Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Política e Plano de Resposta a Incidentes de Segurança

Objetivo

Estabelecer um conjunto de processos e procedimentos para detectar, relatar, avaliar, responder, lidar e aprender com incidentes de segurança da informação, buscando satisfazer os requisitos de boa governança de segurança da informação contidos no art. 50, inciso I, alínea “g” da Lei Geral de Proteção de Dados Pessoais – LGPD.

Visão geral

Um Incidente de Segurança da Informação pode ser definido como qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.

1. Incidentes de Segurança da Informação

Um incidente de segurança com dados pessoais é qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação na segurança de dados pessoais, tais como acesso não autorizado, acidental ou ilícito que resulte na destruição, perda, alteração, vazamento ou ainda, qualquer forma de tratamento de dados inadequada ou ilícita, os quais possam ocasionar risco para os direitos e liberdades do titular dos dados pessoais.

EMBRASI

Políticas e Normas.

Segurança da Informação

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

O art. 47 da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados – LGPD) determina que os agentes de tratamento de dados pessoais devem 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.

2. Identificação de Incidentes de Segurança

Para a identificação das causas do incidente de segurança da informação, devem existir mecanismos de detecção e reporte que incluem, mas não se limitam a:

- Designação de uma equipe específica para atender a eventos e incidentes de segurança da informação;
- Instalação adequada de softwares antivírus e de *firewall*, segundo o disposto na Política de Antivírus e *Malware* e na Política de *Firewall*;
- Manutenção de canais de suporte nas plataformas e sistemas externos e internos da Instituição;
- Observação de mecanismos de controle e revisão contidos nas Políticas e Normas Gerais da Instituição.

Toda notificação de eventos ou incidentes de Segurança da Informação deve possuir identificação numérica única e ser formalmente registrada em um banco de dados específico, conforme Política de Registro em Sistemas de Informação da Instituição.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

Após o registro de qualquer evento ou incidente de Segurança da Informação, a equipe responsável deve concluir pela existência ou inexistência do evento ou incidente, seja ele externo ou interno.

3. Categorização e Triagem de Incidentes de Segurança

Concluindo-se pela existência do evento ou incidente de segurança da informação, a equipe responsável deve realizar a análise adequada para a classificação, categorização, e definição de prioridades acerca daquele evento ou incidente de segurança da informação.

A equipe responsável deve seguir as seguintes diretrizes na classificação, categorização e priorização de eventos e incidentes de segurança da informação:

- Coleta e análise das provas e documentações pertinentes;
- Confirmação da relevância do evento ou incidente nas atividades da Instituição;
- Classificação do evento ou incidente nas seguintes categorias:
  a. Evento: inclui situações cotidianas, tratadas com gestão de riscos e alternativas operacionais;
  b. Incidente: inclui situações que causem indisponibilidade relevante para as atividades da Instituição, afetando alguns dos três pilares da segurança da informação, tratadas com procedimentos de continuidade dos negócios;

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

c. Emergência: inclui situações que causem um alto impacto econômico ou reputacional para a Instituição, tratadas com procedimentos de gestão de crises.

- Apresentação de um plano de ação preliminar contendo as medidas primordiais que deverão ser tomadas e quais destas medidas serão priorizadas.

4. Mitigação de Incidentes de Segurança

Apresentado o plano de ação pela equipe responsável, deve-se proceder com a comunicação a todos os agentes relevantes e também aos responsáveis pelas áreas afetadas dentro da Instituição.

Nesta fase de mitigação, a equipe responsável deverá realizar todas as análises pertinentes acerca do incidente de segurança da informação, incluindo:

(i) Análise das informações disponíveis;
(ii) Pesquisas de resolução;
(iii) Proposição de ações para contenção e mitigação de danos;
(iv) Comunicação interna com colaboradores, diretoria, gerência, coordenação ou líderes;
(v) Comunicação externas com as autoridades, parceiros, consumidores, clientes, fornecedores;
(vi) Elaboração de procedimentos de recuperação.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

A equipe deve necessariamente buscar a erradicação da causa-raiz do incidente. Deve-se assegurar que o recurso atingido esteja seguro e confiável, a fim de que os procedimentos para a sua recuperação sejam iniciados.

A equipe deve documentar e arquivar as conclusões da resposta ao incidente, incluindo:

a. informações sobre o ocorrido;
b. data da ocorrência.
c. pessoa que identificou;
d. a forma de detecção;
e. as medidas tomadas pela equipe para a correção e a mitigação de danos;
f. o status do incidente;
g. quaisquer outros dados coletados durante o processo de remediação;
h. a categorização final do incidente;
i. comentários e sugestões de melhoria.

5. Resposta a Incidentes de Segurança

Após a documentação da resposta ao incidente de segurança da informação, a equipe deve proceder com a elaboração de um relatório final, contendo a classificação final e todas as evidências coletadas.

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

As evidências devem ser armazenadas em repositório no banco de dados da Instituição para futuras auditorias, conforme descrito em Política de Registros de *Logs* da Instituição.

Após todas as providências descritas acima, a equipe deve encerrar a ocorrência nos registros pertinentes e comunicar as suas conclusões para os agentes internos e externos da Instituição, de acordo com a necessidade.

6. Período Posterior ao Incidente de Segurança da Informação

A equipe ou qualquer outra pessoa dentro da Instituição poderá propor melhorias para evitar ou mitigar a recorrência do incidente de Segurança da Informação, com o fim de fortalecer a segurança dos ativos da Instituição. Da mesma forma, devem ser comunicadas todas as outras áreas da Instituição acerca da ocorrência do incidente.

7. Reporte à Agência Nacional de Proteção de Dados – ANPD e ao Titular de Dados

O art. 48 da LGPD determina que é obrigação do controlador comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Recomenda-se que os controladores adotem posição de cautela, de modo que a comunicação seja efetuada mesmo nos casos em que houver dúvida sobre a

Assunto: Governança de Segurança da Informação e Proteção de Dados Pessoais		
Versão: 1.0	Data de Publicação:	Data de Expiração: Anual
Autor:		

relevância dos riscos e danos envolvidos. Ressalte-se, ainda, que eventual e comprovada subavaliação dos riscos e danos por parte dos controladores pode ser considerada descumprimento à legislação de proteção de dados pessoais.

O prazo para informar o incidente encontra-se pendente de regulamentação. recomenda-se que após a ciência do evento adverso e havendo risco relevante, a ANPD seja comunicada com a maior brevidade possível, sendo recomendado o prazo de 2 dias úteis, contados da data do conhecimento do incidente.

Para mais informações sobre os procedimentos a serem tomados na ocorrência de incidentes de segurança, recomenda-se o acesso à página https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca.