Norma para Plano de Resposta a Incidentes de Segurança da Informação

PREFEITURA

Mais **cidade**. Mais **vida**.

Normativa para Plano de Resposta a Incidentes da Prefeitura Municipal de Porto Alegre

Secretaria Municipal de Planejamento e Assuntos Estratégicos

Coordenação de Planejamento e Gestão de Tecnologia da Informação e Comunicação

(SMPAE – CGTI)

Versão 1.0

Última atualização 19 de Janeiro de 2023

PREMISSAS

Todos os servidores públicos, secretarias, órgãos, fornecedores, prestadores de serviço e demais parceiros vinculados devem ter conhecimento de seu importante papel no contexto de **Segurança da Informação (SI)** sendo um dever seguirem as diretrizes e orientações contidas na **Política de Segurança da Informação (PSI)** em sua íntegra, assim evitando expor a informação e os recursos de processamento a situações adversas como comprometimento, alteração, furto e desvio.

GLOSSÁRIO DE TERMOS

Agência Nacional de Proteção de Dados - **ANPD**
Procempa - **TI**
CGTI-SMPAE - **GOVERNANÇA**
Lei Geral de Proteção de Dados - **LGDP**
Time de Resposta a Incidentes - **TRI**
Plano de Recuperação de Desastres - **PRD**
Plano de Continuidade de Negócios - **PCN**
Canal para Comunicação de Eventos de Segurança – **CCES**
Encarregado de Dados - **DPO**

CONCEITOS

Diante de um crescente avanço tecnológico e de um mundo cada vez mais digital as preocupações com incidentes de segurança ocupam uma parte significativa no diário das organizações. Estar preparado para lidar com um eventual incidente de segurança é fator decisivo na continuidade das operações e por isso é preciso estruturar bem um plano de ação.

Em face a **LGPD**, além da preocupação com a segurança dos dados que já existia, agora há também os aspectos legais referentes a proteção do dado pessoal tratado que precisam ser observados, o que tornou a matéria ainda mais importante.

Fundamental ter o entendimento que nem todo incidente de segurança envolverá dados pessoais, mas todo incidente envolvendo dados pessoais será um incidente de segurança, logo, além da equipe responsável, o **DPO** deverá ser envolvido seguindo as orientações e normas da **ANPD**.

A norma em questão tem como base as recomendações da ISO 27035, que se divide em três partes, contemplando detalhadas orientações para gestão de incidentes, o que vem a somar principalmente com a ISO 27001 e a ISO 27002 que tratam do Sistema de Gestão de Segurança Informação e sua implementação.

DIRETRIZES

- Competem a **TI** à implantação de um Plano de Resposta a Incidentes de Segurança da Informação, a disponibilização de um **CCES** para receber os reportes de eventos de segurança, bem como manter uma **TRI** que será acionada após a triagem inicial do **CCES**.

- A Gestão de Incidentes em Segurança da Informação deve ser organizada em um conjunto de processos capazes de contemplar os seguintes itens:
  - Detecção;
  - Aviso;
  - Avaliação;
  - Resposta;
  - Tratamento;
  - Aprendizagem.

- O **CCES** deverá ter sua forma de contato anunciada a toda **PMPA** e funcionar 24x7(vinte e quatro horas por dia, sete dias por semana) de forma a receber os reportes de eventos de Segurança da Informação e dar o destino à equipe especializada contemplando as seguintes fases:
  - Documentação;
  - Triagem;
  - Priorização;
  - Comunicação à **TRI**.

- A **TRI** deve ser composta por corpo técnico capacitado para receber e tratar os eventos de Segurança da Informação envolvendo o **DPO** sempre que o incidente tenha relação com dados da pessoa natural, sejam estes dados pessoais ou sensíveis.

- O Processo de Gerenciamento de Incidentes deve contemplar um escalonamento e ações de envolvimento de acordo com o tipo do evento conforme os itens a seguir:
  - Acionamento da **TRI**;
  - Comunicações Devidas.
  - Aplicação do **PRD** quando necessário;
  - Recuperação de um Incidente;
  - Aplicação do **PCN** quando necessário;

- Os reportes que caracterizarem um incidente de segurança devem passar por um processo de gerenciamento de incidentes que envolva:
  - Avaliação;
  - Monitoramento;
  - Classificação;
  - Análise;
  - Ações Corretivas;
  - Relatórios dos Incidentes;
  - Comunicação a todas as partes interessadas internas e externas;
  - Aprendizado e Melhorias.

- Os relatórios criados para controle histórico, aprendizado e aperfeiçoamento deverão conter os seguintes campos:
  - Data e hora;
  - Nome da pessoa que reporta o incidente;
  - Onde ocorreu o incidente;
  - Qual o problema;
  - Qual o efeito que o incidente causou;
  - Como foi descoberto.

- Devem ser construídos procedimentos para auxiliar a **TRI** a lidar com os Incidentes de Segurança através de formulários e orientações que contemplem:
  - Análise do incidente e sua causa;
  - Medidas para minimizar as consequências;
  - Ações para evitar que o incidente ocorra novamente;
  - Quais partes devem ser comunicadas (partes afetadas e partes responsáveis pela solução).

- De acordo com a relevância e gravidade do incidente a correta coleta de evidências do incidente de segurança é fundamental, não somente para a análise e aprendizado, mas para o respaldo da **PMPA** e devidas ações legais que possam ser necessárias. São pontos a serem observados no tratamento de evidências:
  - O envolvido jurídico ou amparo de lei diante de qualquer implicação legal que uma evidência possa ter;
  - Evidências só tem valor legal se são registros completos e se não foram adulteradas sob-hipótese alguma;
  - Cópias de provas eletrônicas precisam ser idênticas às originais;
  - Evidências geradas em momentos em que um sistema não está funcionando corretamente têm sua credibilidade comprometida, salvo se esta evidência é exatamente a prova do mau funcionamento do sistema.

Histórico de Revisões

Versão	Data	Alterações	Autor	Revisor
1.0	19/01/2023	Versão inicial	(CGTI-SMPAE) Eduardo Hoppe Jefferson Bregalda	(CGTI-SMPAE) Eduardo Hoppe