POLÍTICA DE TRATAMENTO DE INCIDENTES DE SEGURANÇA

Versão: 1.0

31/08/2022

1. OBJETIVO

Incidentes de Segurança da Informação podem expor dados pessoais e sensíveis de titulares que se relacionam com a escola (alunos, responsáveis legais, colaboradores) àqueles que não devem ter acesso a esses dados, potencialmente causando danos à reputação e o risco de incorrer em multas substanciais. Esta política abrange a resposta apropriada de todos os membros do Instituto São José em caso de eventual ocorrência de um incidente.

2. APLICABILIDADE

Esta Política de Segurança da Informação aplica-se a equipe diretiva, pedagógica, funcionários em geral, parceiros de negócio, prestadores de serviço ou fornecedores que se utilizam dos ativos da informação do Instituto São José, os quais são também responsáveis pela referida segurança, estando cientes de seu compromisso com a proteção e o uso adequado da informação.

3. DEFINIÇÃO

Um incidente de segurança da informação é definido como:

> *"Um evento pelo qual qualquer serviço ou informação armazenada ou processada pelo Instituto São José foi, ou potencialmente foi, perdido, destruído, alterado, copiado, transmitido, roubado, usado ou acessado ilegalmente ou por indivíduos não autorizados, acidentalmente ou de propósito".*

Isso inclui, mas não se limita a:

- ✓ Perda ou roubo de qualquer dispositivo, pessoal ou de propriedade do Instituto São José, armazenando dados da escola ou uma conta de e-mail corporativo;
- ✓ A perda ou roubo de qualquer dispositivo, pessoal ou de propriedade do Instituto São José, utilizado com um cliente, parceiro ou prestador de serviço para se conectar à rede corporativa;
- ✓ Tentativa de pessoas não autorizadas de obter acesso a dados ou sistemas de computador da empresa;
- ✓ A presença de um vírus de computador ou *ransomware* em qualquer dispositivo que tenha acesso aos sistemas de rede da empresa;
- ✓ Uma conta de usuário comprometida por golpe de *phishing*;
- ✓ E-mail contendo dados pessoais enviados por engano ao destinatário errado;
- ✓ Perda de registros em papel com dados pessoais ou confidenciais.

4. RELATÓRIOS

Todos os incidentes ou incidentes suspeitos devem ser reportados ao DPO (Encarregado de Proteção de Dados Pessoais) assim que um risco for identificado, idealmente dentro de 24 horas. Quando uma perda de dados pessoais ou confidenciais pode ter ocorrido, isso deve ser relatado no máximo em 24 horas, mas idealmente assim que a perda for notada. Quando uma perda ou roubo é reportado a um órgão regulador, como a polícia, uma cópia do relatório deve ser submetida ao departamento de TI. O relatório deve incluir detalhes completos e precisos do incidente que contém:

- ✓ A natureza do incidente (roubo ou perda de equipamento, *hacking*, etc.);
- ✓ Que tipo de dados (não os dados em si) estavam envolvidos;
- ✓ Detalhes de todas as partes envolvidas.

O responsável pela TI registrará e documentará o incidente.

5. INVESTIGAÇÃO

O DPO (D*ata Protection Officer*, ou Encarregado de Proteção de Dados Pessoais) realizará uma investigação inicial sobre o incidente assim que praticamente possível após o recebimento do relato do incidente. O DPO estabelecerá:

- ✓ A natureza do incidente;
- ✓ A classificação do incidente conforme a sua severidade, para resposta do fluxo de trabalho;
- ✓ Se os dados pessoais ou confidenciais foram expostos, a escola deve identificar o(s) indivíduo(s) associado(s) e o prejuízo em potencial para eles, de acordo com os requisitos da Lei Geral de Proteção de Dados Pessoais;
- ✓ Avaliar quaisquer riscos para os dados empresa, clientes, colaboradores;
- ✓ Avaliar quaisquer consequências legais ou comerciais

O DPO (Encarregado de Proteção de Dados) poderá reunir solicitar auxilio ou maiores informações para o responsável pelo setor em que ocorreu o vazamento de dados, se necessário, delegando tarefas para outros colaboradores, objetivando solucionar o problema da maneira mais célere possível.

Quando uma violação de dados pessoais ou confidenciais tenha acontecido, o DPO deve ser prontamente informado.

6. RESPOSTA

O DPO (Encarregado de Proteção de Dados), sozinho ou em conjunto com o responsável pelo setor em que ocorreu o vazamento de dados determinará o curso apropriado de ação e recursos necessários para limitar o impacto de qualquer violação de dados. Isso pode significar isolar dispositivos e servidores da rede ou tornar redes ou serviços inteiros indisponíveis.

O DPO (Encarregado de Proteção de Dados) pode informar fornecedores ou parceiros de serviço em Segurança da Informação da escola e obter quaisquer conselhos especializados sobre a melhor forma de responder.

O DPO (Encarregado de Proteção de Dados) registrará todas as ações tomadas e as decisões tomadas no registro de incidentes, a ser realizado juntamente com o responsável pela T.I.

Quando uma atividade criminosa possa ter ocorrido, todos os esforços serão feitos para preservar as evidências; isso pode ter precedência sobre a recuperação do sistema.

Medidas apropriadas serão tomadas para recuperar os dados ou restaurar os serviços para retomar o estado normal de operação dos sistemas.

Os indivíduos nomeados expostos em qualquer violação de dados devem ser contatados pelo DPO com detalhes do incidente e quaisquer riscos para eles. Se aplicável, pela natureza ou publicidade do incidente, o DPO também será o responsável pela comunicação com órgãos de imprensa. A esta comunicação, soma-se quaisquer requisitos específicos da Lei Geral de Proteção de Dados, incluindo os prazos legais de comunicação aos titulares e à Agência Nacional de Proteção de Dados.

Os indivíduos não devem pressionar o DPO (Encarregado de Proteção de Dados) para restaurar os serviços em detrimento da devida diligência na execução de suas funções.

7. REVISÃO

O DPO (Encarregado de Proteção de Dados) revisará cada incidente para identificar novos riscos, novos fluxos de trabalho de resposta e alterações nos procedimentos ou políticas necessárias para prevenir incidentes semelhantes e destacar qualquer não conformidade com a política, o que pode resultar em processos disciplinares.

A revisão será encaminhada ao comitê de Lei Geral de Proteção de Dados Pessoais, internamente, caso uma mudança na política seja recomendada.

8. RESPONSABILIDADES

- ✓ O funcionário ou indivíduo que identificar eventual vazamento é responsável por relatar este imediatamente ao DPO (Encarregado de Proteção de Dados).

- ✓ O DPO (Encarregado de Proteção de Dados) é responsável por registrar todos os incidentes de segurança; limitar a disseminação de incidentes e conter a perda de dados; e implementar controles técnicos para evitar incidentes de segurança.
- ✓ A Diretoria do Instituto São José é responsável por revisar incidentes e aprovar as mudanças de políticas propostas.