TERESÓPOLIS
acima de tudo!

Ciência e Tecnologia

PLANO DE RESPOSTA A INCIDENTES

SEGURANÇA DA INFORMAÇÃO E PRIVACIDADE DE DADOS

(Parte estruturante do Plano Operacional de Segurança da Informação)

Versão 2.0

Janeiro / 2025

TERÊGOV DIGITAL

Prefeitura Municipal de Teresópolis

Secretaria Municipal de Ciência e Tecnologia

GESTÃO

José Leonardo Vasconcellos de Andrade
Prefeito

André Muniz Pinto
Secretário Municipal de Ciência e Tecnologia

Larissa Pinheiro Rezende do Nascimento
Subsecretária Municipal de Ciência e Tecnologia

Cleiton Evandro Corrêa Pimentel
Diretor de Governança e Dados

Edmo de Macedo Gonçalves
Assessor Administrativo

André Washington Garcia Suarez
Encarregado de Proteção de Dados (DPO)

Bernardo Rodrigues de Oliveira
Analista Técnico

Gabriel da Costa Garcia
Analista Técnico

Giorgia Pietroluongo Holig
Estagiário / Segurança da Informação

Introdução

Este plano é parte integrante do Plano Operacional da Segurança da Informação (anexo).

Escândalos de vazamentos de dados e de ataques cibernéticos se tornaram comuns atualmente e estes são provenientes de meios cada vez mais sofisticados para burlar os controles e medidas de segurança da informação.

Considerando o volume de dados que a Secretaria de Ciência e Tecnologia da Prefeitura de Teresópolis trata e a relevância de seu papel institucional na entrega de serviços públicos, é importante que esta esteja consciente de que incidentes de segurança revestem-se de uma

realidade possível e que deve ser evitada com medidas de salvaguarda e prevenção.

No entanto, é necessário também que a secretaria esteja preparada para agir em caso de "violação da segurança que provoque, de modo acidental ou ilícito a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento" (definição constante no art. 4º da GDPR). Ademais, assim determina a LGPD:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.
>
> 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo:
>
> I - a descrição da natureza dos dados pessoais afetados;
>
> II - as informações sobre os titulares envolvidos;
>
> III - a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
>
> IV - os riscos relacionados ao incidente;
>
> V - os motivos da demora, no caso de a comunicação não ter sido imediata; e
>
> VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo.
>
> 2º A autoridade nacional verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao controlador a adoção de providências, tais como:
>
> I - ampla divulgação do fato em meios de comunicação; e
>
> II - medidas para reverter ou mitigar os efeitos do incidente.
>
> 3º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis,

no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los.

Neste sentido, em atendimento ao item 5.1 da Etapa 5 do Plano de Adequação da LGPD, foi elaborado este Plano de Resposta a Incidentes de 4 Segurança da Informação e Privacidade - PRISIP, ou seja, um documento da secretaria que deverá ser amplamente conhecido por todos os servidores e que dispõe sobre as medidas que devem ser adotadas no caso de uma situação de emergência ou evento de risco que possa ocasionar danos aos ativos tecnológicos, viabilizando, inclusive, a comunicação apropriada e tempestiva à ANPD, quando for o caso.

Objetivos

Com a implementação deste Plano, pretende-se alcançar o seguinte objetivo geral:

Orientar como responder às situações de emergência e exceção, de forma documentada, formalizada, rápida e confiável, ao passo em que resguarde as evidências que possam ajudar a prevenir novos incidentes e a atender às exigências legais de comunicação e transparência.

Ademais, pretende-se alcançar os seguintes objetivos específicos:

a. conferir clareza sobre o fluxo de procedimentos adequados e responsáveis no caso de incidentes;

b. preservar a reputação e imagem da SMCT;

c. assegurar respostas rápidas, efetivas e coordenadas;

d. quantificar e monitorar desempenho;

e. evoluir continuamente com as lições aprendidas;

Para que estes objetivos sejam alcançados, foram identificadas as seguintes premissas básicas:

1. apoio da alta gestão;

2. reunião de inteligência de incidentes de várias fontes;

3. definição de linhas de comunicação claras, incisivas e concisas;

4. definição dos atores envolvidos e dos Comitês;

5. consideração sobre os processos, sistemas e limitações existentes.

Cabe ressaltar, em relação à premissa 3 acima, que este Plano não aborda um tipo específico de incidente, mas estabelece etapas acionáveis, com linhas de comunicação, funções e notificações necessárias para responder a qualquer violação de segurança.

É necessário reforçar que na hipótese de um incidente não há tempo para estudo de uma política complexa e detalhada para, então, agir.

Abrangência e Prazo de Vigência

Este Plano de Resposta a Incidentes de Segurança da Informação e Privacidade - PRISIP abrange todos os recursos computacionais e físicos pertencentes, operados, mantidos e controlados pela Secretaria de Ciência e Tecnologia da Prefeitura de Teresópolis.

O PRISIP entrará em vigor na data de sua publicação, por tempo indeterminado, podendo ser revisto e alterado anualmente ou sempre que identificada a necessidade.

Termos e Definições

- agentes de tratamento: corresponde ao controlador e operador em conjunto; não são considerados controladores ou operadores os indivíduos subordinados, tais como os funcionários, os servidores públicos ou as equipes de trabalho de uma organização, já que atuam sob o poder diretivo do agente de tratamento;
- anonimização: é a utilização de meios técnicos razoáveis e disponíveis por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
- ataque: evento de exploração de vulnerabilidades, ocorre quando um atacante tenta executar ações maliciosas, como invadir um sistema, acessar informações confidenciais ou tornar um serviço inacessível;
- Autoridade Nacional de Proteção de Dados ou ANPD: é o órgão da administração pública nacional responsável por fiscalizar e zelar pelo cumprimento da Lei Geral de Proteção de Dados em todo o território brasileiro;
- controlador: é toda pessoa física ou jurídica, de direito público ou privado, a quem competem decisões referentes ao tratamento de dados pessoais;
- dados pessoais sensíveis: são dados pessoais que digam respeito a origem racial ou étnica, convicção religiosa, prática ou orientação sexual, informações médicas ou de saúde, como histórico médico e prontuário físico ou eletrônico, informações genéticas ou biométricas, crenças políticas ou filosóficas, filiação política ou sindical, número do seguro social, número da carteirinha do plano de saúde e informações bancárias;

- dados pessoais: qualquer informação relacionada a um indivíduo que possa ser usada para identificá-lo, direta ou indiretamente, ou para entrar em contato, por conta própria ou quando combinada com outras informações;
- encarregado ou Data Privacy Officer (DPO): é pessoa física designada pelo controlador, responsável por assegurar o cumprimento da legislação local aplicável, além de atuar como contato para os titulares dos dados e para a Autoridade Nacional de Proteção de Dados Pessoais (ANPD);
- expurgo de dados: significa destruição segura e definitiva de informações, ou seja, quando os dados não existem mais ou não podem mais ser acessados pelo controlador de qualquer forma;
- incidente: qualquer ato, suspeita, ameaça ou circunstância que comprometa a confidencialidade, integridade ou a disponibilidade de informações que estão em posse da SMCT ou que ela venha a ter acesso;
- IP: Protocolo da Internet (Internet Protocol), número utilizado para identificar um dispositivo de tecnologia da informação em uma rede, ou Internet;
- LGPD: acrônimo utilizado para identificação da Lei Geral de Proteção de Dados, a Lei nº. 13.709/2018, que regula as atividades de Tratamento de Dados no Brasil.
- log: processo de registro de eventos relevantes num sistema computacional;
- operador: é toda pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados em nome do controlador; o operador será sempre uma pessoa distinta do controlador, isto é, que não atua como profissional subordinado a este ou como membro de seus órgãos;
- porta: uma porta de conexão está sempre associado a um endereço IP de um host e ao tipo de protocolo de transporte utilizado para a comunicação. Exemplo: o servidor de email que executa um serviço de SMTP ele usa a porta 25 do protocolo TCP;
- scripts: conjunto de instruções para que uma função seja executada em determinado aplicativo;
- sistemas: hardware, software, network de dados, armazenador de mídias e demais sistemas usados, adquiridos, desenvolvidos, acessados, controlados, cedidos ou operados para dar suporte na execução de suas atividades.
- spam: termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
- spyware: programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros;
- tratamento: qualquer operação ou conjunto de operações efetuadas sobre os dados, por meios automatizados ou não, incluindo, mas não se limitando, a coleta, gravação,

organização, estruturação, alteração, uso, acesso, divulgação, cópia, transferência, armazenamento, exclusão, combinação, restrição, adaptação, recuperação, consulta, destruição ou anonimização;

- trojan: programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário;
- vazamento de dados: qualquer quebra de sigilo ou vazamento de dados que possa resultar, criminosamente ou não, na perda, alteração, compartilhamento, acesso, transmissão, armazenamento ou processamento de dados não autorizado;
- violação de privacidade: qualquer violação à legislação aplicável ou conduta e evento que resulte na destruição acidental ou ilícita dos dados, bem como sua perda, roubo, alteração, divulgação ou acesso não autorizado, danos ou desvio de finalidade em seu tratamento.
- vírus: programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos;
- worm: programa capaz de se propagar automaticamente pelas redes, enviando cópias de si mesmo de computador para computador;

Atores e Responsabilidade

- Notificador - pessoa ou sistema de monitoração que notifica o incidente; (André)
- Acionadores (Atendimento e Suporte de TI): equipe do CPD / gestor da Segurança da informação;
- Comitê de Resposta a Incidentes (CRI) - time de especialistas de tecnologia da informação da SMCT para conduzir e documentar as respostas aos incidentes relacionados a recursos computacionais.
- Comitê de Resposta – grupo de servidores designados pelo Secretário de Ciência e Tecnologia para atuar nos casos de incidentes de segurança da informação e privacidade não relacionados a recursos tecnológicos;
- Responsável por Sistema ou Controlador de Sistema: patrocinador ou analista responsável identificado no inventário de soluções tecnológicas (quando houver), com capacidade de propor soluções de resposta a serem apreciadas pelo Comitê de Resposta a Incidentes (CRI), para autorizar ou vetar procedimentos de emergência (preferencialmente deve ser identificado no inventário de soluções, com formas de contato para emergências);
- Responsável por Processo ou Negócio: gerente ou chefe de setor identificado na estrutura organizacional, com capacidade de propor soluções de resposta a serem apreciadas pelo Setor de Segurança da Informação (SSI), para autorizar ou vetar procedimentos de emergência;

- Encarregado(a) pelo Tratamento de Dados Pessoais (ou DPO)

Descrição dos Processos

Este Plano de Resposta a Incidentes de Segurança da Informação e Privacidade consiste essencialmente em processos, os quais estão estruturados conforme as etapas a seguir descritas:

Processo 1 - Incidentes de Segurança da Informação e Privacidade Relacionados a Recursos Computacionais

Início

1) Um novo incidente é notificado, por pessoa externa ou por alarme da monitoração, usando o sistema (ou outra que vier a substituir). A comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como e-mails, sistema 1Doc, telefone, “Fale Conosco” (TIA), eOuve, devendo todas serem cadastradas, diretamente pelo notificador ou com auxílio do Atendimento e Suporte de TI, no sistema 1Doc, ou outra que vier a substituir para triagem.

Triagem

2) O Acionador (Atendimento e Suporte de TI da SMCT) deve fazer a avaliação preliminar ou contatar imediatamente outro Acionador em condições de realizar a referida avaliação, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

3) Na avaliação preliminar, devem ser buscadas informações sobre os sistemas que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver resposta imediata.

4) Conforme a avaliação preliminar, incidentes que não envolvem sistemas online e que seguramente não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para trâmites regulares da Equipe de Segurança da Informação e Encarregado pelo Tratamento de Dados Pessoais, caso o incidente envolva dados pessoais.

5) Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o Setor de Segurança da Informação (SSI) deve ser acionado e passa-se para as fases seguintes.

Avaliação

6) Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente pelo Setor de Segurança da Informação (SSI), classificando-o e definindo sua criticidade.

7) São exemplos de classificação de incidentes:

- Conteúdo abusivo: spam, assédio, etc;
- Código malicioso: worm, vírus, trojan, spyware, scripts;
- Prospecção por informações: varredura, sniffing, engenharia social;
- Tentativa de intrusão: tentativa de exploração de vulnerabilidades, tentativa de acesso lógico;
- Intrusão: acesso lógico indesejável, comprometimento de conta de usuário, comprometimento de aplicação;
- Indisponibilidade de serviço ou informação: negação de serviço, sabotagem;
- Segurança da informação: acesso não-autorizado à informação, modificação não autorizada da informação;
- Fraude: violação de direitos autorais, fingir ou falsificar identidade pessoal ou institucional, uso de recursos de forma não-autorizada;
- Outros: incidente não categorizado.

8) Em caso de vários incidentes, é importante definir uma ordem de atendimento de acordo com a urgência de tratamento e o impacto nas áreas de negócio. A criticidade do incidente pode ser definida de acordo com as classificações:

- Alto (Impacto Grave) - Incidente que afeta sistemas relevantes ou informações críticas, com potencial para gerar impacto negativo sobre a instituição;
- Médio (Impacto Significativo) - Incidente que afeta sistemas ou informações não críticas, sem impacto negativo à instituição;
- Baixo (Impacto Mínimo) - Possível incidente, sistemas não críticos; investigações de incidentes ou de colaboradores; investigações de longo prazo envolvendo pesquisa extensa e/ou trabalho forense detalhado.

9) Deve-se procurar identificar a causa do incidente, endereços IP e credenciais envolvidas, transações e transferências de dados irregulares, métodos e vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos sistemas afetados para colaborar e isso deve ser feito a critério do Setor de Segurança da Informação (SSI) a qualquer momento que julgar adequado e viável.

10) Caso as soluções impactadas tenham responsáveis identificados no inventário de soluções, estes devem ser acionados, para que se manifestem sobre os procedimentos de contenção e erradicação propostos pelo Setor de Segurança da Informação (SSI), colaborando nas estratégias de atuação.

Contenção e Erradicação

11) O objetivo das medidas de contenção e erradicação é limitar o dano e isolar os sistemas afetados para evitar mais danos. Aqui, conforme a necessidade e a autorização obtida, será realizado o desligamento dos sistemas inteiros ou de funcionalidades específicas, exposição de avisos de indisponibilidade para manutenção, sempre que possível tomando cuidados para não impactar evidências que poderiam ser usadas para identificar autoria, origem e método usado para quebrar a segurança.

12) Em caso de incidente envolvendo máquinas virtuais, deve ser feito o registro do estado em que se encontrem os sistemas, aplicações ou arquivos afetados (snapshot) para posterior análise.

Recuperação

13) Caso exista um Plano Operacional Política de Segurança da Informação, ele deve ser iniciado, conforme especificado.

14) A recuperação é o conjunto de medidas para restaurar os serviços completamente, mas pode ser feita de forma gradual, conforme viabilidade e decisão do responsável pelo sistema.

15) O Setor de Segurança da Informação (SSI) tem a responsabilidade de passar as informações que obteve para o desenvolvimento da solução e sua instalação.

16) Para a recuperação devem ser tomadas medidas identificadas na Avaliação, tais como restauração de backups, clonagem de máquinas virtuais, reinstalação de sistemas.

17) Pode ser necessário o desenvolvimento e instalação de atualizações de aplicação ou do Sistema Operacional, por isso esta fase pode ser prolongada, de acordo com a priorização dada.

Lições Aprendidas

18) Com o incidente contido e sua resolução encaminhada, o Setor de Segurança da Informação (SSI) deve agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os sistemas e processos, avaliar a eficácia deste Plano de Resposta a Incidentes de Segurança de Informação e Privacidade e subsidiar a documentação da causa-raiz, bem como outras provas.

19) As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

Documentação

20) O Setor de Segurança da Informação (SSI) deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Comunicações

21) Assim que possível, no caso de incidente envolvendo dados pessoais, a situação deve ser encaminhada para análise da Diretoria Executiva e da Assessoria Técnica do Gabinete para avaliar se houve risco ou dano relevante aos titulares dos dados impactados.

22) Caso a Diretoria Executiva e da Assessoria Técnica do Gabinete conclua que o incidente acarretou risco ou dano relevante aos titulares de dados, deverá o Encarregado de Tratamento de Dados (DPO) e a Assessoria de Comunicação fazer as comunicações obrigatórias por Lei, bem como informar e subsidiar. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados e imprensa, bem como relatórios formais para a ANPD.

Processo 2 - Incidentes de Segurança da Informação e Privacidade Não Relacionados a Recursos Computacionais

Início/Detecção

1) Um novo incidente é notificado, por pessoa externa ou por alarme da monitoração, usando o sistema (ou outra que vier a substituir). A comunicação inicial do incidente pode ser proveniente de qualquer fonte, tais como e-mails, sistema 1Doc, telefone, “Fale Conosco” (TIA), eOuve, devendo todas serem cadastradas, diretamente pelo notificador ou com auxílio do Atendimento e Suporte de TI, no sistema 1Doc, ou outra que vier a substituir para triagem.

Triagem

2) O Setor de Segurança da Informação (SSI) deve fazer a avaliação preliminar, descartando as notificações nulas ou claramente improcedentes, tomando os devidos cuidados.

3) Na avaliação preliminar, devem ser buscadas informações sobre os procedimentos que foram alegadamente impactados, sua criticidade, quais os danos aparentes e o risco da situação se agravar se não houver ação imediata.

4) Conforme a avaliação preliminar, incidentes que não apresentam riscos aumentados pela falta de ação imediata podem ser reencaminhados para trâmites regulares dos setores pertinentes, caso haja já um trâmite pré-estabelecido.

5) Em caso de incidentes que exigem resposta imediata ou melhor avaliação, o Setor de Segurança da Informação avança para as fases seguintes.

Avaliação

6) Nesta fase deve ser iniciada uma avaliação mais detalhada do incidente pelo SSI, classificando-o e definindo sua criticidade.

7) A criticidade do incidente pode ser definida de acordo com as seguintes classificações:

- Alto (Impacto Grave) - Incidente que afeta informações críticas, com potencial para gerar impacto negativo sobre a instituição;
- Médio (Impacto Significativo) - Incidente que afeta informações não críticas, sem impacto negativo à instituição;
- Baixo (Impacto Mínimo) - Possível incidente.

8) Deve-se procurar identificar a causa do incidente, atores e ações envolvidas, vulnerabilidades exploradas, visando determinar ações para as demais fases. Pode ser importante engajar especialistas dos setores afetados para colaborar e isso deve ser feito a critério do SSI a qualquer momento que julgar adequado e viável.

9) Caso os processos envolvidos tenham chefes responsáveis identificados na estrutura organizacional, estes devem ser acionados, para que se manifestem sobre os procedimentos de resposta propostos pelo SSI, colaborando nas estratégias de atuação.

Contenção, Erradicação e Recuperação

10) O objetivo das medidas de contenção, erradicação e recuperação é limitar o dano e restabelecer a segurança. Como neste fluxo trata-se de incidentes não relacionados a recursos computacionais, mas essencialmente de atividade humana, os procedimentos podem envolver sindicância administrativa, processo administrativo disciplinar, entre outras medidas dispostas na legislação aplicável ao caso.

11) Neste sentido, poderão ser acionados órgãos, conforme o caso, como o Controle Interno, Comitê Gestor de Proteção de Dados e o Setor de Infraestrutura e Rede da Secretaria de Ciência e Tecnologia.

Lições Aprendidas

12) Com o incidente contido e sua resolução encaminhada, o Setor de Segurança da Informação (SSI) deve agendar e conduzir uma reunião de Lições Aprendidas, com convidados a seu critério, com o objetivo de discutir erros e dificuldades encontradas, propor melhorias para os processos de segurança e de privacidade da informação, avaliar a eficácia deste Plano de Resposta a Incidentes de Segurança de Informação e Privacidade e subsidiar a documentação da causa-raiz, bem como outras provas.

13) As melhorias sugeridas na reunião, com o devido consenso, devem ser encaminhadas aos responsáveis para definição sobre a adoção.

Documentação

14) O Setor de Segurança da Informação deve documentar o incidente em base de conhecimentos apropriada, detalhando as informações obtidas, linha de tempo, atores envolvidos, evidências, conclusões, decisões, autorizações e ações tomadas, inclusive as da reunião de lições aprendidas.

Comunicações

15) Assim que possível, no caso de incidente envolvendo dados pessoais, a situação deve ser encaminhada para análise da Diretoria Executiva e da Assessoria Técnica do Gabinete para avaliar se houve risco ou dano relevante aos titulares dos dados pessoais impactados.

16) Caso a Diretoria Executiva e a Assessoria Técnica do Gabinete conclua que o incidente acarretou risco ou dano relevante aos titulares de dados pessoais, deverá o Encarregado de Tratamento de Dados (DPO) e a Assessoria de Comunicação fazer as comunicações obrigatórias por Lei. Essas comunicações podem incluir agradecimentos ao notificador, informações para os titulares de dados e imprensa, bem como relatórios formais para a ANPD.

FLUXOGRAMA CONTINGENCIAL