Documento de normas para incidente de vazamento de fotos pessoais dos clientes da Empresa S.A. para a internet.

Preparação:
Tendo identificado o incidente, é de extrema necessidade da Empresa S.A. o informe a todos da equipe envolvida na manutenção do computador do cliente. Buscando assim a organização entre eles e a preparação para a aplicação das diretrizes de resposta a incidente, tendo essas sido pré estabelecidas nas políticas anteriormente vistas da Empresa S.A. Os colaboradores após o informe devem manter a calma e começar o quanto antes a analise para contenção dos danos, pois o vazamento de dados pessoais dos clientes ameaça quebrar a imagem de mercado da Empresa S.A. que baseasse na confiança prestador -> cliente. Os colaboradores envolvidos devem estar plenamente capacitados para atender gentilmente o cliente quando este retornar assustado questionando sobre suas informações vazadas.

Detecção e Análise:
Com a equipe devidamente alertada e preparada, deve-se iniciar a analise em busca de quais informações do cliente foram vazadas e qual o peso delas para ele. Tendo essas informações, a equipe deve direcionar os esforços para a identificação do COMO, POR ONDE e PORQUE esses dados foram vazados, é de suma importância nesta etapa identificar o POR ONDE pois o vazamento pode significar uma quebra na segurança da rede de toda a Empresa S.A. pondo em risco não somente os dados de vários clientes com a integridade sistêmica da empresa. A identificação do POR ONDE juntamente de COMO auxiliaram diretamente na contenção de danos, sendo informações cruciais, já o PORQUE abre (ou não) o leque para o acionamento de autoridades afim de investigação criminal.

Contingência:
Tendo as devidas informações de origem a Empresa S.A. deve-se isolar a maquina, por onde foi identificado o ataque, da rede; podendo ser utilizado de qualquer métodos decididos pelos colaboradores que não firam o patrimônio. Neste momento a equipe responsável deve organizar-se em três principais grupos, 1. Responsável pelo controle da maquina isolada, 2. Responsável por monitorar a infraestrutura da Empresa S.A. afim de garantir que não aja infecção em/para outros dispositivos da rede, 3. Responsável por capturar o trajeto dos dados vazados dentro das redes, afim de identificar possíveis autores. Tendo como principal objetivo identificar QUEM e o impacto que os dados causados podem causar.

Erradicação:
Identificado o COMO, POR ONDE, POR QUE, QUEM e IMPACTO; a equipe envolvida no incidente deve acionar as autoridades caso necessário, e utilizar de todo o escopo técnico na elaboração de planos corretivos respectivos a cada área de atuação, tendo o corpo técnico TI o foco na infraestrutura, o corpo técnico RH o foco na elaboração de ações judicias e escopos de relações publicas da Empresa S.A. com o cliente e as autoridades, e o corpo técnico administrativo o foco no tocar das atividades da empresa apesar do incidente em ocorrência. Os colaboradores devem buscar a documentação de validação das medidas tomadas, unindo ao reforço na segurança de processos e interfaces dos usuários da Empresa S.A. afim de evitar-se semelhante ocorrido dentro de um curto período.

Restauração:
Após a contenção e entendimento do incidente de segurança ocorrido, a Empresa S.A. deve-

se junto dos colaboradores envolvidos analisar o cenário pós vazamento e buscar as possibilidades de recuperação dos dados vazados e/ou dos danos morais causados ao cliente e a própria organização. Aqui é importante que através de reuniões regulares a equipe envolvida possa minimizar ao máximo as perdas do valor da empresa e os dados do cliente e/ou empresa afetados.

Pós-incidente:
Apesar de medidas já terem sido tomadas durante a resposta ao incidente de segurança, é de extrema importância para a Empresa S.A. que o time de SI juntamente com os envolvidos no incidente discutam e apliquem rotineiramente correções e fortalecimentos para os sistemas de acordo com as vulnerabilidades e dados estudados e analisados durante o incidente. Recomenda-se que após o incidente e definição de novas politicas de segurança da informação a elaboração de reuniões gerais informativas pela Empresa S.A. e que seja atualizado as diretrizes de consentimentos dos clientes de acordo com essas leis.