MORAIS ANDRADE

LEANDRIN | MOLINA ADVOGADOS

GUIA DE FRAMEWORK DE SEGURANÇA

MORAIS ANDRADE

LEANDRIN | MOLINA ADVOGADOS

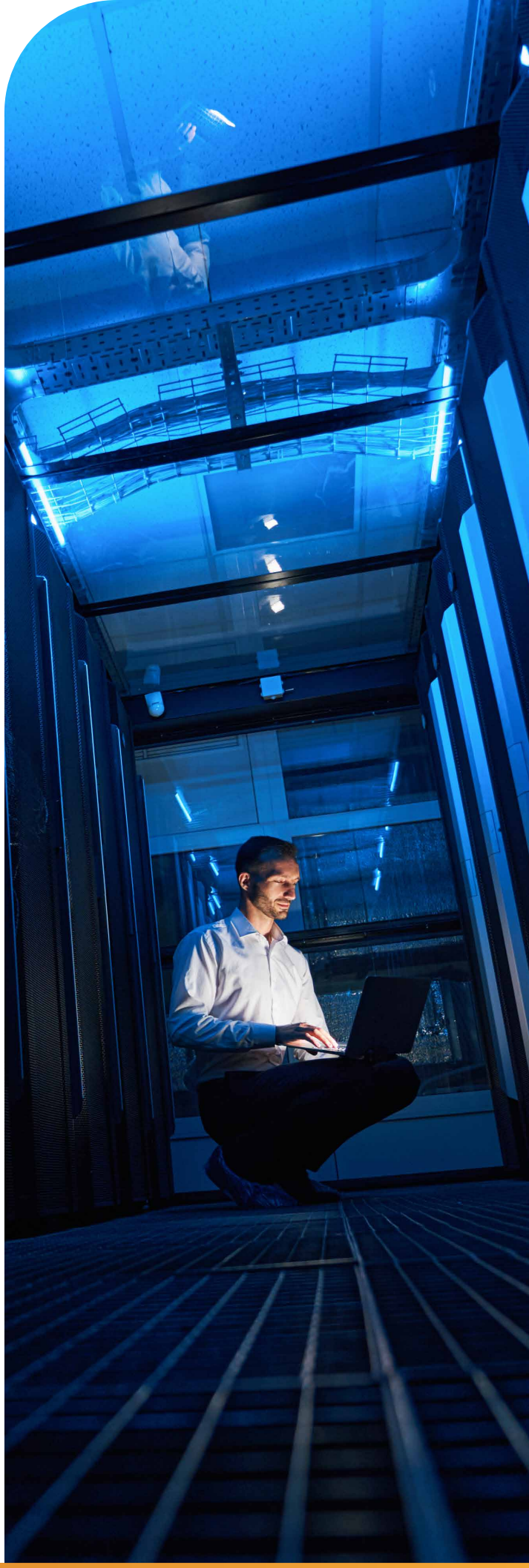
GUIA DE FRAMEWORK DE SEGURANÇA

Publicado pelo Governo Digital no dia 15 de dezembro de 2021, em sua segunda versão, **o Guia de Framework de Segurança promove a difusão de práticas internacionais na matéria de segurança da informação**, com o direcionamento aos órgãos e às entidades da Administração Pública Federal brasileira, no que se refere à aplicação dos termos do capítulo VII da Lei Geral de Proteção de Dados (LGPD), intitulado como "Da segurança e das boas práticas".

Quanto ao objetivo, o **Guia de Framework busca oferecer aos profissionais da área de segurança da informação uma maneira de identificação e verificação das possíveis lacunas de segurança da informação presentes na instituição em relação aos 18 Controles de Segurança** elaborados pelo Center for Internet Security (CIS), garantindo a gestão de risco pré-existente.

A nível de explicação, os Controle do CIS, desenvolvidos por profissionais experientes e dos diversos setores da economia, representam os mecanismos de ações que atuam de forma coletiva na defesa de sistemas e infraestrutura através da implementação de práticas que possam mitigar desde os mais comuns aos mais complexos tipos de ataques.

Sendo assim, como garantia para a implementação aos mais variados tipos de instituições, foram criados três Grupos de Implementação (GI), com medidas de seguranças específicas para cada nível de complexidade, sendo cumulativas a cada grupo avançado.



Grupo de Implementação 1

Instituições de pequeno a médio porte com limitado corpo de profissionais de TI e experiência em cibersegurança. Dados de sensibilidade baixa, representados, principalmente, por informações financeiras e de funcionários. Medidas destinadas a impedir ataques gerais não direcionados.

Grupo de Implementação 2

Instituições que gerenciam e protegem a infraestrutura de TI, com a tratativa de dados relacionados a informações confidenciais ou sensíveis de cidadãos, incluindo dados pessoais. Inclui as medidas no GI 1.

Grupo de Implementação 3

Instituições que empregam especialistas em segurança, aptos ao trabalho relacionado ao gerenciamento de risco, teste de penetração e segurança de aplicativos. Neste caso, há a tratativa de dados que, na hipótese de violação, podem causar danos significativos ao bem-estar público. Inclui as medidas do GI 1 e do GI 2, igualmente.

Por conseguinte, para o cumprimento de seus objetivos, o CIS enquadra as cincos funções de Segurança da Estrutura Básica, de acordo com o Guia de Aperfeiçoamento da Segurança Cibernética para Infraestrutura Crítica do NIST, sendo elas:

Identificar

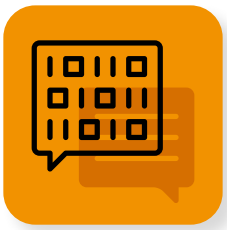
Desenvolvimento de uma compreensão de organização para gerenciar o risco de segurança cibernética em relação a sistemas, pessoas, ativos, dados e recursos, como estratégias de gerenciamento de riscos e governança.

Proteger

Desenvolvimento de práticas que garantam as proteções necessárias para a garantia dos serviços, a exemplo da conscientização e treinamento, segurança de dados e proteção da informação.

Detectar

Desenvolvimento de atividades necessárias, como o monitoramento contínuo de segurança, para a identificação de eventos de insegurança cibernética.



Responder

Desenvolvimento de respostas eficazes para atuar contra um incidente cibernético, através do planejamento de resposta, mitigação e aperfeiçoamentos.

Recuperar

Desenvolvimento de atividades que permitam a restauração de quaisquer recursos ou serviços que sejam alvos de um incidente de segurança cibernético, a exemplo do planejamento de restabelecimento.

OS 18 CONTROLES DA CIS

Controle 1

Inventário e Controle de Ativos Institucionais

Controle 2

Inventário e Controle de Ativos de Software

Controle 3

Proteção de Dados

Controle 4

Configuração Segura de Ativos Institucionais e Software

Controle 5

Gestão de Contas

Controle 6

Gestão do Controle de Acesso

Controle 7

Gestão Contínua de Vulnerabilidades

Controle 8

Gestão de Registros de Auditoria

Controle 9

Proteções de E-mail e Navegador Web

Controle 10

Defesas Contra Malware

Controle 11

Recuperação de Dados

Controle 12

Gestão da Infraestrutura de Rede

Controle 13

Monitoramento e Defesa da Rede

Controle 14

Conscientização e Treinamento de Competências sobre Segurança

Controle 15

Gestão de Provedor de Serviços

Controle 16

Segurança de Aplicações

Controle 17

Gestão de Resposta a Incidentes

Controle 18

Testes de Invasão

Para acessar e conhecer o Guia do Framework de Segurança da LGPD, visite:

https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/GuiadoFrameworkdeSegurancaV2SISP3.pdf

Você sentiu falta de algum tema ou quer conversar melhor sobre essas mudanças?

Entre em contato agora mesmo com a nossa área de Direito Digital!

www.moraisandrade.com
55 + 11 5555-6128
direitodigital@moraisandrade.com
linkedin.com/company/morais-andrade-advogados/
Al. Casa Branca, 35, 10º andar - cj. 1006/1009 - Jardim Paulista
Cep: 01408-001 - São Paulo - SP