PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA

1. Considerações Iniciais

O presente Plano de Resposta a Incidentes de Segurança dá-se em cumprimento à Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), a qual determina a obrigação dos agentes de tratamento, dentre eles o Controlador (a exemplo desta autarquia), em "*adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito*", conforme Art. 46, *caput*, daquele diploma.

Orienta-se, este plano, no Guia de Resposta a Incidentes de Segurança, versão 2.0 (dezembro de 2021), expedido pelo Ministério da Economia, à luz do Princípio da Cooperação que deve reger a relação entre os órgãos públicos em nosso país, haja vista a necessária Eficiência (Art. 37, *caput*, da CF/1988).

2. Objetivos

O PRIS tem por objetivo orientar esta autarquia, quando da eventualidade de incidentes de segurança envolvendo dados pessoais, visando à rápida identificação da ocorrência havida, estabelecendo parâmetros procedimentais na atuação da Casa Médica quanto à confirmação do ocorrido, assim como quanto à contenção, erradicação e superação das eventuais falhas detectadas.

Neste sentido, objetivando à rápida resposta institucional, assim como ao cumprimento das obrigações decorrentes da LGPD, inclusive quanto à comunicação ao titular envolvido e à Autoridade Nacional de Proteção de Dados (ANPD), nas hipóteses previstas na legislação.

3. Atores Envolvidos

3.1. Notificador: pessoa, física ou jurídica, ou sistema de monitoramento que notifica o incidente.

3.2. Encarregado: funcionário indicado pela autarquia com a competência legal prevista na LGPD, incluindo a atuação como canal de comunicação entre o órgão, os titulares de dados e a ANPD, assim como quanto à orientação da entidade a respeito das práticas a serem adotadas em relação à proteção de dados pessoais.

3.3. Responsável Pelo Sistema: o Coordenador da TI ou outro funcionário a ser designado pela Diretoria da Casa, com conhecimentos técnicos, apto a propor soluções, autorizar ou vetar procedimentos de emergência.

3.4. Time de Resposta a Incidentes (TRI): grupo de funcionários do Conselho, com acessos, habilidades e conhecimentos para responder aos incidentes havidos. **O TRI será designado de acordo com as especificidades de cada incidente, sendo composto pelo Responsável Pelo Sistema e por funcionários por ele indicados** que detenham capacidades aptas à atuação na apuração e solução das ocorrências atinentes ao incidente.

Poderão ser inclusos no TRI funcionários de outras áreas, a serem designados pela Diretoria da Casa, conforme seu juízo de conveniência e oportunidade, visando à melhor abordagem em face do incidente havido.

O Encarregado deverá ser informado, sempre que necessário, de todas as medidas relevantes adotadas pelo TRI, para efetuar as possíveis orientações no plano jurídico, à luz do Art. 41, § 2º, III, da LGPD.

3.5. Comitê de Resposta a Incidentes (CRI): grupo formado pelo Responsável Pelo Sistema, pelo Encarregado e por terceiro integrante a ser designado pela Diretoria da Casa, a fim de promover as deliberações necessárias na abordagem ao incidente.

É também sua atribuição avaliar – posteriormente à ocorrência do incidente – as eventuais falhas havidas, os procedimentos adotados e as soluções possíveis, visando a encaminhar à Diretoria da Casa propostas de medidas futuras com a finalidade de excluir ou minorar os riscos geradores do incidente.

4. Conceitos Aplicáveis

Para os fins do presente plano de resposta, "**dado pessoal**" é "*toda informação relacionada a pessoa natural identificada ou identificável*". "**Incidente de segurança**" é "*qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores*", assim como de todo e qualquer banco de dados pessoais administrado por este órgão público.

Deste modo, "**incidente de segurança com dados pessoais**" é "*qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação de dados pessoais, sendo acesso não autorizado, acidental ou ilícito que resulte em destruição, perda, alteração vazamento ou qualquer forma de tratamento de dados ilícita ou inadequada, que tem a capacidade de pôr em risco os direitos e as liberdades dos titulares dos dados pessoais*".

A "**notícia do fato**" consiste no relatório inicial de triagem, quando da suspeita de incidente, oriunda de notificador externo ou através de conhecimento de ofício por parte desta autarquia, através de qualquer um de seus funcionários ou colaboradores (notificador interno).

O "**relatório técnico**" é o relatório confeccionado pela TRI, a ser encaminhado ao CRI após a solução do ocorrido, contendo informações técnicas apuradas quando do enfrentamento ao incidente.

O "**relatório conclusivo**" é o relatório final quanto ao incidente, a ser confeccionado pelo CRI e direcionado à Diretoria da Casa, o qual deverá indicar resumo dos fatos, dando ênfase em sugestões e melhorias a serem adotadas visando ao aprimoramento do tratamento de dados pessoais no Conselho.

5. Roteiro de Procedimentos

5.1. Identificação: o possível incidente é noticiado por terceiro, alheio ao Conselho, ou identificado pela estrutura interna da autarquia, seja através dos funcionários responsáveis pelo Setor, seja por sistemas de informática próprios.

A comunicação deverá se dar através do contato de *e-mail* do Encarregado, constante do *site* do Conselho, ou através de todo e qualquer meio possível, incluso telefones, *e-mails*, etc.

A comunicação por via diversa daquela direta ao Encarregado em hipótese alguma será considerada como motivo para seu não conhecimento.

5.2. Triagem: uma vez sendo noticiado o possível incidente, o mesmo será formalizado, em notícia do fato, pelo funcionário que dele tomar ciência, ou por seu superior imediato, descrevendo-se os fatos relacionados e coletando os dados pessoais (nome, CPF/CNPJ, endereço e *e-mail*) aptos a identificar o noticiante, para posterior comunicações, caso se trate de notificador externo.

5.2.1. Acaso a suspeita de incidente se verifique de ofício, por parte do quadro de pessoal desta Casa, ou através de seus sistemas de informática próprios (notificador interno), o mesmo será formalizado, em notícia do fato, pelo funcionário que dele tomar ciência, ou por seu superior imediato, descrevendo-se os fatos relacionados.

5.2.2. Após, a notícia do fato, deverá ser encaminhada ao Responsável Pelo Sistema, ao Encarregado e à Diretoria da Casa, para que tomem ciência dos fatos relatados.

5.2.3. Uma vez recebida a notícia do fato, de plano, o Responsável Pelo Sistema deverá nomear os demais funcionários e colaboradores para a formação do TRI, noticiando ao Encarregado e à Diretoria da Casa o quadro por ele formado para eventual inclusão de funcionários e colaboradores de outras áreas, conforme exista a necessidade à luz das especificidades do caso concreto.

5.2.4. Composto o TRI, o grupo deverá – de imediato – avaliar os fatos relatados, atendo-se com especial ênfase na análise **preliminar** quanto à veracidade da ocorrência, os sistemas alcançados pelo evento, a dinâmica do incidente, os eventuais prejudicados com o ocorrido, os dados pessoais envolvidos no incidente, a gravidade da vulneração ocorrida, além da possibilidade de agravamento do infortúnio.

5.2.5. Sendo possível a sustação sumária da vulneração havida, o TRI deverá atuar de moto-próprio, promovendo as medidas que – à luz de seu conhecimento técnico – fizerem-se necessárias para o imediato encerramento do incidente.
Referida atuação deverá ser determinada pelo Responsável Pelo Sistema, em havendo urgência ou possibilidade de imediata sustação do incidente, independente das medidas formais previstas neste tópico (itens 5.2 a 5.2.4), o que poderá ser efetuado posteriormente à bem do Princípio da Eficiência (Art. 37, *caput*, da CF/1988).

5.3 Avaliação: na hipótese do item 5.2.5, após solvido o incidente de segurança, de forma sumária, deverá ser formalizado o relatório técnico do TRI, de que trata o item 5.5, sendo o mesmo encaminhada ao CRI para a confecção de relatório conclusivo, nos termos dos itens 5.5.1 e 5.5.2, o qual posteriormente deverá ser encaminhado à Diretoria da Casa, para deliberação, nos termos do item 5.5.3.
5.3.1. Não sendo possível atuação sumária por parte do TRI (item 5.2.5), a notícia do fato, acompanhada de breve relatório do ocorrido, deverá ser apreciada de imediato pelo CRI, o qual deverá atuar de plano, nos moldes que entender adequado para o enfrentamento do caso concreto, ainda que não tenha ocorrido a indicação do terceiro integrante por parte da Diretoria da Casa, como previsto no item 3.5, o que poderá ser efetuado posteriormente.
5.3.2. O CRI deverá determinar ao TRI que apure a irregularidade ocorrida (*spam*, vírus, atuação de hacker, compartilhamento indevido de dados, etc), coletando informações aptas à determinação e à identificação das irregularidades havidas, incluso a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas.
5.3.4. Uma vez identificada a modalidade da irregularidade, o TRI deverá apurar os dados levantados buscando definir a "**gravidade do impacto**" do incidente, adotando os seguintes parâmetros:

Alta: A organização não é mais capaz de fornecer tratamentos de dados pessoais, com a devida segurança, à integralidade dos titulares abrangidos por sua atuação.

Média: A organização perdeu a capacidade de fornecer tratamentos de dados pessoais, com a devida segurança, a um subconjunto dos titulares abrangidos por sua atuação.

Baixa: Efeito mínimo; a organização ainda pode fornecer tratamentos de dados pessoais, com segurança, para titulares abrangidos por sua atuação, mas foi identificada ineficiência pontual a ser combatida ou incidente que atinge número pequeno de titulares envolvidos.

5.3.5. O TRI deverá identificar, para cada eventual irregularidade identificada (item 5.3.2), a "**recuperalidade**" da higidez do sistema, considerando os recursos disponíveis e a relevância do incidente para a organização.

5.3.6. Em havendo várias irregularidades identificadas no incidente, o TRI deverá formalizar ordem de prioridade para o enfrentamento das mesmas, em juízo equânime que considere a "**gravidade do impacto**" e a "**recuperalidade**", conforme itens 5.3.4 e 5.3.5.

5.4. Contenção, Erradicação e Recuperação: evidenciado o incidente de segurança, deverá ser determinado o imediato isolamento e a suspensão dos sistemas ou das funcionalidades abrangidas, visando à cessação da continuidade do dano à segurança de dados pessoais. A medida será adotada por determinação do CRI, ou diretamente por deliberação do próprio Responsável Pelo Sistema, caso necessário.

5.4.1. Caberá ao TRI, obrigatoriamente, adotar medidas que impeçam que o isolamento e a suspensão dos sistemas ou das funcionalidades abrangidas ocasione a exclusão de dados e evidências necessárias à identificação da(s) irregularidade(s) ocorrida(s).

5.4.2. Segundo sua avaliação técnica, o TRI deverá adotar as demais medidas de contenção, erradicação e recuperação do incidente, as quais julgar necessárias, ainda que não referidas nas determinações do CRI, informando-o de forma justificada posteriormente.

5.4.3. Segundo sua avaliação técnica, o TRI deverá adotar as medidas de erradicação que julgar necessárias, ainda que não referidas nas determinações do CRI, informando-o de forma justificada posteriormente.

As medidas de erradicação poderão abranger a eliminação de resquícios do incidente, como exclusão de *malware*, exclusão de contas violadas, identificação e tratamento das vulnerabilidades exploradas, dentre outras que se mostrarem necessárias.

5.4.4. Durante a erradicação, o TRI deverá identificar todos os recursos da organização que foram atingidos, assim como os que possam ser corrigidos.

5.4.5. Durante a recuperação, o TRI deverá restaurar os sistemas envolvidos para seu estado normal, cabendo aos administradores dos sistemas confirmar se tais sistemas estão operando de maneira adequada.

A recuperação pode envolver ações como alteração de senhas de rede, reconfiguração de regras de *firewall*, restauração de *backup*, reconstrução de sistemas e de toda base de dados, instalação de *patches* de segurança, substituição de arquivos corrompidos por versões limpas, dentre outras medidas que o TRI julgar adequadas.

5.4.6. O TRI deverá – sempre que possível – identificar a origem das irregularidades evidenciadas durante o tratamento de incidentes, o que deverá constar do relatório técnico (item 5.5). Não obstante, dando prioridade a contenção, erradicação e recuperação relacionada ao incidente.

5.5. Atividades Pós-Incidente e Lições Aprendidas: após a fase de Contenção, Erradicação e Recuperação, o TRI deverá confeccionar relatório técnico detalhado quanto ao diagnóstico do incidente ocorrido, englobando:

a. A modalidade da(s) irregularidade(s) detectadas(s) (*spam*, vírus, atuação de hacker, compartilhamento indevido de dados, etc).

b. Dados relacionados ao incidente, a exemplo de endereços IP, credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, dentre outras.

c. A causa do incidente.

d. A gravidade do impacto (item 5.3.4).

e. A ordem de prioridade para o enfrentamento das irregularidades envolvidas no incidente, justificando-as (item 5.3.6).

f. As medidas de **Contenção, Erradicação e Recuperação** adotadas para o enfrentamento do incidente.

5.5.1. O relatório técnico do TRI deverá ser encaminhado ao CRI o qual ficará responsável por confeccionar relatório conclusivo, ao qual ficará anexado o relatório técnico, dando ênfase às medidas que entender adequadas para a exclusão do risco quanto à ocorrência de novos incidentes, incluindo sugestões e melhorias a serem adotadas visando ao aprimoramento do tratamento de dados pessoais no Conselho, à luz da LGPD.

5.5.2. O relatório conclusivo do CRI deverá tratar também, obrigatoriamente, da eventual necessidade de comunicação à autoridade nacional e ao titular envolvido, quanto à ocorrência do incidente de segurança, o que é imperativo caso a ocorrência possa acarretar risco ou dano relevante aos titulares (Art. 48, *caput*, da LGPD).

5.5.3. O relatório conclusivo do CRI deverá ser encaminhado à Diretoria da Casa para deliberação quanto às medidas e sugestões propostas pelo CRI.