Diário Oficial
Estado de São Paulo
Poder Executivo
Seção I
Palácio dos Bandeirantes
Av. Morumbi, 4.500 - Morumbi - CEP 05698-900 - Fone: 3745-3344

Nº 195 - DOE – 09/10/2024 – Seção – 1 – p.76

SECRETARIA DE GESTÃO E GOVERNO DIGITAL
GABINETE DO SECRETÁRIO

Resolução SGGD nº 33, de 07-10-2024

Institui o Guia de Boas Práticas em Cibersegurança no âmbito da Administração Pública direta e autárquica do Estado de São Paulo.

O SECRETÁRIO DE GESTÃO E GOVERNO DIGITAL DO ESTADO DE SÃO PAULO, no uso das atribuições legais que lhe são conferidas pelo artigo 10 do Decreto nº 67.799, de 13 de julho de 2023,

CONSIDERANDO a Estratégia de Governo Digital (EGD), instituída pelo Decreto nº 67.799/2023, que estabelece diretrizes para a implementação de soluções digitais eficientes e seguras, alinhadas aos princípios de interoperabilidade, segurança da informação, privacidade, inovação tecnológica e foco no usuário, em especial:

Artigo 3º, inciso VI, que estabelece como um dos princípios da EGD a privacidade e segurança da informação, enfatizando o investimento contínuo em soluções tecnológicas que assegurem a segurança física e lógica de dados e informações;

Artigo 3º, inciso VII, dada a vinculação da segurança cibernética à prevenção de ilícitos e desvios de conformidade através de soluções tecnológicas;

Artigo 4º, inciso XIII, que determina como objetivo da EGD o constante aprimoramento da infraestrutura e da segurança física e lógica dos recursos de tecnologia da informação e comunicação, fortalecendo a resiliência do ambiente digital;

Artigo 5º, inciso I, alínea “d”, que prevê a necessidade de que os Planos Diretores de Tecnologia da Informação e Comunicação (PDTIC) incluam medidas de segurança digital;

Artigo 6º, inciso II, que atribui à Secretaria de Gestão e Governo Digital (SGGD) a competência para coordenar a implementação da EGD, incluindo ações de cibersegurança;

Artigo 7°, que atribui à Companhia de Processamento de Dados do Estado de São Paulo (PRODESP) o papel de prestar os serviços de tecnologia da informação e comunicação necessários ao Sistema Estadual de Tecnologia da Informação (SETIC) e à execução da EGD e dos PDTICs.

CONSIDERANDO a crescente sofisticação e frequência de ataques cibernéticos, bem como a necessidade premente de proteger os sistemas e infraestruturas críticas do Estado, garantindo a continuidade dos serviços públicos;

CONSIDERANDO a necessidade de fortalecer a resiliência cibernética dos órgãos e entidades estaduais, promovendo a continuidade dos serviços públicos e a proteção das infraestruturas tecnológicas críticas; e

CONSIDERANDO a importância de estabelecer diretrizes claras para a gestão de riscos cibernéticos, alinhadas às melhores práticas internacionais, como o *NIST Cybersecurity Framework,*

RESOLVE:

Artigo 1º - Fica instituído o Guia de Boas Práticas em Cibersegurança, destinado aos órgãos e entidades da Administração Pública direta e autárquica do Estado de São Paulo, conforme anexo desta Resolução.

Artigo 2º - O Guia de Boas Práticas em Cibersegurança tem por objetivo orientar e recomendar ações para o aprimoramento da segurança cibernética, promovendo a proteção dos sistemas e infraestruturas críticas e a continuidade dos serviços públicos.

Artigo 3º - Os órgãos e entidades deverão adotar as diretrizes e recomendações contidas no Guia, observadas suas particularidades e necessidades específicas.

Artigo 4º - A SGGD, por meio da Subsecretaria de Serviços ao Cidadão, Tecnologia e Inovação (SSCTI), promoverá a atualização periódica do Guia de Boas Práticas em Cibersegurança, assegurando sua adequação às inovações tecnológicas e às melhores práticas internacionais.

Artigo 5º - A PRODESP disponibilizará, em colaboração com os órgãos e entidades a que se refere o Artigo 1º, processo de diagnóstico e avaliação de maturidade em cibersegurança, incluindo o suporte técnico, ferramentas, metodologias e consolidação de resultados.

Artigo 6º - A SSCTI deverá divulgar amplamente o Guia entre os órgãos e entidades da Administração Pública Estadual, recomendando sua aplicação efetiva.

Artigo 7º - Esta Resolução entra em vigor na data de sua publicação.

CAIO MÁRIO PAES DE ANDRADE

Secretário de Gestão e Governo Digital do Estado de São Paulo

ANEXO

GUIA DE BOAS PRÁTICAS EM CIBERSEGURANÇA

CAPÍTULO 1 - DISPOSIÇÕES PRELIMINARES

1. Este Guia visa:

1.1. Orientar os órgãos e entidades da Administração Pública Estadual na adoção de práticas que fortaleçam a segurança cibernética;

1.2. Promover a conscientização sobre a importância da cibersegurança para a continuidade e eficiência dos serviços públicos;

1.3. Facilitar a implementação de medidas preventivas e reativas contra ameaças cibernéticas, visando proteger sistemas e infraestruturas críticas do Estado.

CAPÍTULO 2 - GLOSSÁRIO

2. Para os fins deste Guia, considera-se:

2.1. Cibersegurança: Conjunto de práticas e medidas destinadas a garantir a segurança física e lógica de sistemas, redes e dados, assegurando a confidencialidade, integridade e disponibilidade das informações;

2.2. Diagnóstico de Cibersegurança: Avaliação da postura de segurança de um órgão ou entidade, identificando vulnerabilidades, ameaças e riscos em seus ativos tecnológicos;

2.3. Avaliação de Maturidade em Cibersegurança: Análise da capacidade do órgão de implementar, gerenciar e aprimorar controles de segurança, com base em modelos reconhecidos, como o NIST Cybersecurity Framework e o modelo das 7 Camadas de Segurança;

2.4. *NIST Cybersecurity Framework*: conjunto de diretrizes e boas práticas desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) e que oferece uma abordagem estruturada para a gestão de riscos cibernéticos, auxiliando as organizações a identificar, proteger, detectar e responder a incidentes de segurança;

2.5. Modelo das 7 Camadas de Segurança: Estabelece a implementação de múltiplas camadas de proteção, fundamentadas no princípio de Defesa em Profundidade, com o objetivo de garantir a segurança dos sistemas, redes e dados, abordando aspectos específicos, a saber:

2.5.1. Camada de Perímetro: Proteção da fronteira entre a rede interna e o ambiente externo, objetivando impedir que ameaças externas tenham acesso não autorizado ao sistema;

2.5.2. Camada de Rede: Proteção do tráfego de dados dentro da rede, objetivando controlar a comunicação interna, identificar e isolar ameaças;

2.5.3. Camada de Aplicação: Proteção das aplicações contra vulnerabilidades e acessos indevidos, objetivando garantir que as aplicações operem de forma segura, prevenindo falhas que possam ser exploradas;

2.5.4. Camada de Endpoint: Proteção dos dispositivos que acessam a rede, objetivando proteger os dispositivos contra malware e tentativas de acesso não autorizadas;

2.5.5. Camada de Ativos Críticos: Proteção dos sistemas e servidores críticos para a operação, objetivando assegurar que os sistemas essenciais estejam protegidos contra ataques e falhas;

2.5.6. Camada de Dados: Proteção dos dados em repouso e em trânsito, objetivando garantir que os dados estejam seguros contra acessos indevidos e vazamentos;

2.5.7. Camada Humana: Foco na conscientização e treinamento dos usuários, objetivando prevenir falhas humanas e comportamentos de risco cibernético.

2.6. Vulnerabilidade: Fragilidade que pode ser explorada para comprometer a segurança de um sistema;

2.7. Ameaça Cibernética: Potencial evento ou ação que pode causar danos a sistemas ou informações;

2.8. Risco Cibernético: Probabilidade de ocorrência de uma ameaça explorando uma vulnerabilidade, causando impacto negativo;

2.9. Ativo: Qualquer recurso de valor para a organização, incluindo informações, sistemas e pessoas;

2.10. Impacto: Consequência negativa resultante da exploração de uma vulnerabilidade, podendo incluir perdas financeiras, interrupção de serviços, danos à reputação e vazamento de dados.

CAPÍTULO 3 - PRINCÍPIOS ORIENTADORES

3. As boas Práticas em cibersegurança devem fundamentar-se nos seguintes princípios:

3.1. Abordagem Sistêmica: Consideração integrada de todos os aspectos da segurança da informação;

3.2. Gestão de Riscos: Identificação e mitigação contínua de riscos cibernéticos;

3.3. Defesa em Profundidade: Implementação de múltiplas camadas de segurança para proteção reforçada;

3.4. Cooperação: Colaboração entre órgãos e entidades para compartilhamento de informações e estratégias;

3.5. Cultura de Segurança: Promoção de valores e comportamentos que priorizem a segurança em todas as atividades.

CAPÍTULO 4 - DO DIAGNÓSTICO E AVALIAÇÃO DE MATURIDADE EM CIBERSEGURANÇA E DEMAIS RECOMENDAÇÕES

4.1. Recomenda-se que os órgãos e entidades realizem diagnósticos periódicos de cibersegurança, com o objetivo de identificar vulnerabilidades, ameaças e riscos em seus ambientes tecnológicos, abrangendo hardware, software, redes, dados, processos e pessoas.

4.2. O diagnóstico de cibersegurança deverá contemplar, no mínimo, as seguintes etapas:

4.2.1. Análise de Vulnerabilidades: Identificação de fragilidades em sistemas, aplicações e infraestrutura de rede, utilizando ferramentas e metodologias adequadas;

4.2.2. Avaliação de Risco: Análise do potencial impacto das vulnerabilidades identificadas, considerando a probabilidade de ocorrência e o possível dano aos ativos;

4.2.3. Análise de Superfície de Ataque: Mapeamento dos pontos de entrada e vetores de ataque potenciais, incluindo endpoints, aplicações, usuários e infraestrutura de rede;

4.2.4. Monitoramento de Tráfego de Rede: Análise do tráfego de rede para identificar comportamentos anômalos, tentativas de intrusão e comunicações com fontes maliciosas;

4.2.5. Análise de Logs: Coleta e exame dos registros de segurança para identificar eventos suspeitos e investigar incidentes.

4.3 Recomenda-se que a avaliação de maturidade em cibersegurança seja realizada com base no modelo das 7 (sete) Camadas de Segurança, considerando os seguintes aspectos:

4.3.1. Camada de Perímetro: Proteção da fronteira da rede contra acessos não autorizados;

4.3.2. Camada de Rede: Segurança do tráfego interno e detecção de atividades maliciosas;

4.3.3. Camada de Aplicação: Garantia da integridade e segurança dos sistemas e aplicações;

4.3.4. Camada Humana: Conscientização e treinamento dos usuários para prevenir erros e ações maliciosas;

4.3.5. Camada de Endpoint: Proteção dos dispositivos finais que acessam a rede;

4.3.6.Camada de Ativos Críticos: Segurança reforçada em sistemas e servidores essenciais;

4.3.7. Camada de Dados: Salvaguarda das informações, assegurando confidencialidade, integridade e disponibilidade.

4.4 Ao final do diagnóstico e da avaliação de maturidade, recomenda-se a elaboração de um relatório contendo:

4.4.1. Resultados Encontrados: Detalhamento das vulnerabilidades e riscos identificados;

4.4.2. Recomendações de Cibersegurança: Sugestões de medidas para mitigar riscos e corrigir vulnerabilidades;

4.4.3. Plano de Ação: Proposta de cronograma e responsabilidades para a implementação das melhorias necessárias.

4.5 Recomenda-se que os órgãos e entidades:

4.5.1. Implementem as Recomendações do Diagnóstico: Apliquem as medidas identificadas no plano de ação elaborado;

4.5.2. Promovam Capacitação: Invistam em treinamento e conscientização dos servidores sobre cibersegurança;

4.5.3. Elaborem Planos de Resposta a Incidentes: Estabeleçam procedimentos claros para atuação em caso de eventos cibernéticos;

4.5.4. Mantenham Atualizados os Sistemas: Garantam que softwares e dispositivos estejam sempre com as últimas atualizações e correções de segurança;

4.5.5. Gerenciem Acessos e Identidades: Controlem rigorosamente o acesso a sistemas e informações, adotando políticas de senhas fortes e autenticação multifator;

4.5.6. Monitorem Continuamente: Implementem soluções de monitoramento contínuo para detecção precoce de ameaças e incidentes.