POLÍTICA DE RESPOSTA A INCIDENTE DE SEGURANÇA DE DADOS

Conselho Regional de Contabilidade do Estado de São Paulo

Conselho Diretor

José Donizete Valentina - **Presidente**

José Aparecido Maion - **Vice-presidente de Administração e Finanças**

João Carlos Castilho Garcia - **Vice-presidente de Fiscalização, Ética e Disciplina**

Marcelo Roberto Monello - **Vice-presidente de Desenvolvimento Profissional**

Mariano Amadio - **Vice-presidente de Registro**

Comissão de Implantação da Lei Geral de Proteção de Dados – LGPD do CRCSP

Domingos Sávio Mota - **Coordenador**
Cláudio Rafael Bifi – ***Vice Coordenador***

Membros

Ronaldo César da Silva
Fernando Eugênio do Santos
Gilmar Pires de Simões
Valeria Vanessa de Campos Pinezi
Reginaldo Gomes Ferreira
Clarindo Bibiano de Araújo
Luiz Fernando Lopes
Rosa Maria Pereira
Luciana de Souza Ramos
Elaine Constantino Santos
Guilherme Andreas Campos Del Guerra
Andrea Fernandes dos Santos Guenka

Política de Resposta a Incidente de Segurança de Dados

(Versão 1.1)

Histórico de Alterações

Data	Versão	Descrição	Autor
31/01/2023	1.1	Alteração do formulário e orientações para envio de comunicação de incidente a ANPD.	Valéria Vanessa de Campos Pinezi

Sumário

1. Introdução

O tratamento de incidentes envolvendo a segurança da informação é fundamental no combate a eventos que possam resultar em perda, dano ou acesso não-autorizado às informações. Esse tratamento corresponde a medidas planejadas e organizadas para detecção, análise e reação em situações que levem a um rompimento na tríade que configura a segurança da informação: confidencialidade, integridade e disponibilidade.

Dentre as ações que podem gerar esse rompimento, é possível destacar: negação de serviço; código malicioso; vírus; acesso não autorizado ou uso inapropriado de contas ou sistemas; instalação ou uso de softwares não autorizados; perda de arquivos essenciais as atividades; roubo ou perda de equipamentos; dano acidental ou proposital a equipamentos de tecnologia; saída não-autorizada de dados; divulgação não-autorizada de informações confidenciais ou secretas; entre outros.

2. Objetivos

Definir os critérios para a gestão de incidentes de Segurança da Informação, possibilitando uma resposta rápida e eficaz ao incidente, preservando a reputação e a imagem do CRCSP, minimizando os prejuízos financeiros.

3. Abrangência

Esta política se aplica a todos do CRCSP, quais sejam: conselheiros, funcionários, estagiários, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações do CRCSP. Todos serão tratados nesta política como usuários.

4. O que é 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. Conforme artigo 47 da Lei nº. 13.709/18, cabe ao agente de tratamento de dados pessoais a adoção de medidas de segurança.

5. Diretrizes da Resposta a Incidentes de Segurança da Informação

5.1. Contexto Geral

As respostas aos incidentes de Segurança da Informação visam: assegurar o

restabelecimento do nível normal do ambiente tecnológico, após o acontecimento de um sinistro, através do direcionamento na utilização dos recursos e procedimentos fundamentais, no intuito de garantir uma resposta efetiva.

5.2. Planejamento

Esta atividade compreende identificar, prever e descrever situações de possíveis sinistros, bem como suas respectivas ações de mitigação, responsáveis, tempos e registros, de forma que, em situações reais, as atividades já estejam previamente mapeadas e as ações já preestabelecidas. Assim, deve constar no planejamento:

a) A definição de uma equipe de planejamento, suas responsabilidades e papéis predefinidos, para prever situações de sinistro e as possíveis respostas, assim como atuar no monitoramento e na resposta aos incidentes;

b) A definição do catálogo dos recursos tecnológicos existentes no parque do CRCSP, bem como aqueles necessários para possibilitar uma atuação efetiva na resposta aos incidentes, como por exemplo: cadastro de todas as máquinas do tipo servidor;

c) O detalhamento das ações necessárias na resposta a incidentes, conforme o tipo e criticidade desses, deve abordar o tempo mínimo de resposta e a quem os incidentes devem ser reportados, entre outros, conforme tabela anexa.

d) Os casos que, em virtude de sua relevância, devem ser previamente autorizados pela alta gestão;

e) Elaborar relatório à Diretoria responsável com a avaliação do incidente, informando as medidas tomadas e a análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas (Art. 6º, X da LGPD).

5.3. Identificação

Esta atividade compreende realizar ações para identificação e registro dos sinistros.

a) Através dos recursos de detecção na rede, no monitoramento dos servidores e recursos de tecnologia ou através de problemas reportados pelos usuários, podem ser identificados alertas de segurança que configurem incidentes de segurança. Diante disso, a Comissão LGPD poderá ser acionada para que o alerta seja analisado e sejam tomadas as devidas providências, tanto no tratamento do incidente, quanto no encaminhamento do problema para a gestão;

b) Algumas situações podem ser consideradas na notificação de um evento de Segurança da Informação:

I. Violação da disponibilidade, confidencialidade e integridade da informação;
II. Inconformidade das políticas e/ou procedimentos;
III. Alterações de sistemas sem controle;
IV. Funcionamento indevido de software ou hardware;
V. Violação de acesso lógico.

c) Eventos, mesmo que apenas suspeitos, devem ser analisados e validados rapidamente. Uma vez confirmada a ocorrência de um incidente, então a análise do escopo daquele incidente deverá ser executada. Essa análise deve prover informações suficientes que permitam identificar e priorizar as atividades subsequentes;

d) Todos os usuários são responsáveis por relatar qualquer tipo de eventos e fragilidades, que possam causar danos à segurança da Informação. A notificação do evento ou fragilidades por parte do usuário deverá ser registrada através HelpDesk.

5.4. Resposta

A atividade de resposta a incidentes de segurança da informação compreende reações aos possíveis ataques realizados.

a) A partir de uma detecção de um incidente de segurança, é importante controlá-lo antes que uma possível extensão comprometa outros recursos. Como exemplo, tem-se uma infecção por vírus em um computador e que, se não for controlado em tempo, pode comprometer outros computadores da rede;

b) A estratégia de resposta ao incidente de segurança da informação a ser adotada deve ser baseada no tipo (ex: vírus, perda de arquivo, incêndio, etc.) e na criticidade do incidente (ex: impacta na imagem ou na operação do CRCSP, compromete várias áreas, entre outros);

c) Após a identificação e a confirmação que o incidente se trata de um evento de Segurança da Informação, ou seja, que viole a disponibilidade, a confidencialidade ou a integridade da informação, a resposta deverá ser realizada a partir das seguintes ações:

I. Preservar, na medida do possível, todas as evidências, para que seja possível identificar o problema e rastrear a possível causa;

II. Verificar se existem planos de ação em que o sinistro identificado esteja previsto, no intuito de seguir o planejamento;

III. Agir para que os serviços afetados sejam disponibilizados em seu estado normal de funcionamento no menor tempo possível;

IV. Utilizar todos os recursos necessários para a implementação de uma estratégia de reação, seja permanente ou provisória;

V. Utilizar atividades de recuperação, tais como: a restauração de backups de sistemas, a instalação de patches, a alteração de senhas e a revisão da segurança do perímetro da rede do CRCSP.

d) Quando as consequências do incidente estiverem contidas, é necessário que sejam removidos todos os componentes do incidente, como por exemplo: um código malicioso ou desabilitar contas de usuários violadas.

5.5. Vistoria

A vistoria consiste em ações realizadas após a ocorrência do incidente, como auditorias e análises de vulnerabilidade.

a) É fundamental assegurar que as atividades envolvidas nas respostas aos incidentes sejam adequadamente registradas para futuras análises. Os registros servirão de banco de conhecimento para resposta em incidentes semelhantes;

b) De acordo com o incidente, uma análise mais aprofundada deve ser conduzida para identificar a origem do incidente para que o tratamento das fragilidades e/ou não conformidade encontradas contribuam para a resolução do incidente;

c) Periodicamente, a área de tecnologia da informação deve realizar uma análise no ambiente tecnológico com o objetivo de identificar possíveis vulnerabilidades e, de forma antecipada, eliminá-las;

d) Após a identificação das possíveis vulnerabilidades, deverá ser gerado um relatório e, após análise da Comissão e aprovação do Conselho Diretor, às áreas responsáveis devem ser comunicadas para as devidas tratativas. Após a resolução, o relatório deve ser arquivado com o registro das ações realizadas.

5.6. Melhores Práticas

a) Evitar implantações ou atualizações de softwares que estejam fora das especificações ou escopo da infraestrutura atual do ambiente, pois isso pode acarretar em novos incidentes de segurança;

b) Os usuários não podem tentar provar a fragilidade do ambiente tecnológico, salvo a equipe técnica responsável com a devida autorização;

c) O processo de recuperação pode envolver o acionamento de um processo de continuidade do negócio, a fim de restabelecer a operação normal do CRCSP. Assim, é fundamental ter um Plano de Continuidade do Negócio (PCN) que envolva os ambientes e processos críticos do CRCSP.

6. Comunicação do Incidente

A Comissão LGPD deverá avaliar internamente a relevância do risco ou dano do incidente de segurança, para determinar se há a necessidade de enviar comunicações à ANPD e aos Titulares, observando os critérios abaixo:

a) Quando o incidente de segurança acarretar um risco ou dano relevante aos titulares afetados;

b) A probabilidade de risco ou dano relevante para os titulares, conforme a lei, será maior sempre que o incidente envolver dados sensíveis ou de indivíduos em situação de vulnerabilidade, incluindo crianças e adolescentes, ou tiver o potencial de ocasionar danos materiais ou morais, tais como discriminação, violação do direito à imagem e à reputação, fraudes financeiras e roubo de identidade. Da mesma forma, deve-se considerar o volume de dados envolvido, o quantitativo de indivíduos afetados, a boa-fé e as intenções dos terceiros que tiveram acesso aos dados, após o incidente e a facilidade de identificação dos titulares por terceiros não autorizados;

c) Seguindo o disposto no artigo 48 da referida Lei, é obrigação do controlador comunicar à autoridade nacional e ao titular dos dados a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. Devendo esta comunicação ser feita em prazo razoável, conforme definição da autoridade nacional.

6.1. Comunicação aos Titulares

Em caso de comprovação de Incidente de Segurança (Vazamento de Dados), e após análise da Comissão de LGPD em concluir a alta relevância do risco ou dano do incidente de segurança, os Titulares deverão ser comunicados, conforme procedimentos abaixo:

a) No prazo de 2 (dois) dias úteis, contados da data do conhecimento do incidente, é obrigação do CRCSP o envio de comunicação aos Titulares (artigo 48 da LGPD);

b) O comunicado deverá ser encaminhado por e-mail aos Titulares afetados, com informações sobre o incidente e ações tomadas;

c) Deverá ser publicado no Portal do CRCSP, texto aprovado pelo Conselho Diretor, com

informações sobre o incidente e ações tomadas;

d) Novas informações sobre o assunto serão divulgadas tempestivamente e com a devida transparência, nos mesmos meios acima elencados.

6.2. Comunicação à Autoridade Nacional de Proteção de Dados

Em caso de comprovação de Incidente de Segurança (Vazamento de Dados), e após análise da Comissão de LGPD concluir a alta relevância do risco ou dano do incidente de segurança, deverá ser feita a comunicação à ANPD, conforme procedimentos abaixo:

a) É obrigação do (a) DPO comunicar à Autoridade Nacional de Proteção de Dados (ANPD), a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (artigo 48 da LGPD), no prazo de 5 (cinco) dias úteis, contados da data do conhecimento do incidente;

b) O comunicado deverá ser encaminhado a ANPD através de formulário próprio, através de Peticionamento Eletrônico:

I. Formulário ANPD:

https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis/formulario_cis_anpd1.docx

II. Orientações da ANPD para Comunicação de Incidência de Segurança:

https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis

7. Adequação à Política

a) Os novos projetos ou novas aquisições devem seguir os padrões estabelecidos nesta política;

b) As implementações para o ambiente tecnológico existente, deverão ser adequadas a esta política no prazo de 1 (um) ano, a partir de sua publicação;

c) Caso não seja possível a adequação das ferramentas, a Comissão LGPD deve documentar essa informação, bem como seus motivos, para fins de auditoria interna.

8. Anexo – Detalhamento das ações necessárias na resposta a incidentes

INCIDENTE	CRITICIDADE	AÇÃO	RESPONSABILIDADE	TEMPO MÍNIMO DE RESPOSTA	A QUEM REPORTAR	COMO REPORTAR
Pasta (repositório) não encontrado ou excluído no servidor de arquivos	Alta	Restaurar pasta (repositório) do servidor de arquivo. Contactar empresa que cuida do suporte Segurança.	TI	24h	Gestor da TI	Acionar o Comite
Banco de Dados SPI/TOTVS invadido	Alta	Restaurar Bancos de dados Comprometido. Contactar empresa que cuida do suporte Segurança.	TI	8h	Gestor da TI	Acionar o Comite
Vazamento de contas de e-mails Funcionários	Alta	Restaurar Bancos de dados Comprometido. Contactar empresa que cuida do suporte Segurança.	TI	8h	Gestor da TI	Acionar o Comite