TecnoTech
Sistemas

POLÍTICA DE RESPOSTA A INCIDENTES E PROCEDIMENTOS

PROGRAMA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

Tecnotech Sistemas

Felipe Santos de Andrade / Wanderson Camara dos Santos

Política de respota a incidentes e procedimentos

Versão 1.0

Tecnotech Sistemas

Diretoria de Implementação e Projetos

Política criada sob a supervisão de

Romney Dutra / Lucas Diniz - Prolinx

Março de 2023

Abreviaturas e siglas

Dados pessoais sensíveis: São informações que se referem à intimidade, privacidade e liberdade das pessoas, como origem racial ou étnica, convicção religiosa, orientação sexual, informações médicas, genéticas ou biométricas, filiação política ou sindical, número do seguro social, número de cartão de plano de saúde e informações bancárias.

Incidente: Refere-se a qualquer evento que possa comprometer a segurança ou a privacidade das informações, incluindo acessos não autorizados, vazamento de dados, perda, destruição ou modificação indevida de informações.

IP: Protocolo da Internet é um número exclusivo que identifica um dispositivo em uma rede, permitindo sua comunicação com outros dispositivo.

Log: Processo de registro de eventos relevantes em um sistema computacional, incluindo acesso, uso ou modificação de dados.

Operador: Pessoa física ou jurídica que realiza o tratamento de dados em nome do controlador, seguindo suas instruções.

Tratamento: Refere-se a qualquer operação realizada com dados pessoais, incluindo coleta, armazenamento, uso, acesso, compartilhamento, transferência, exclusão ou nonimização.

Vazamento de dados: É a exposição não autorizada de informações confidenciais ou pessoais, seja por meio de ataques cibernéticos, falhas de segurança ou ações mal-intencionadas de terceiros.

Violação de privacidade: Refere-se a qualquer ação que comprometa a segurança ou privacidade das informações pessoais, incluindo acessos não autorizados, modificação, roubo ou perda de dados.

Vírus: Programa de computador malicioso que se propaga e infecta outros programas e arquivos, podendo causar danos aos sistemas ou roubar informações pessoais.

Dados pessoais: Refere-se a qualquer informação relacionada a uma pessoa física, como nome, endereço, e-mail, número de telefone, entre outros.

Controlador: Pessoa física ou jurídica responsável pelas decisões referentes ao tratamento de dados pessoais.

Autoridade Nacional de Proteção de Dados (ANPD): Órgão responsável pela fiscalização e garantia do cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro.

Anonimização: É o processo pelo qual os dados pessoais são tornados irreversivelmente anônimos, de modo que não possam mais ser associados a um indivído.

Agentes de tratamento: efere-se ao conjunto formado pelo Controlador e Operador, responsáveis pelo tratamento de dados pessoais.

Engenharia social: Técnica utilizada por criminosos virtuais para obter informações confidenciais ou acesso a sistemas, através da manipulação psicológica de usuários desavisados.

Conteúdo

Lista de Tabelas 7

1 INTRODUÇÃO 8

2 OBJETIVOS 9

3 O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS? 10

4 OS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS PODEM SER DE VÁRIOS TIPOS, INCLUINDO 12

5 PAPÉIS E RESPONSABILIDADES 14

5.1 NOTIFICADOR 14

5.2 EQUIPE DE RESPOSTA A INCIDENTES 15

5.3 DESENVOLVEDORES E OPERADORES 15

5.4 DATA PROTECTION OFFICER 16

6 DETECÇÃO DO INCIDENTE 17

7 FLUXOGRAMA 18

8 GRAVIDADE DO INCIDENTE 19

9 PROCEDIMENTOS PARA RESPOSTA 20

9.1 NOTIFICAÇÃO DO INCIDENTE 20

9.2 DETERMINAR SE OCORREU O INCIDENTE 21

9.3 CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO 22

9.4 CONTENÇÃO 22
9.5 ERRADICAÇÃO 23
9.6 RESTAURAÇÃO 23
9.7 DOCUMENTAÇÃO DO INCIDENTE 23
9.8 COMUNICAÇÃO PÓS INCIDENTE DE SEGURANÇA 24

10 MUDANÇAS NA POLÍTICA **25**

11 CONTROLE DE VERSÕES **26**

12 CONCORDÂNCIA **27**

Lista de Tabelas

11.1 Tabela de versões 26

Capítulo 1

INTRODUÇÃO

A política de respostas a incidentes é um conjunto de orientações, regras e procedimentos que a equipe de respostas a incidentes da tecnotech segue. Seu objetivo principal é garantir uma resolução rápida dos incidentes e fornecer um atendimento eficiente aos usuários, minimizando os impactos nos negócios e serviços prestados.

Capítulo 2

OBJETIVOS

ste documento tem como objetivo estabelecer as funções e responsabilidades da equipe de resposta da tecnotech, bem como as medidas a serem tomadas em caso de incidentes envolvendo dados pessoais. A tecnotech tem como prioridade a integridade dos sistemas, a proteção dos dados pessoais e a privacidade dos seus titulares, para manter a confiabilidade de seus produtos e serviços. É importante destacar que o conceito de dados pessoais compreende todas as informações que possam viabilizar a identificação de uma pessoa física. Também estão compreendidas as informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, informações referentes à saúde ou à vida sexual, dados genéticos ou biométricos e quaisquer dados que, quando tratados de forma combinada com outras informações, possam permitir inferir informações dessa natureza (dados sensíveis).

Política de resposta a incidentes da tecnotech se aplica a qualquer caso de incidentes envolvendo dados pessoais e deverá ser cumprido por todas as áreas e colaboradores da Empresa, incluindo os sócios, diretores, empregados e prestadores de serviços e parceiros que, no âmbito de suas relações com a tecnotech, possam ter acesso às informações e dados pessoais dos titulares. O objetivo é garantir que a tecnotech responda adequadamente a um incidente, sempre prezando pela integridade dos sistemas, proteção dos dados pessoais e privacidade dos titulares.

Capítulo 3

O QUE É UM INCIDENTE DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS?

Um incidente de segurança da informação envolvendo dados pessoais é qualquer evento que comprometa a confidencialidade, integridade ou disponibilidade desses dados. Ele pode ocorrer de diversas formas, como por exemplo, o acesso não autorizado a informações, perda ou destruição de dados, divulgação indevida ou roubo de informações pessoais

Os incidentes podem ter origem em ações maliciosas, como ataques hackers ou phishing, ou podem ser decorrentes de falhas técnicas ou humanas, como erros de configuração ou de operação de sistemas. Em todos os casos, é importante que sejam tratados de forma adequada, para minimizar os danos e evitar a ocorrência de novos incidentes no futuro.

ara proteger os dados pessoais de seus clientes e usuários, a tecnotech adota medidas de segurança adequadas, como criptografia, autenticação forte, monitoramento de atividades suspeitas e backups frequentes. Além disso, contar com um plano de resposta a incidentes, que permita identificar e avaliar a gravidade dos incidentes, notificar as autoridades competentes e tomar as medidas necessárias para mitigar os riscos e garantir a segurança dos dados envolvidos.

A Lei Geral de Proteção de Dados (LGPD) estabelece que as empresas devem manter um registro de todos os incidentes de segurança que envolvam dados pessoais, e que esses incidentes devem ser comunicados às autoridades competentes e aos titulares dos dados afetados, de forma clara e transparente.

Dessa forma, é fundamental que as empresas estejam preparadas para lidar com incidentes de segurança da informação, garantindo a proteção dos dados pessoais de seus clientes e usuários.

Capítulo 4

OS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO ENVOLVENDO DADOS PESSOAIS PODEM SER DE VÁRIOS TIPOS, INCLUINDO

Vazamento de Dados Pessoais: Refere-se à situação em que Dados Pessoais são expostos e disponibilizados de forma indevida, seja por meio físico ou digital, a um número indeterminado de pessoas, tanto no Brasil quanto em qualquer outro país. Esse incidente pode resultar em graves consequências, como a perda da privacidade e da segurança dos dados pessoais afetados.

Negação de Serviço: Trata-se de um Incidente em que o acesso lógico ou físico a um sistema que armazena Dados Pessoais é prejudicado ou impossibilitado, comprometendo a integridade dos dados afetados de forma permanente, uma vez que o acesso fica indisponível. Esse incidente pode ter origem em ataques cibernéticos ou falhas técnicas.

Acesso Não Autorizado: Refere-se ao Incidente em que o acesso lógico ou físico a um sistema que contém Dados Pessoais é tentado ou obtido sem a devida autorização para tal acesso. Qualquer tipo de acesso que não tenha sido concedido, como conexão, leitura, gravação, autenticação, modificação, eliminação ou criação, é considerado um acesso não autorizado.

Uso Inapropriado: efere-se ao Incidente em que ocorre a violação das políticas de uso de dados, informações e sistemas da Empresa, incluindo a Política de Privacidade e de Segurança da Informação. Isso pode acontecer devido a ações maliciosas ou negligentes de funcionários, prestadores de serviços ou outras pessoas que tenham acesso aos dados pessoais.

Capítulo 5

PAPÉIS E RESPONSABILIDADES

5.1 NOTIFICADOR

notificação de um novo incidente pode ser feita por qualquer pessoa interna ou externa à tecnotech, ou ainda através de um alarme de monitoramento. A comunicação inicial do incidente pode ser feita por diversos meios, como e-mails, ofícios, service desk, telefone ou sistemas internos. Quando se tratar de notificação do titular dos dados pessoais, a comunicação deverá ser feita diretamente pelo Encarregado. É importante que todas as notificações sejam registradas pelo Notificador para fins de documentação e acompanhamento do incidente.

5.2 EQUIPE DE RESPOSTA A INCIDENTES

A Equipe de Resposta a Incidentes é responsável por coordenar a resposta da tecnotech diante de um Incidente de Segurança da Informação envolvendo Dados Pessoais. Suas obrigações incluem:

- **Receber as notificações de Incidentes e realizar uma análise preliminar.**
- **Avaliar a gravidade do Incidente e adotar as medidas necessárias para conter, erradicar seus efeitos.**
- **Garantir a preservação da integridade dos Dados Pessoais afetados pelo Incidente.**
- **Manter registro de todos os Incidentes de Segurança da Informação ocorridos na Empresa, bem como das medidas adotadas para sua solução e contenção.**
- **Monitorar a eficácia das medidas de segurança da informação adotadas pela Empresa e Realizar ajustes quando necessário.**

5.3 DESENVOLVEDORES E OPERADORES

O DEV/OPS é importante nas situações de incidentes de segurança da informação na tecnotech, sendo indicado pela empresa para atuar como um líder na resposta ao incidente. Ele deve possuir conhecimento técnico suficiente para propor soluções de resposta e tomar decisões de forma ágil e precisa. É responsabilidade dele autorizar ou vetar procedimentos de emergência para garantir a proteção dos dados pessoais da empresa. Sua atuação é crucial para minimizar os danos causados pelo incidente e restabelecer a normalidade do sistema de forma segura e eficiente.

5.4 DATA PROTECTION OFFICER

DPO é um membro especial da Equipe de Resposta a Incidentes, com a responsabilidade específica de encaminhar comunicações formais em casos de incidentes que envolvam vazamentos de dados pessoais. O DPO deve ter conhecimento especializado em questões relacionadas à proteção de dados e estar apto a avaliar a extensão do incidente e suas implicações para os titulares dos dados pessoais envolvidos. Realizar a comunicação dos Incidentes de Segurança da Informação às autoridades Competentes e às pessoas afetadas pelo Incidente, quando necessário.

Capítulo 6

DETECÇÃO DO INCIDENTE

Detectar um Incidente rapidamente é fundamental para minimizar os possíveis impactos na empresa. Existem várias maneiras de detectar um Incidente, incluindo invasões de rede, phishing, malware e perda de dados, entre outras. É responsabilidade de todos os colaboradores da tecnotech estar atentos a esses sinais e comunicar imediatamente a Equipe de Resposta a Incidentes caso detectem algo suspeito. A comunicação deve incluir informações como a data e hora da suspeita, tipo de informações envolvidas, causa e extensão do Incidente e qualquer outra informação relevante que possa ajudar na compreensão do evento. É importante lembrar que a falta de comunicação sobre um Incidente suspeito pode resultar em sanções disciplinares para o colaborador, dependendo da gravidade do incidente e da comprovação de negligência.

Capítulo 7

FLUXOGRAMA

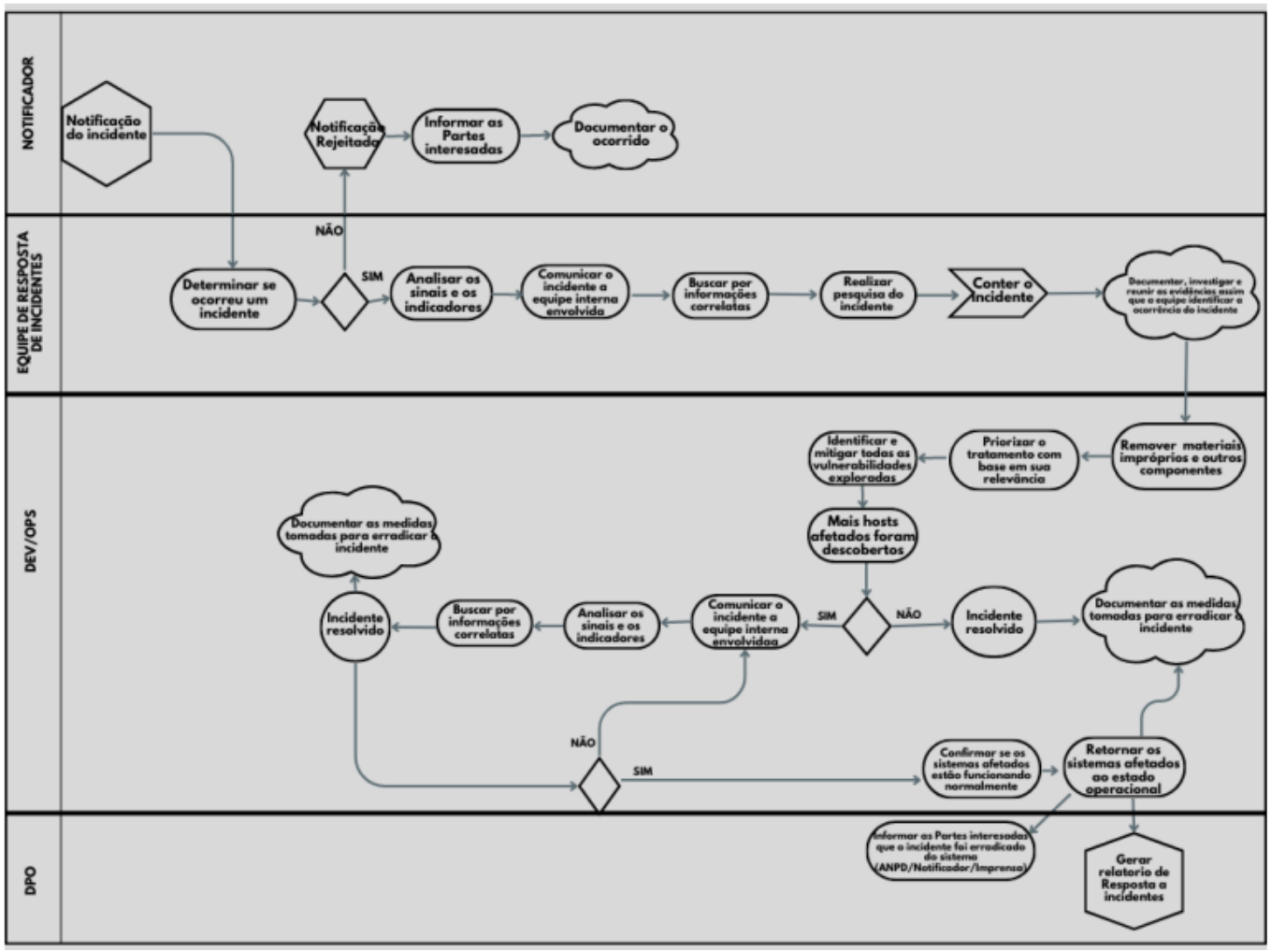

Figura 7.1: Fluxograma de detecção de incidente.

Capítulo 8

GRAVIDADE DO INCIDENTE

Uma vez que o Incidente seja identificado e classificado, é necessário priorizá-lo conforme o nível de risco oferecido à Empresa e aos titulares dos Dados Pessoais eventualmente afetados e a gravidade da ocorrência.

Figura 8.1: Gravidade da ocorrência.

Capítulo 9

PROCEDIMENTOS PARA RESPOSTA

9.1 NOTIFICAÇÃO DO INCIDENTE

Um novo incidente é notificado por pessoa, externa ou não a tecnotech, ou por alarme da monitoração a identificação de um incidente pode ocorrer pela interrupção não planejada de um serviço de TI, que pode ser percebida pelos usuários finais ou por meio dos sistemas de monitoramento de desempenho e disponibilidade. É importante que a equipe de TI esteja preparada para identificar rapidamente essas interrupções e investigar a causa raiz do problema, a fim de tomar as medidas necessárias para restaurar o serviço o mais rápido possível e minimizar o impacto aos usuários e à empresa como um todo.

9.2 DETERMINAR SE OCORREU O INCIDENTE

A equipe de resposta a incidentes é responsável por avaliar a notificação de incidente e determinar se ocorreu um incidente de segurança da informação e privacidade. Para isso, é importante que a notificação possa conter algumas das seguintes informações:

Origem do incidente:informação sobre a unidade, setor ou organização à qual o dispositivo ou processo que originou o incidente pertence.

Contato da origem: informação de contato do informante do incidente, como e-mail, telefone ou outro meio disponível.

Registro do tempo da ocorrência do incidente: data e hora na qual o incidente foi identificado.

Local onde originou o incidente: Local onde originou o incidente: endereço IP (IPv4 ou IPv6) do dispositivo ou serviço que originou o incidente.

Recursos utilizados pela origem do incidente: Recursos utilizados pela origem do incidente: especificação do tipo do protocolo (IP, TCP, UDP, etc) e portas, ou procedimentos operacionais, adotados na ação do incidente.

Endereço do alvo: endereço IP (IPv4 ou IPv6) do dispositivo ou endereço de acesso do serviço que foi o alvo do incidente.

Serviços envolvidos: especificação do serviço que foi alvo do incidente (http, ftp, smtp, etc.) e versões de sistemas utilizados.

Descrição do incidente: breve descrição do incidente, incluindo o tipo do ataque, motivação aparente ou outras características relevantes.

Logs ou evidências: anexação das porções de log, imagens, códigos de erro ou outros registros que evidenciem a ocorrência do incidente.

Essas informações são essenciais para que a equipe de resposta a incidentes possa avaliar a situação, determinar a gravidade do incidente e tomar as medidas necessárias para mitigá-lo.

9.3 CONTENÇÃO, ERRADICAÇÃO E RECUPERAÇÃO

Após a identificação de um incidente, é importante acionar imediatamente os desenvolvedores dos sistemas impactados para que possam orientar sobre os procedimentos de contenção e erradicação, conforme indicado na documentação.

O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados, evitando a propagação do incidente e minimizando prejuízos. É importante ressaltar que as ações tomadas devem ser cuidadosamente planejadas e executadas, a fim de evitar a perda de evidências que possam ser usadas para identificar a autoria, origem e método utilizado para o ataque.

pendendo da gravidade do incidente, pode ser necessário desligar os sistemas inteiros ou funcionalidades específicas, bem como colocar avisos de indisponibilidade para manutenção. Em caso de incidentes envolvendo máquinas virtuais, a tecnotech faz snapshot para análise posterior

Após a contenção do incidente, é fundamental garantir a restauração da integridade do sistema e verificar se as funcionalidades estão ativas. Além disso, devem ser implementadas medidas de segurança para evitar novos comprometimentos.

9.4 CONTENÇÃO

- **Desconectar o sistema comprometido ou isolar a rede afetada.**
- **Desativar o sistema para evitar maiores perdas quando há perda ou roubo de informações durante o ataque.**
- **Alterar políticas de roteamento dos equipamentos de rede ou bloquear padrões de tráfego, interrompendo o fluxo malicioso.**
- **Desabilitar serviços vulneráveis, inibindo comprometimento de outras funcionalidades do sistema.**

9.5 ERRADICAÇÃO

- **Garantir que as causas do incidente foram removidas, assim como todas as atividades e arquivos associados ao incidente.**
- **Assegurar a remoção de todos os métodos de acesso utilizados pelo invasor: novas contas de acessos backdoors e, se aplicável, acesso físico ao sistema comprometido.**

9.6 RESTAURAÇÃO

- **Restaurar a integridade do sistema.**
- **Garantir que o sistema foi recuperado corretamente e que as funcionalidades estejam ativas.**
- **Implementar medidas de segurança para evitar novos comprometimentos.**
- **Restauração do último e íntegro backup completo armazenado.**

9.7 DOCUMENTAÇÃO DO INCIDENTE

Durante o início do incidente até a resolução, é importante documentar e registrar todas as ações tomadas e as medidas de contenção adotadas. Isso permite que a equipe de resposta a incidentes possa analisar e avaliar a eficácia das medidas de contenção adotadas e, posteriormente, realizar melhorias para evitar futuros incidentes.

9.8 COMUNICAÇÃO PÓS INCIDENTE DE SEGURANÇA

- **A comunicação será feita em prazo razoável, conforme definido pela Autoridade Nacional, e deverá mencionar.**
- **Descrição da natureza dos dados pessoais afetados.**
- **As informações sobre os titulares envolvidos.**
- **A indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial.**
- **Os riscos relacionados ao incidente.**
- **Os motivos da demora, no caso de a comunicação não ter sido imediata.**
- **As medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.**

Capítulo 10

MUDANÇAS NA POLÍTICA

A presente versão 1.0 desta Política de resposta a incidentes foi atualizada pela última vez em: 07/03/2023. O editor se reserva o direito de modificar, a qualquer momento as presentes normas, especialmente para adaptá-las às evoluções, seja pela disponibilização de novas funcionalidades, seja pela supressão ou modificação daquelas já existentes. Esta Política de resposta a incidentes poderá ser atualizada em decorrência de eventual atualização normativa, razão pela qual se convida o usuário a consultar periodicamente esta seção.

Capítulo 11

CONTROLE DE VERSÕES

Tabela 11.1: Tabela de versões

Versão	Descrição	Responsável	Publicação
1.0	Versão para divulgação	Wanderson câmara - Felipe Andrade	07/03/2023

Capítulo 12

CONCORDÂNCIA

Eu li e entendi a Política de resposta a incidentes da TECNOTECH SISTEMAS. Entendo que se eu violar as diretrizes estabelecidas nesta Política, posso enfrentar ações legais e/ou disciplinares de acordo com as leis aplicáveis e as normas internas da TECNOTECH SISTEMAS.

Assinatura do funcionário Data