamento de dados pessoais realizados pela instituição?

(1199)

Tipo: (L/list-radio)

Adota parcialmente

50

9.5 Ao fornecer a base de informações para órgãos de pesquisa, os dados pessoais são anonimizados ou pseudoanonimizados?

(1200)

Tipo: (L/list-radio)

Não adota

0

9.6 A instituição implementa processos para que o tratamento dos dados pessoais seja preciso, completo, atualizado, adequado e relevante para a finalidade de uso?

(1201)

Tipo: (L/list-radio)

Iniciou plano para adotar

20

9.7 A instituição monitora continuamente as ações de proteção de dados pessoais, a fim de determinar o progresso no cumprimento dos requisitos de conformidade com a proteção de dados pessoais e dos controles de proteção de dados pessoais, comparar o desempenho em toda a organização, identificar vulnerabilidades e lacunas na política e na implementação e identificar modelos de sucesso?

(1202)

Tipo: (L/list-radio)

Não adota

0

Dimensão 10 - Levantamento de Contratações e do Ambiente Tecnológico da Instituição (300)

10.1 Informe a quantidade de ativos de segurança da Informação (hardware) ou software a Instituição possui e se está(ão) em garantia e com contrato de suporte vigente.

(2696)

Tipo: (;/array-multi-flexi-text)

Balanceador de carga - SQ04	2	SIM	SIM

	Quantidade - SQ01	**Suporte vigente (Sim/Não) - SQ02**	**Garantia vigente (Sim/Não) - SQ03**
Web Application Firewall - SQ05	2	SIM	SIM
Antivírus, Antispam - SQ06	3	SIM	SIM
Solução de VPN - SQ11	2	SIM	SIM
Sistema de Gerenciamento de Eventos de Segurança - SQ10	0	NÃO	NÃO
Proteção de Vazamento de Dados - SQ07	2	SIM	SIM
Ferramenta de Scan de Vulnerabilidades - SQ09	1	SIM	SIM
Outros [especificar] - SQ08	0	NÃO	NÃO

10.2 Informe quantos links de internet a instituição possui?

(2697)

Tipo: (L/list-radio)

2

AO02

10.2.1 Informe o volume mensal do tráfego de Internet da Instituição para cada link

(2698)

Tipo: (;/array-multi-flexi-text)

	Volume GB - SQ01
Link 1 - SQ01	1300
Link 2 - SQ02	1300
Link 3 - SQ03	
Link 4 - SQ04	
Link 5 - SQ05	

10.3 Informe se a Instituição possui equipe dedicada para gerenciar os ativos de segurança

(2699)
Tipo: (L/list-radio)

Sim

AO01

10.4 Em caso de contratação centralizada de serviços de segurança, informar quais serviços abaixo seriam estratégicos para a Instituição e o nível da necessidade da contratação.

(2700)
Tipo: (F/array-flexible-row)

Não se aplica - AO04

Serviço de Gestão de Vulnerabilidades (2764)

Urgente - AO01

Serviço de Coleta, Consolidação e Correlacionamento de Eventos (2765)

Necessário - AO02

Serviço de Administração e Monitoramento de Segurança (2766)

Urgente - AO01

Serviço de Detecção e Resposta à Incidentes de Segurança (2767)

Não se aplica - AO04

Serviço de Balanceamento de carga para sites e aplicações, e Firewall de Aplicações Web (2768)

Pouco Importante - AO03

Serviço de Monitoramento de Segurança da Infovia (2769)

Não se aplica - AO04

Prevenção a Perda de Dados (DLP) (2770)

Necessário - AO02

Serviços de Capacitação (2771)

Necessário - AO02

Serviços Técnicos Especializados (sob demanda) (2772)

Não se aplica - AO04

Outros (descrever) (2773)

10.5 De quais fontes acredita ser importante coletar e correlacionar eventos de log:

(2701)
Tipo: (M/multiple-opt)

☑

Servidores Web (2707)

☑

Banco de dados (2711)

☑

Servidores de AD/DHCP (2715)

☑

DNS (2721)

☑

Proxies (2726)

☑

Firewall (2730)

☑

Antivírus (2732)

☑

Antispam (2736)

☑

SIEM (2739)
Ferramenta de Escaneamento de Vulnerabilidades (2740)

☑

Sistema de Proteção de Perda de Dados (DLP) (2743)
Balanceador de Carga (2746)

☑

Web Application Firewall (WAF) (2748)

☑

Máquinas Virtuais (2750)

☑

Desktops (2752)

☑

Impressoras (2753)

10.6 Em caso de contratação de Serviços Gerenciados de Segurança, informe se existe óbice caso os serviços do SOC (Security Operations Center) estejam hospedados fora da instituição?

(2702)
Tipo: (L/list-radio)

Não

AO02

10.7 No caso da contratação de Serviços Gerenciados de Segurança, informe se a Instituição considera como risco de Segurança empresa privada receber logs dos ativos de rede e ambientes e fazer o tratamento dessas informações em Datacenter próprio ou em nuvem.

(2703)
Tipo: (L/list-radio)

Sim

AO01

10.8 No caso de contratação de Serviços Gerenciados de Segurança, informe se a Instituição considera risco de Segurança empresa pública receber logs dos ativos de rede e ambientes e fazer o tratamento dessas informações em Datacenter próprio ou em núvem.

(2704)
Tipo: (L/list-radio)

Não

AO02

10.9 No caso de contratação de Serviços Gerenciados de Segurança, por conta das atribuições inerentes ao Centro de Operação de Segurança, os analistas poderão ter acesso a logs que contenham informação sob proteção de Sigilo? (2705)
Tipo: (L/list-radio)

Não

AO02

10.10 Os fornecedores das ferramentas e equipamentos de segurança contratados pelo Órgão poderão ser contactados diretamente pela equipe do Centro de Operações de Segurança (SOC) em caso de duvidas técnicas ou incidentes de segurança? (2706)
Tipo: (L/list-radio)

Não

AO02

Cálculos (215)

0.655

(1128)
Tipo: (*/equation)
0.655

0.481

(1144)
Tipo: (*/equation)
0.481

0.566

(1149)
Tipo: (*/equation)
0.566

0.425

(1153)
Tipo: (*/equation)
0.425

0.318

(1163)
Tipo: (*/equation)
0.318

0.505

(1164)
Tipo: (*/equation)
0.505

0.05

(1165)
Tipo: (*/equation)
0.05

0.72

(1167)
Tipo: (*/equation)
0.72

0.195

(1204)
Tipo: (*/equation)
0.195

0.44737

(1195)
Tipo: (*/equation)
0.44737

Basico

(1168)
Tipo: (*/equation)
Basico

Dimensões	Índice
Dimensão 1 – Estruturação e Organização	**0.66**
Dimensão 2 – Gestão de Riscos e de Vulnerabilidades	**0.48**
Dimensão 3 – Gestão de Configuração e Mudanças	**0.57**
Dimensão 4 – Gestão de Incidentes	**0.43**
Dimensão 5 – Desenvolvimento Seguro	**0.32**
Dimensão 6 – Capacidade, Redundância e Continuidade	**0.51**
Dimensão 7 – Capacitação, Conscientização e Sensibilização	**0.05**
Dimensão 8 – Controles de Acesso Lógico	**0.72**
Dimensão 9 – Privacidade	**0.2**

Nota iGestSI **0.45**
Nível de Gestão de SI **Basico**

(1166)
Tipo: (X/boilerplate)
