SECRETARIA DA CONTROLADORIA GERAL DO ESTADO

GOVERNO DE PERNAMBUCO ESTADO DE MUDANÇA

INSTRUÇÃO DE SERVIÇO INTERNO SCGE Nº 01, DE 30 DE JULHO DE 2024

A **SECRETÁRIA DA CONTROLADORIA-GERAL DO ESTADO DE PERNAMBUCO**, no uso das atribuições que lhe são conferidas pelo inciso XXIII do art. 1º da Lei nº 18.139, de 18 de janeiro de 2023 e, considerando os requisitos estabelecidos pela Política de Segurança da Informação, Anexo Único da Portaria SCGE nº 14, de 22 de abril de 2022, **RESOLVE**:

TÍTULO I - DAS DISPOSIÇÕES GERAIS

Art. 1º. Instituir a **Política de Resposta a Incidentes de Segurança da Informação** como parte integrante da Política de Segurança da Informação Local da SCGE com objetivo de tratar os incidentes de segurança da informação ocorridos no âmbito da Secretaria da Controladoria-Geral do Estado de Pernambuco

Art. 2º. Para efeitos desta Instrução de Serviço Interna, os conceitos a seguir devem ser considerados por todos os componentes responsáveis pelo tratamento dos incidentes de segurança da informação da SCGE-PE:

I.

- Segurança da Informação: Medidas de salvaguarda da confidencialidade, integridade, disponibilidade a autenticidade das informações, estejam elas armazenadas ou em trânsito e em sua forma eletrônica, escrita ou falada, abrangendo, inclusive, a segurança dos recursos humanos, das áreas e instalações das comunicações, processamento e armazenamento, assim como as medidas destinadas a prevenir, detectar, deter e documentar eventuais ameaças e incidentes;

II.

- Privacidade: Direito fundamental que tem como virtude o controle que cada pessoa tem sobre as informações que lhe dizem respeito e que circunscrevem sua esfera pessoal, incluindo aspectos relacionados à intimidade e a atos que, embora possam ser externados, ainda permanecem sob a esfera de controle do próprio indivíduo;

III.

- Parte Interessada: Pessoa ou organização que pode afetar, ser afetada, ou perceber-se afetada por uma decisão ou atividade;

IV.

- Dado Pessoal: Informação relacionada a pessoa natural identificada ou identificável;

V.

- Autoridade Nacional de Proteção de Dados: Autarquia federal de natureza especial, responsável por zelar, implementar e fiscalizar o cumprimento da Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados) em todo o território nacional.

VI.

- Incidente de Segurança da Informação: Qualquer evento adverso, confirmado ou suspeito, que comprometa a privacidade, a confidencialidade, a integridade e

disponibilidade dos dados ou sistemas de informação mantidos sob a responsabilidade da SCGE;

VII.

- Sistemas de Informação: Sistema cujo elemento principal é a informação. Seu objetivo é armazenar, tratar e fornecer informações de tal modo a apoiar as funções ou processos de uma organização;

VIII.

- Encarregado de Dados Pessoais; Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

IX.

- Gestor do Processo: Pessoa designada pelo Órgão, responsável pela gestão das atividades do processo de trabalho, assim como pela incorporação de melhorias propostas e pelo monitoramento dos indicadores de desempenho do processo,

facilitando as ações e o fluxo de trabalho interno;

X.

- Equipe de Resposta a Incidentes de Segurança da Informação: Grupo temporário de resposta a Incidentes de segurança da informação com as atribuições de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança da informação ocorridos na SCGE/PE;

Art. 3º. Esta Instrução de Serviço Interno aplica-se a todos os ativos de segurança da informação sob a responsabilidade da Secretaria da Controladoria-Geral do Estado de Pernambuco

TÍTULO II - DO PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 4º. Define-se como **Plano de Resposta a Incidentes de Segurança da Informação** o conjunto ordenado de procedimentos e medidas estabelecidos pela SCGE para assegurar uma ação institucional completa e tempestiva em face da ocorrência de incidentes de segurança da informação.

Art. 5º. O **Plano de Resposta a Incidentes de Segurança da Informação** proposto nesta Política tem por referência as boas práticas elaboradas pelo Centro de Estudos, Resposta e

Tratamento de Incidentes de Segurança no Brasil (CERT.br) e a norma ABNT NBR ISO/IEC 27002:2013

Art. 6º. O **Plano de Resposta a Incidentes de Segurança da Informação** será composto pelas seguintes fases:

I.

- Detecção e notificação;

II.

- Avaliação e decisão estratégica;

III.

- preparação;

IV.

- contenção;

V.

- erradicação;

VI.

- recuperação;

VII.

- monitoramento das respostas a incidentes;e

VIII.

- lições aprendidas.

Art. 7º. São partes interessadas do **Plano de Resposta a Incidentes de Segurança da Informação**:

I.

- Encarregado de Dados Pessoais;

II.

- Gestor do Processo;

III.

- Equipe de Resposta a Incidentes de Segurança da Informação;

IV.

- Assessoria Especial de Controle Interno - AECI

V.

- Diretoria de Tecnologia da Informação do Controle Interno - DTCI

VI.

- Secretário da Controladoria-Geral do Estado – SCGE

VII.

- Coordenadoria de Proteção de Dados Pessoais

Parágrafo Único. A Equipe de Resposta a Incidentes de Segurança da Informação deverá ser designada formalmente pela DTCI, com a aprovação da secretária da SCGE e será

composta por, no mínimo:

I.

Um Representante da Gerência de Infraestrutura e Suporte de Tecnologia da Informação;

II.

I O encarregado de dados pessoais;

III.

Um Representante responsável pela área de negócio afetada, indicado pelo Gestor do Processo.

CAPÍTULO I - DA DETECÇÃO E NOTIFICAÇÃO

Art. 8º. O Gestor do Processo deverá comunicar imediatamente à Secretária da Controladoria Geral do Estado, à DTCI e ao Encarregado de Dados Pessoais, caso envolva dados pessoais, sobre todo evento suspeito relevante de segurança da informação na SCGE de que tenha conhecimento.

Art. 9º. A secretária, com o auxílio da DTCI, fará uma análise preliminar do evento suspeito e, uma vez encontrados indícios da ocorrência de um incidente de segurança da informação, deverá:

I.

- Acionar a Equipe de Resposta a Incidentes de Segurança da Informação para que proceda com a coleta de evidências e se prepare para as fases posteriores previstas no **Plano de Resposta a Incidentes de Segurança da Informação**;

II.

- Acionar o encarregado de dados, para casos onde houver dados pessoais envolvidos, e a DTCI, para casos onde não houver dados pessoais envolvidos, para notificarem a ocorrência do Incidente de segurança da informação às partes interessadas, em cada

caso, conforme descrito no Título III desta Instrução normativa.

§1º. O acionamento da Equipe de Resposta a Incidentes de Segurança da Informação pela secretária deverá ocorrer através do Sistema Eletrônico de Informação (SEI), por meio de processo classificado como sigiloso e utilização de modelo definido pela DTCI.

Art. 10. O Gestor do Processo deverá apresentar os motivos da demora na comunicação do evento suspeito, caso a comunicação com a DTCI não tenha sido imediata.

Art. 11. O Gestor do Processo deverá definir um responsável da área de negócio afetada para contribuir no desempenho das ações e encaminhará a decisão à Equipe de Resposta a Incidentes de Segurança da Informação, que manterá relação atualizada de todos os responsáveis escolhidos.

CAPÍTULO II - DA AVALIAÇÃO E DECISÃO ESTRATÉGICA

Art. 12. A Equipe de Resposta a Incidentes de Segurança da Informação, uma vez acionada pela Secretária, deverá propor, com o auxílio do responsável da área de negócio e do Encarregado de Dados Pessoais da SCGE, caso envolva dados pessoais, uma **Proposta Inicial de Resposta ao Incidente**, contendo, no mínimo:

I.

- A determinação do tipo de não conformidade ou violação;

II.

- A classificação do incidente, por nível de impacto do na Organização;

III.

- A definição do escopo da resposta;

IV.

- A relação de autoridades que deverão ser contatadas;

V.

- A estratégia de atuação;

Art. 13. Devem ser considerados os seguintes **tipos de não conformidade ou violação**:

I.

- Tentativas, com ou sem sucesso, de acesso não autorizado a um sistema ou a seus dados;

II.

- Interrupções indesejadas de serviço;

III.

- Uso não autorizado de sistema;

IV.

- Modificações no sistema sem o conhecimento ou sem o consentimento prévio do responsável técnico;

V.

- Sistemas desatualizados ou incorretamente configurados, permitindo abuso;

VI.

- Uso abusivo, em desrespeito à política de uso aceitável do provedor de serviço;

VII.

- Outras não conformidades.

Art. 14. Devem ser considerados os seguintes **níveis de impacto do incidente**:

I.

- GRAVE: afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;

II.

- SIGNIFICATIVO: afeta sistemas ou informações não críticas, sem impacto negativo à instituição;

III.

- MÍNIMO: possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

Art. 15. A Equipe de Resposta a Incidentes de Segurança da Informação, uma vez aprovada a
Proposta Inicial de Resposta ao Incidente pela secretária, deverá:

I.

- Realizar a avaliação técnica do incidente;

II.

- Convocar servidores de outras áreas da SCGE-PE, se necessário;

III.

- Solicitar à secretária a contratação tempestiva, e em caráter temporário, de agentes externos ao Órgão para atuação ad-hoc no caso, se necessário;

Art. 16. A avaliação técnica do incidente deverá considerar os seguintes itens:

I.

- A vulnerabilidade explorada no incidente: Abrange situações como: acesso indevido aos dados pessoais; roubo de dados; ataques cibernéticos; erros de programação de aplicativos e sistemas internos; engenharia social; descartes indevidos; repasse de dados pessoais; roubo, venda e utilização de dados tutelados pela entidade; comprometimento de senhas de acesso; e outras;

II.

- A fonte dos dados pessoais: meio pelo qual foram obtidos os dados pessoais, tais como preenchimento de formulário eletrônico ou não eletrônico por parte do titular, API, uso compartilhado de dados, XML e cookies;

III.

- A categoria de dados pessoais: dados sensíveis, dados pessoais de crianças e adolescentes;

IV.

- A extensão do vazamento: quantificação dos titulares e dos dados pessoais que tiveram a sua segurança violada neste evento;

V.

- O impacto aos titulares de dados pessoais: quais são os impactos que o incidente pode gerar aos titulares;

VI.

- O impacto nos serviços ofertados pelo Órgão: os impactos que o incidente pode gerar a entidade como perda de confiabilidade do cidadão, ações judiciais, dano à imagem da instituição em âmbito nacional e internacional, prejuízo à entidade em contratos com fornecedores e clientes, e impacto total ou parcial nas atividades desenvolvidas pela entidade;

VII.

- Os ativos de informação envolvidos no incidente: considerando as configurados de registro de eventos relevantes de segurança da informação, contendo, pelo menos, a identificação inequívoca do usuário, a natureza do evento, a data, hora e fuso horário, o identificador do ativo de informação, as coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento;

VIII.

- O sistema de monitoramento de aplicações, alertas e vulnerabilidades utilizado para auxiliar na detecção e tratamento de incidentes de segurança cibernética.

CAPÍTULO III - DA PREPARAÇÃO

Art. 17. A fase de preparação envolve a coleta e documentação das evidências do incidente, a abertura de canais de comunicação direta entre as partes interessadas e o detalhamento da **Proposta Inicial de Resposta ao Incidente**, com vistas a assegurar uma resposta adequada e tempestiva do Órgão.

Art. 18. A Equipe de Resposta a Incidentes de Segurança da Informação deverá, **em até 3 dias úteis** da aprovação da **Proposta Inicial de Resposta**, elaborar o **Plano de Resposta ao Incidente**, indicando, no mínimo:

I.

- Seleção dos Procedimentos Padrões de Respostas a Incidentes, ou a descrição dos Procedimentos Padrões de Respostas elaborados;

II.

- Medidas de Contenção, Erradicação e Recuperação previstas;

III.

- Cronograma de ação;

IV.

- Matriz de Comunicação; e

V.

- Matriz de Responsabilidades.

Art. 19. A DTCI, conforme planejamento anual, deverá elaborar, e manter atualizados, Procedimentos Padrões de Respostas relacionados aos principais tipos de incidente, de modo a manter a SCGE preparada para atuar de maneira tempestiva em face da ocorrência de incidentes no futuro.

CAPÍTULO IV - DA CONTENÇÃO

Art. 20. Esta fase corresponde à etapa “emergencial” do Plano, visto que busca evitar que os efeitos do incidente se estendam e a organização sofra maiores danos.

Art. 21. A depender do tipo de incidente, a Equipe de Resposta a Incidentes de Segurança da Informação promoverá dois tipos de contenção:

I.

- De Curto Prazo: resposta imediata, com o objetivo de impedir a materialização do

dano ou mitigar os efeitos do incidente de segurança da informação com a maior celeridade possível;

II.

- De Longo Prazo: restabelecimento temporário e seguro dos sistemas de informação afetados à sua produção normal, para que possam ser utilizados normalmente, enquanto a restauração completa ainda não se conclui. Envolve atualizações de segurança dos sistemas e a neutralização de backdoors e de arquivos maliciosos que viabilizaram o ataque.

Art. 22. Como parte da contenção de curto prazo, a Equipe de Resposta a Incidentes de Segurança da Informação deverá tomar medidas instantâneas de contenção caso identifique um incidente relevante de segurança da informação, mesmo antes da notificação pelo Gestor de Processo.

Art. 23. As informações preliminares sobre o incidente de segurança da informação, bem como as medidas imediatas de contenção realizadas pela Equipe de Resposta a Incidentes de Segurança da Informação citadas no art. 22 serão repassadas ao Gestor de Processo.

Art. 24. Nos casos em que seja inviável a preservação das mídias de armazenamento em razão da necessidade de pronto restabelecimento do serviço afetado, a Equipe de Resposta a Incidentes de Segurança da Informação deverá coletar e armazenar 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.

Parágrafo único. O armazenamento de cópias dos arquivos afetados, antes do restabelecimento dos sistemas, é fundamental pois propicia:

I.

- A preservação de vestígios da materialidade e da autoria do incidente, caso o incidente seja decorrente de conduta ilícita, civil ou penalmente reprovada;

II.

- A coleta de dados, em função da observação do comportamento dos sistemas durante e após o evento, com o objetivo de evitar a ocorrência de novos incidentes causados por inconformidades já mapeadas.

CAPÍTULO V - DA ERRADICAÇÃO

Art. 25. Após a contenção do incidente, será realizada a fase de erradicação pela Equipe de Resposta a Incidentes de Segurança da Informação com a:

I.

- Restauração de todos os sistemas corporativos afetados pelo incidente de segurança;

II.

- Remoção de qualquer vestígio do ataque;

III.

- Atualização dos sistemas e medidas corretivas essenciais para evitar a repetição do incidente.

CAPÍTULO VI - DA RECUPERAÇÃO

Art. 26. Concluída a erradicação, será iniciada a fase de recuperação pela Equipe de Resposta a Incidentes de Segurança da Informação, com a:

I.

- Iniciação dos serviços impactados conforme o Plano de Continuidade de Negócio, caso exista;

II.

- Restauração da integridade do sistema, considerando a sua recuperação correta e a ativação de todas as funcionalidades;

III.

- Restauração do último e íntegro backup completo armazenado.

Art. 27. A Equipe de Resposta a Incidentes de Segurança da Informação deverá realizar uma análise com o objetivo de verificar a ocorrência de perdas de dados relevantes e a identificação de maneiras de recuperá-los, através de procedimentos de segurança.

CAPÍTULO VII - DO MONITORAMENTO DAS RESPOSTAS

Art. 28. O **Plano de Resposta ao Incidente** deverá ser atualizado dinamicamente pela Equipe de Resposta a Incidentes de Segurança da Informação a partir das informações coletadas até o momento ou diante do acontecimento de novos episódios.

Art. 29. O **Plano de Resposta ao Incidente** deverá estar acessível ao Comitê Deliberativo de Gestão (CDG) , à AECI e ao Encarregado de Dados Pessoais, caso o incidente envolva dados pessoais, para fins de apoio técnico e monitoramento contínuo das ações planejadas.

Art. 30. Todas as medidas tomadas na execução do **Plano de Resposta ao Incidente** deverão ser documentadas pela Equipe de Resposta a Incidentes de Segurança da Informação, com a indicação das justificativas, restrições e riscos.

Art. 31. O Gestor de Processo será informado pela Equipe de Resposta a Incidentes de

Segurança da Informação dos resultados após o incidente ter sido considerado resolvido.

Art. 32. A Equipe de Resposta a Incidentes de Segurança da Informação ficará responsável pela gestão e monitoramento dos **Planos de Resposta a Incidentes** abertos na SCGE.

CAPÍTULO VIII - DAS LIÇÕES APRENDIDAS

Art. 33. Após a confirmação da resolução do incidente, a Equipe de Resposta a Incidentes de Segurança da Informação deverá analisar as evidências encontradas, avaliar as ações tomadas e, após consulta às partes interessadas, definir medidas técnicas e ajustes organizacionais necessários para a promoção de melhorias no ambiente de segurança da informação da SCGE, tais como:

I. **-** Definição de medidas de segurança para evitar novos comprometimentos;

II. **-** Elaboração e atualização de Procedimentos Padrões de Respostas a Incidentes;

III. **-** Capacitação da Equipe de Resposta a Incidentes de Segurança da Informação em função da identificação de características específicas de incidentes;

IV. **-** Treinamento dos funcionários da SCGE no tema de segurança da informação;

V. **-** Desenvolvimento de estatísticas e métricas relativas ao processo de resposta a incidentes;

Art. 34. Ao final dos trabalhos, a Equipe de Resposta a Incidentes de Segurança da Informação deverá elaborar um relatório técnico consolidado, contendo:

I.

- Histórico da ocorrência, com informações resumidas de como e quando o incidente aconteceu;

II.

- Extrato da avaliação técnica realizada na fase de avaliação e decisão estratégica;

III.

- Ações empreendidas para a contenção dos danos causados e da erradicação dos efeitos;

IV.

- Trabalhos realizados na recuperação dos sistemas afetados;

V.

- Medidas técnicas e institucionais previstas para a prevenção de eventos similares;

VI.

- Informações sobre os dados pessoais afetados e o impacto do incidente aos titulares;

§1º. Uma versão preliminar do relatório deverá ser encaminhada ao Secretário da Controladoria-Geral do Estado e às demais partes envolvidas no **Plano de Resposta a Incidentes de Segurança da Informação**, para que possa haver o compartilhamento de responsabilidades e sugestões de aperfeiçoamentos no documento final.

§2º. A versão final do Relatório Técnico Consolidado deverá ser submetida à aprovação do Comitê Deliberativo de Gestão (CDG)

TÍTULO III - DA NOTIFICAÇÃO DO INCIDENTE ÀS PARTES INTERESSADAS

Art. 35. A depender do tipo de incidente, são considerados autoridades ou grupos de interesses externos ou fóruns que tratam de questões relativas a incidentes de segurança da informação:

I.

- Agência Estadual de Tecnologia da Informação - ATI;

II.

- Delegacia de Polícia de Repressão aos Crimes Cibernéticos - DPCRICI;

III.

- Autoridade Nacional de Proteção de Dados Pessoais - ANPD;

IV.

- Fornecedores dos ativos de informação;

V.

- Titular de Dados Pessoais

Art. 36. A DTCI avaliará a necessidade de enviar cópia do **Relatório Técnico Consolidado** para a ATI, com o objetivo de:

I.

- Manter atualizado o banco de dados estadual de incidentes de Segurança da Informação;

II.

- Melhoria da capacidade geral do Estado de detecção de incidentes e prevenção de novas ocorrências;

Art. 37. A SCGE deverá notificar formalmente a ocorrência do incidente de segurança para todas as partes interessadas, sempre que necessário, nos moldes estabelecidos nas legislações específicas.

§º1. Enquanto controladora de dados pessoais, a SCGE deverá comunicar à Autoridade Nacional de Proteção de Dados e aos titulares de dados, a ocorrência de incidente de segurança que ocasione risco ou dano relevante aos titulares, em atenção ao art. 48 da LGPD.

§2º A DPCRICI deverá ser acionada sempre que a Equipe de Resposta a Incidentes de Segurança da Informação identificar indícios de que o incidente decorreu de conduta deliberada de pessoa natural ou jurídica, em desacordo com a legislação penal aplicável.

Art. 38. As comunicações de incidentes poderão ser realizadas por e-mail, considerando a facilidade de automatização e a escalabilidade na submissão de grandes quantidades de incidentes.

Parágrafo único. Caso a comunicação por e-mail não tenha se mostrado efetiva ou não esteja disponível, utilizar-se-á o telefone ou a elaboração de uma nota de ampla divulgação em meios de comunicação.

Art. 39. Todos os atos, bem como as comunicações realizadas ao longo da execução dos planos de resposta a incidentes, devem ocorrer de maneira sigilosa e preferencialmente através do Sistema Eletrônico de Informação (SEI).

TÍTULO IV - DAS DISPOSIÇÕES FINAIS

Art. 40. A Secretaria da Controladoria-Geral do Estado deverá orientar os funcionários,

terceirizados e fornecedores a não tentar provar fragilidades de segurança da informação suspeitas caso não sejam previamente autorizados.

Art. 41. Esta Instrução de Serviço Interno entra em vigor na data de sua divulgação.

ERIKA GOMES LACET
Secretária da Controladoria-Geral do Estado

ANEXO A - Modelo de Notificação de Evento de Segurança da Informação

ITEM	**ORIENTAÇÃO DA RESPOSTA**
Descrição dos incidentes	Detalhes do fato, indicando questões tais como: Onde ocorreu o incidente; Quem relatou ou descobriu o incidente; Como foi descoberto; situação atual e as condições anteriores; e os impactos causados ou impactos potenciais.
Registro do tempo da ocorrência do incidente	Data e hora em formato GMT na qual o incidente foi identificado. Exemplo: “10:23, 20 de Março de 2021”, caso seja possível identificar.
Local onde originou o incidente	Endereço IP (IPv4 ou IPv6) do dispositivo ou serviço que originou o incidente, caso seja possível identificar.
Logs ou evidências	Indicação em anexo do Processo SEI das porções de log, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente.
Classificação e descrição das informações afetadas (Ref.: Política de Classificação da Informação.)	1. Pública; 2. Restrita (tipo) 3. Sigilosa (tipo)
Tipos de titulares de dados pessoais envolvidos com descrição, caso envolva dados pessoais (Ref.: Inventário de Dados Pessoais)	1. Funcionários; 2. Usuários/Cidadãos (Clientes); 3. Usuários/Cidadãos (Clientes Potenciais); 4. Fornecedores; 5. Prestadores de serviço; 6. Candidatos; 7. Outros.

Tipo de não conformidade ou violação com a descrição das ocorrências de mau funcionamento e/ou mensagens na tela. (Ref.: Art. 6º.)	1. Tentativas, com ou sem sucesso, de ganhar acesso não autorizado a um sistema ou a seus dados; 2. Interrupção indesejada de serviço; 3. Uso não autorizado de um sistema; 4. Modificações do sistema sem o conhecimento ou consentimento prévio de seu responsável técnico; 5. Sistemas desatualizados ou incorretamente configurados, permitindo abuso; 6. Uso abusivo, em desrespeito à política de uso aceitável do provedor de serviço; 7. Outras não conformidades.
Nível de impacto do incidente (Ref.: Art. 7º.)	1 - Grave; 2 - Significativo; 3 - Mínimo.
Motivos da demora, caso a comunicação não tenha sido imediata (Ref.: Art. 8º.)	Justificativas sobre a demora de notificar o incidente.
Informações do contato da área de negócio para contribuir no desempenho das ações de respostas (Ref.: Art. 9º.)	Nome completo, cargo, matrícula, telefone e e-mail.

ANEXO B - Check list do Plano de Resposta a Incidentes de Segurança da Informação

FASE	CHECK LIST	FONTE
- A - DETECÇÃO E NOTIFICAÇÃO	A1. O Gestor do processo comunicou à secretária imediatamente após tomar conhecimento da ocorrência do evento suspeito? Se NÃO, apresentou os motivos da demora?	Art. 8º
	A2. A DTCI realizou uma análise prévia do evento suspeito?	Art. 9º, caput
	A3. O encarregado de dados pessoais e a DTCI notificaram as partes interessadas sobre a ocorrência do Incidente de Segurança da Informação?	Art. 9º, II
	A4. A secretária, quando cabível, acionou a Equipe de Resposta a Incidentes de Segurança da Informação por meio do SEI?	Art. 9º, §1º

	A5. O Gestor de Processo indicou um servidor da área de negócio para auxiliar a Equipe de Resposta a Incidentes de Segurança da Informação no tratamento do incidente?	Art. 11
- B - AVALIAÇÃO E DECISÃO ESTRATÉGICA	B1. A Equipe de Resposta a Incidentes de Segurança da Informação elaborou a Proposta Inicial de Resposta ao Incidente de acordo com as regras contidas nesta PRI?	Art. 12
	B2. A Equipe de Resposta a Incidentes de Segurança da Informação realizou a Avaliação Técnica do Incidente de acordo com o art. 16 desta PRI?	Art. 15
- C - PREPARAÇÃO	C1. A Equipe de Resposta a Incidentes de Segurança da Informação elaborou o Plano de Resposta ao Incidente no prazo máximo de 3 dias da aprovação da Proposta Inicial de Resposta ao Incidente ?	Art. 18
	C2. A Equipe de Resposta a Incidentes de Segurança da Informação elabora e mantém atualizados Procedimentos Padrões de Respostas relacionados aos principais tipos de incidente enfrentados pelo Órgão?	Art. 19
- D - CONTENÇÃO	D1. A Equipe de Resposta a Incidentes de Segurança da Informação conseguiu isolar problema? Todos os sistemas afetados estão isolados dos sistemas não afetados?	Art. 21, I
	D2. A Equipe de Resposta a Incidentes de Segurança da Informação tomou medidas instantâneas de contenção, mesmo antes da notificação pelo Gestor de Processo?	Art. 22
	D3. A Equipe de Resposta a Incidentes de Segurança da Informação informou o Gestor de Processo sobre as medidas iniciais de contenção tomadas?	Art. 23

	D4. Foram criadas cópias dos arquivos e sistemas afetados pelo incidente (“cópias forenses”) para análise posterior? Tais cópias estão armazenadas em local seguro?	Art. 24
	D5. A Equipe de Resposta a Incidentes de Segurança da Informação, no caso de os sistemas precisarem permanecer em produção, removeu todos os malwares, e outros artefatos que viabilizaram o ataque, com vistas a fortalecer os sistemas afetados contra novos ataques até que uma circunstância ideal permita sua restauração completa?	Art. 21, II
- E - ERRADICAÇÃO	E1. Todos os malwares e outros artefatos deixados pelos invasores foram removidos pela Equipe de Resposta a Incidentes de Segurança da Informação, e os sistemas afetados estão protegidos contra novos ataques?	Art. 25
- F - RECUPERAÇÃO	F1. O Órgão procedeu com a prestação dos serviços impactados, inclusive de acordo com um Plano de Continuidade dos Negócios, caso existente?	Art. 26, I
	F2. Os sistemas afetados foram corrigidos e protegidos contra o ataque recente e, na medida do possível, contra ataques futuros?	Art. 26, II
	F3. A Equipe de Resposta a Incidentes de Segurança da Informação considerou a ocorrência de eventuais perdas de dados relevantes e, como contramedida, empreendeu medidas para a recuperação de tais informações, tais como a restauração de cópias de segurança?	Art. 27
- G - MONITORAMENTO DAS RESPOSTAS	G1. O Plano de Resposta ao Incidente encontra-se atualizado e disponível a todos os atores envolvidos no Plano de Resposta a Incidentes de Segurança da Informação?	Art. 28
	G2. A Equipe de Resposta a Incidentes de Segurança da Informação comunicou o Gestor de Processo sobre os resultados após o incidente ter sido considerado resolvido?	Art. 31

- H - LIÇÕES APRENDIDAS	H1. Toda a documentação necessária do incidente foi escrita? Se SIM, a Equipe de Resposta a Incidentes de Segurança da Informação gerou o Relatório Técnico Consolidado? Se não, tenha a documentação escrita o mais rápido possível antes que qualquer informação seja perdida e deixada de fora do relatório.	Art. 34
	H2. O Relatório Técnico Consolidado contempla as informações previstas no art. 34 desta PRI?	Art. 34, caput
	H3. Uma versão preliminar do relatório foi encaminhada ao Secretário da Controladoria-Geral do Estado e às demais partes envolvidas no **Plano de Resposta a Incidentes de Segurança da Informação**?	Art. 34, P.U

Documento assinado eletronicamente por **Erika Gomes Lacet**, em 30/07/2024, às 16:33, conforme horário oficial de Recife, com fundamento no art. 10º, do Decreto nº 45.157, de 23 de outubro de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.pe.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **50342601** e o código CRC **05FAF508**.

SECRETARIA DA CONTROLADORIA GERAL DO ESTADO

Rua Santo Elias, 535, - Bairro Espinheiro, Recife/PE - CEP 52020-095, Telefone: 3183-0800