PLANO DE RESPOSTA A INCIDENTE DA AGÊNCIA REGULADORA DE SERVIÇOS PÚBLICOS DO MUNICÍPIO DE SÃO PAULO -SP REGULA

1) Introdução

A Agência Reguladora de Serviços Públicos do Município de São Paulo – SP Regula, foi criada pela Lei nº 17.433/2020, sob a forma de autarquia de regime especial, vinculada ao Gabinete do Prefeito, com sede e foro no Município de São Paulo e prazo de duração indeterminado.

A lei prevê que a Agência atuará com autonomia administrativa, financeira e orçamentária (art. 2º), e independência e obediência aos princípios da legalidade, imparcialidade, impessoalidade, moralidade, publicidade, proporcionalidade e eficiência, para a regulação e a fiscalização de todo e qualquer serviço municipal delegado que lhe tenha sido atribuído pelo Executivo mediante decreto. (art. 3º)

Até o momento, foram atribuídos pelo Executivo os serviços delegados (concessão, permissão, autorização) de: 1) Saneamento Ambiental: Coleta e destinação de resíduos domiciliares (concessão); Coleta e destinação de resíduos de saúde (concessão); Coleta e destinação de resíduos de grandes geradores (autorização); Coleta e destinação de resíduos da construção civil (autorização). Esses serviços vieram para a Agência por meio do Decreto nº 60.941/21; 2) Iluminação Pública: Manutenção e Modernização da rede de iluminação pública (Parceria Público Privada - PPP); Manutenção e Modernização da rede semafórica (serviço associado à PPP). Esses serviços foram atribuídos para a Agência por meio do Decreto nº 60.941/21; 3) Abastecimento e Lazer: Mercado Municipal Paulistano, Mercado Kinjo Yamato; Mercado Municipal de Santo Amaro, transferido por meio do Decreto nº 61.989/22; 4) Serviços Funerários e Cemiteriais: contratos de concessão que têm por objeto a gestão, operação, manutenção, exploração, revitalização e ampliação de cemitérios e crematórios públicos e a prestação de serviços funerários no Município de São Paulo, assinados em 22/11/2022. A Agência também integrou a Comissão Especial de Transição Institucional do Serviço Funerário do Município de São Paulo (CETISF), responsável pela transição institucional da governança de concessões e a organização e operacionalização da extinção do Serviço Funerário do Município de São Paulo

(SFMSP), que ocorreu em 26/12/2023; 5) Concessão do Circuito de Compras São Paulo SPE S.A, para a Agência Reguladora de Serviços Públicos do Município de São Paulo – SP Regula, o Contrato de concessão de obra pública, da construção, operação, manutenção e exploração econômica do Circuito de Compras foi sub-rogado em outubro de 2023.

A lei prevê que a Diretoria atuará em regime de colegiado e será composta por 5 (cinco Diretores, que decidirão por maioria absoluta, cabendo ao Diretor-Presidente além do voto de qualidade, a representação da Agência e o exercício de todas as competências administrativas. A estrutura organizacional das unidades funcionais da SP Regula foram previstas no Regimento Interno da Agência (Decreto nº 61.425/2022), que estabeleceu as atribuições específicas e comuns das Superintendências, atualmente sete: Jurídica; Planejamento; Supervisão; Regulamento; Contratos de Delegação; Controle interno; Superintendência Administrativa, Financeira, de Tecnologia da Informação e de Pessoal. A estrutura e as atribuições das gerências estão estabelecidas em Resoluções Internas da Agência, de acordo com as atividades desempenhadas e estão divididas em seis: Tecnologia da informação (Res/SPR nº 4/22); Gestão Contábil, Orçamentária e Financeira (Res/SPR nº 5/22; Saneamento Ambiental (Res/SPR nº 6/22); Iluminação pública (Res/SPR nº 7/22); Abastecimento e Lazer (Res/SPR nº8/22); Serviços funerários e cemitérios (Res/SPR nº 9/22).

Na estrutura da SP Regula, a Gerência de Tecnologia e Informação está subordinada à Superintendência Administrativa, Financeira, de Tecnologia da Informação e de Pessoal, que se reporta à Diretoria Executiva da Agência. A Resolução estabelece que a gerência é responsável por: (i) disponibilizar e administrar os recursos de tecnologia da informação e infraestrutura; (ii) desenvolver e manter sistemas de apoio às áreas de negócios da SP Regula; (iii) implementar sistemas de apoio à gestão do SP Regula; (iv) promover a segurança da informação; (v) implementar um processo de transformação digital e uma cultura de inovação contínua; (vi) exercer outras atribuições relacionadas à sua área de atuação que lhe sejam delegadas. A gestão está integrada em duas áreas: Infraestrutura corporativa e desenvolvimento e inovação.

Cabe ao gerente de TI (i) coordenar, supervisionar e gerenciar a execução das atividades relacionadas aos processos de gestão de tecnologia da informação; (ii) disciplinar hierarquicamente o trabalho dos seus órgãos subordinados; (iii) assessorar

o Superintendente Administrativo e Financeiro nos assuntos de sua competência; (iv) exercer outras atribuições relacionadas à sua área de atuação que lhe sejam delegadas.

Diante da Lei de Proteção de Dados Pessoais (Lei nº 13.709/2018) e do Decreto nº 59.767 /2020 que regulamentou a lei no Município de São Paulo, a SP Regula deve realizar o plano de adequação a LGPD. O plano é definido pelo Decreto como "o conjunto de regras de boas práticas e governança de dados pessoais que estabelecem as condições organizacionais, regime de funcionamento, procedimentos, padrões de segurança, padrões técnicos, obrigações específicas para os diversos agentes envolvidos no tratamento, ações educativas, internas mecanismos de supervisão e mitigação de riscos, o plano de resposta a incidentes de segurança e demais aspectos relacionados ao tratamento de dados pessoais" (art. 2°, XIII).

Entre os instrumentos do plano de adequação está a necessidade de realização do plano de resposta a incidentes de segurança. Ademais, o plano de adequação deve conter informações relativas ao tratamento de dados por órgãos e entidades, atender às exigências da ANPD e manter os dados em formato interoperável e estruturado para uso compartilhado de dados e informações (art. 15), deve realizar e manter o mapeamento dos dados pessoais e dos fluxos de dados pessoais existentes em suas unidades; análise de risco; e o relatório de impacto na proteção de dados pessoais, quando solicitado (art. 4º).

A LGPD dispõe no art. 41, § 2º, as atividades que competem ao Encarregado de Proteção de Dados Pessoais: (i) acolher reclamações e comunicações dos titulares dos dados, prestar esclarecimentos e tomar providências; (ii) receber comunicações da autoridade nacional e adotar medidas; (iii) orientar os empregados e contratados da entidade quanto às práticas a serem adotadas em relação à proteção de dados pessoais; e (iv) exercer outras atribuições determinadas pelo controlador ou estabelecidas em norma complementar.

O Encarregado de Proteção de Dados Pessoais é um ator fundamental na estrutura de compliance, sendo responsável por: a) auxiliar no compliance por meio da implementação de ferramentas de responsabilização; b) auxiliar na avaliação do impacto da Proteção de Dados Pessoais; c) auxiliar em auditorias; d) atuar como intermediário entre os interessados – ANPD; titular dos dados e áreas da organização; (e) monitorar o cumprimento da LGPD: (coletar informações para identificar as atividades de tratamento; analisar e verificar o cumprimento das atividades de

tratamento; emitir conselhos e recomendações ao controlador e operador; auxiliar na realização do Relatório de Impacto à Proteção de Dados Pessoais, notificação de dados pessoais; priorizar atividades e esforços baseados no risco; manter registros das atividades de processamento de dados.

2) Breve visão geral dos sistemas, redes e dados críticos da SP Regula

A infraestrutura de rede da SP-REGULA faz parte de rede privada da Prefeitura Municipal de São Paulo fornecida pela PRODAM. A rede local (LAN) está dividia em 3 redes internas, sendo 1 cabeada e 2 sem fio (padrão e serviços).

O acesso externo aos sistemas internos da Prefeitura (intranet), como SIGPEG e SOF (sistema financeiro), ocorre somente via VPN, pois estes serviços estão disponíveis somente na rede privada da PMSP.

Devido a uma decisão estratégica e operacional, os serviços de tecnologia utilizados pela Agência são, majoritariamente, em arquitetura web e hospedados em serviços de nuvem e, portanto, não existe nenhum serviço de tecnologia operando dentro da estrutura física da Agência.

Para o armazenamento corporativo de dados, é usado um serviço em nuvem onde foram criadas pastas departamentais com restrição de acesso controlado pela equipe de TI.

A Agência contrata empresas prestadoras de serviços, a maioria delas junto ao PRODAM, que é uma empresa pública, e realiza o monitoramento.

Existem outros sistemas de gestão contratados, como: (i) o Sistema de Gerenciamento de Resíduos, é acessado para cadastrar geradores de resíduos especiais (Saúde, Construção civil e Grandes Geradores) com controle de acesso para empresas autorizadas. A base de dados pertence à SP Regula mas está sob gestão da empresa contratada detentora do Sistema. Além do cadastro, o sistema emite os documentos necessários para o transporte de resíduos (Controle de Transporte de Resíduo - CTR), que autoriza a empresa a transportar determinados resíduos no âmbito do Município; (ii) O Sistema FISC SP, é utilizado para fiscalização e autuações dos autorizatários da construção civil. Ele gerencia infrações e emite alerta para fiscalização; (iii) O Sistema de Iluminação Pública é de propriedade da concessionária e não está interligado com o

da Prefeitura; (iv) O Sistema Hagape, subrrogado do Serviço Funerário, foi transferido para a SP Regula recentemente e há um contrato com empresa terceirizada para a sustentação e desenvolvimento evolutivo e de suporte. A Agência sub-rogou esse contrato; (v) O Sistema de Recursos Humanos, está hospedado em núvem privada, fornecida pela contratada dentro do contrato de uso do sistema. O Sistema possui um portal web de funcionários em ambiente público, podendo ser acessado de qualquer lugar. Este serviço é publicado em um IP de internet válido. O data center é do fornecedor do sistema e há dados pessoais sensíveis de servidores e funcionários.

Para o armazenamento dos arquivos e materiais corporativos, a Agência criou pastas departamentais acessadas por áreas específicas, com controle interno de acesso pela equipe de TI. O acesso às redes e sites da Internet pelos servidores da Agência é livre, incluindo canais de vídeo e redes sociais. Porém, há restrição a alguns sites e monitoramento do uso e consumo de recursos (proxy) realizado pela Prodam, e caso alguma ameaça seja detectada no monitoramento realizado, a Prodam bloqueia o site.

O Sistema do Serviço Funerário (Hagape) foi desenvolvido para fazer toda a gestão do serviço funerário. O Sistema e o Código fonte eram de propriedade do Serviço Funerário do Município de São Paulo (Autarquia em processo de extinção) e foi transferido para a SP Regula.

3) Prevenção: Medidas preventivas que a SP Regula deve realizar para se prevenir de um ataque cibernético.

Medidas preventivas para proteção contra-ataque cibernético na SP Regula

Face às vulnerabilidades de sistemas de informação (sistemas, redes e dados sewnsíveis), é necessário instituir medidas preventivas para proteção de dados pessoais, e para uma segurança da informação eficaz que garanta a confidencialidade, integridade e disponibilidade de sistemas de informação na SP Regula.

Diante das atividades realizadas pela Agência e da necessidade de adequação da Lei de Proteção de Dados Pessoais, vê-se a necessidade de inclusão de cláusulas gerais e específicas nos contratos da Agência, de acordo com a criticidade dos dados envolvidos. A análise e adequação de contratos visa garantir o cumprimento da Lei

Geral de Proteção de Dados Pessoais - LGPD, para garantir a segurança, adequação e responsabilização da informação.

Nesse sentido, a Encarregada de Proteção de Dados Pessoais revisou os contratos e verificou que eles devem ser aditados para se adequarem a LGPD. Neste momento, a Encarregada está verificando as cláusulas necessárias gerais e específicas que devem ser incluídas e observadas pelas delegatárias e contratadas, para o estabelecimento de responsabilidades e conformidade com a LGPD.

O Plano de adequação da Agência[1], de acordo com o previsto na Lei Proteção de Dados Pessoais[2] (Lei nº 13.709/2018) e no Decreto nº 59.767/2020, que regulamentou a LGPD no Município de São Paulo, será encaminhado para as áreas da Agência com questionamentos necessários para verificar a necessidade de atualização de informações.

Além do plano de adequação que deve conter as informações referentes a tratamento de dados pelos órgãos e entidades, atender as exigências que forem realizadas pela ANPD e manter dados em formato interoperável e estruturado para uso compartilhado de dados e informações (art. 15), deve realizar e manter atualizado o mapeamento dos dados pessoais existentes e dos fluxos de dados pessoais em suas unidades; a análise de risco; e o relatório de impacto à proteção de dados pessoais[3], quando solicitado (art. 4°).

---

[1] O plano de adequação compreendido como "o conjunto das regras de boas práticas e de governança de dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais" (art. 2°, XIII).

[2] A LGPD prevê que a Autoridade Nacional de Proteção de Dados Pessoais - ANPD poderá solicitar ao controlador Relatório de Impacto de Proteção de Dados Pessoais, e deve conter: (i) identificação de agentes de tratamento e do Encarregado; (ii) necessidade de elaboração do relatório; (iii) descrição, natureza, escopo, contexto e finalidade do tratamento o ciclo de vida dos dados pessoais na unidade; (iv) partes interessadas consultadas a fim de obter opiniões legais, técnicas ou administrativas; (v) avaliação da necessidade e proporcionalidade de acordo com a finalidade para a realização de tratamento de dados; (vi) identificação e avaliação de riscos; (vii) medidas para tratar os riscos; (viii) aprovação; (ix) revisão anual.

[3] O relatório de impacto à proteção de dados pessoais é definido como a documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. A LGPD prevê em seu art. 6º que As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: finalidade, adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; responsabilização e prestação de contas. No princípio da adequação deve ser demonstrada a compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento. O Decreto Municipal nº 59.767/2020 que Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta, definiu no art. 2º, XIII, o plano de adequação como o conjunto das regras de boas práticas e de governança de

Na identificação dos agentes de tratamento faz-se necessário a análise de contratos, processos e políticas para atender a LGPD, a implementação de medidas de segurança e de controle de acesso aos dados, sendo necessária a análise da privacidade na concepção dos serviços que estão sendo implementados para que não haja falha de segurança que possa resultar em vazamento de dados, bem como deve ser publicizada no site da entidade a forma como ocorre o tratamento de dados dentro da instituição, garantindo o fácil acesso aos titulares, de forma clara e precisa.

Ademais, a implementação de controles para proteção de dados dentro da entidade envolve a análise de risco de vazamento de dados pessoais e a realização de plano de ação em integridade que contemple a LGPD, treinamentos sobre a lei para todos os funcionários da instituição, controle de acesso, criptografia de dados sensíveis, autenticação multifator, auditoria para análise da segurança da informação e de sistemas.

Essas medidas estão relacionadas ao estabelecimento de uma Governança de Segurança Cibernética eficaz. Embora algumas medidas específicas que fazem parte da "política de segurança da organização", tenham sido previstas no Programa de Integridade, que podem contribuir para o estabelecimento de uma cultura organizacional (Código de Ética, Comitê de Ética, treinamento), e outras a serem implementadas e verificadas por TI (testes de penetração). É necessário fortalecer e instituir novas medidas, pois atualmente não há avaliação; análise; tratamento e monitoramento dos riscos cibernéticos no âmbito da SP Regula e nos serviços prestados pelos delegados e sistemas contratados, com relatório de métricas vigentes, e disponibilização de auditorias periódicas para apuração do escopo da segurança da informação, plano de incidentes de segurança, seguros cibernéticos, entre outros.

---

dados pessoais que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos agentes envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos, o plano de respostas a incidentes de segurança e outros aspectos relacionados ao tratamento de dados pessoais. O Decreto estabelece que cabe às entidades da Administração indireta elaborar a e manter um plano de adequação (art. 10), devendo observar, no mínimo: (i) publicidade das informações relativas ao tratamento de dados em veículos de fácil acesso, preferencialmente nas páginas dos órgãos e entidades na internet; (ii) atendimento das exigências que vierem a ser estabelecidas pela Autoridade Nacional de Proteção de Dados; (iii) manutenção de dados em formato interoperável e estruturado para o uso compartilhado de dados com vistas à execução de políticas públicas, à prestação de serviços públicos, à descentralização da atividade pública e à disseminação e ao acesso das informações pelo público em geral.

Portanto, faz-se necessário realizar algumas mudanças e sugestões sobre como implementar a Governança de Segurança da Informação de forma adequada e de acordo com as atividades da Agência, incluindo a EISP com definição de políticas, com objetivos claros e definidos do que se pretende proteger; definição, análise e monitoramento da segurança de rede da Agência e das contratadas. Observada a avaliação dos riscos sobre dados, informações e atividades da Agência, entre elas a Gestão de Riscos de delegatários para: (i) a garantia do atendimento aos requisitos de cada serviço observado o contexto; (ii) estabelecimento de responsabilidade por não conformidade; (iii) Avaliação de riscos e obrigações contratuais observadas: a) Confidencialidade; b) SLA; c) Resposta a Incidentes; d) Continuidade; e) Segurança física; f) Controle de Acesso; g) Rescisão pela não adequação; h) Direito de Auditoria para analisar a política de segurança cibernética das concessionárias e verificar a necessidade de inclusão ou modificação de cláusulas contratuais, ainda mais considerando ser um sistema com diversos dispositivos e usuários, é fundamental conseguir rastrear cada ação realizada no sistema individualmente. Estabelecer a responsabilidade por essas ações envolve avaliar os logs do sistema que registram o que ocorreu no sistema e quem executou, quais recursos estão envolvidos e quando são acessados. Se o sistema for comprometido, esses logs podem ser rastrear o ocorrido por todo o percurso, e se houve erros de programa ou ações do usuário. As trilhas de auditoria estão diretamente relacionadas a este rastreamento.

A formação e a sensibilização são essenciais para estabelecer uma cultura de segurança da informação e estabelecer a Política de Segurança e Informação na Agência.

Entre as medidas previstas para serem implementadas pela Agência, para proteção contra possíveis ataques cibernéticos, está a contratação de uma empresa de segurança cibernética para realizar um serviço de monitoramento por meio de um Centro de Operações de Segurança (SOC), um Centro de Monitoramento de Segurança com telas e monitoramento de pessoas 24 horas. por dia, monitora firewall, máquinas e fluxo de dados de entrada e saída e Security Information and Event Management (SIEM), para monitorar LOGs e eventos da Agência por meio de SIEM e Endpoint Protection. Quanto aos dispositivos móveis, a ideia é ter uma rede segregada.

Quanto à segurança física, foram recentemente implementados controlo biométrico e monitorização por câmeras em parte da Agência, para garantir a segurança

perimetral. Também é necessário, como mencionado em projetos anteriores, capacitar os colaboradores.

No que diz respeito à segurança da instalação, o edifício onde está instalada a Agência dispõe de uma equipa de bombeiros, de um corpo de bombeiros próprio e de um sistema central de controlo e prevenção de incêndios. Todos os sistemas da agência estão na nuvem e em diversos servidores para garantir a disponibilidade.

Em termos de gestão de compliance, atualmente está em implantação o plano de adequação, à Lei Geral de Proteção de Dados Pessoais – LGPD (Lei nº 13.709/2018), os contratos foram analisados e precisam ser adaptados, com cláusulas de acordo com a criticidade dos dados envolvidos na operação. A adaptação, em fase de implementação, visa garantir o cumprimento da LGPD. O tratamento de dados pessoais realizado pelas áreas da Agência foi mapeado no plano e foram enviadas perguntas para complementar e atualizar informações relacionadas ao fluxo interno, armazenamento, compartilhamento com terceiros, quem decide quais dados pessoais devem ser coletados. Além da adequação dos contratos, será avaliado o estabelecimento de uma política geral para tratar da aplicação da LGPD no âmbito da Agência.

Dada a criticidade de alguns dados pessoais tratados no âmbito da Agência, especialmente relacionados com o serviço funerário, é necessário nomear Administrador destes dados e restringir o controlo de acesso ao Gestor de Informática preferencialmente, para garantir que quem está a aceder ou alterar informação ativos Se você estiver fazendo isso em uma função apropriada e suas ações puderem ser rastreadas, isso será fundamental para proteger as informações, determinar a causa de uma violação e até mesmo relatar incidentes. Além disso, a criptografia neste caso é recomendada. Além disso, a avaliação e gestão dos riscos com a aplicação das medidas necessárias é fundamental para o cumprimento do direito constitucional do cidadão à proteção dos dados pessoais, sendo especialmente relevante a formação e o estabelecimento de uma cultura em segurança da informação dentro da Agência, para conscientizar servidores e prestadores de serviços.

Conforme relatado em outros projetos, é fundamental a capacitação de todos os colaboradores, desde o Conselho de Administração até os estagiários, para a implementação de uma cultura de segurança da informação, estando alguns temas vinculados ao programa de conscientização em segurança cibernética.

O treinamento para colaboradores de áreas que não realizam tratamento de dados pessoais em função de sua função abordará conceitos básicos a) Introdução: LGPD - Da gestão de dados ao uso responsável de dados; b) Principais conceitos, princípios e obrigações de proteção de dados; c) Bases Legais para Tratamento/Tratamento de Dados Pessoais; d) Tratamento/Tratamento de dados pessoais sensíveis; e) Os direitos dos titulares dos dados e a forma de os tratar; f) funções e responsabilidades: o Controlador e o Operador; g) A autoridade nacional de proteção de dados pessoais; h) O papel do Encarregado de Proteção de Dados ´Pessoais e a interação com o resto da organização;

O treinamento deve conter assuntos básicos de conscientização necessários e fundamentais para todos os níveis da organização. Os colaboradores das áreas que têm acesso a dados pessoais sensíveis e informações confidenciais passariam por treinamento com material mais completo e avançado e passariam por treinamento específico para desempenhar suas funções com eficácia e segurança. As áreas da Agência que deveriam ter formação mais avançada na área de segurança de dados e cibersegurança seriam: TI; RH; Controle interno; Saneamento básico; cemitério e serviços funerários.

Fundamentos de Privacidade a) Introdução: LGPD – Da gestão de dados ao uso responsável de dados; b) Principais conceitos, princípios e obrigações de proteção de dados; c) Bases Legais para Tratamento/Tratamento de Dados Pessoais; d) Tratamento/Tratamento de dados pessoais sensíveis; e) Os direitos dos titulares dos dados e a forma de os tratar; f) Estabelecer e implementar uma estrutura de conformidade com a LGPD, g) funções e responsabilidades: o Controlador e o Operador (Processador); h) A autoridade nacional de proteção de dados pessoais; i) O papel do DPO e a interação com o resto da organização; j) exemplos práticos: Princípios de privacidade, intervenientes e direitos dos titulares de dados na prática; l) Proteção de dados desde a conceção e por defeito; m) Avaliações de impacto na proteção de dados; n) Gestão da segurança de dados no âmbito da LGPD/GDPR; o) Incidentes de segurança; p) Violação de dados: Violação de dados pessoais, comunicação, plano de resposta a incidentes. Também um módulo sobre conscientização sobre a importância do servidor reportar imediatamente qualquer ameaça ou incidente.

A análise de riscos e do que é necessário ser implementado para atendimento do direito constitucional do cidadão à proteção de dados pessoais e para a adequação

das normas é medida fundamental. Para isso é necessário, além de implementar as medidas citadas acima, observar a avaliação dos riscos sobre dados, informações e atividades da Agência, entre elas a Gestão de Riscos. Além de treinamento e de cultura em segurança da informação para a conscientização dos servidores e prestadores de serviços, fundamentais para estabelecimento de uma cultura em segurança da informação e na instituição da Política de Segurança e Informação Empresarial (EISP).

4) Planejamento: Envolvidos na Equipe de Resposta a Incidentes e suas funções

Em conformidade com a estrutura organizacional da Agência SP e com o papel da equipe de gerenciamento de incidentes de agir tempestivamente e tomar as medidas técnicas, políticas e legais apropriadas em caso de violação ou incidente cibernético, e de definir ações com procedimentos para a ser seguido, o critério seguido para composição é a competência e atribuições legais para atuação em caso de eventual incidente.

A equipe de resposta a incidentes deverá ser composta por: (i) um membro do Conselho de Administração, a ser escolhido pelo Diretor Presidente; (ii) Superintendente Administrativo, Financeiro e de TI; (iii) Gerente de TI; Analista de Sistemas na área de TI; Analista de Suporte de TI; (iv) Superintendente Jurídico; (v) Superintendente de Controle Interno, atualmente responsável pela Proteção de Dados Pessoais;

(i) Um membro do Conselho de Administração deverá fazer parte da equipe para entender os fatos relatados e detectados, monitorar as informações em tempo real e direcionar quaisquer ações necessárias, além daquelas previstas no plano de resposta a incidentes. A participação de um membro do Conselho é necessária para a avaliação política e agilizará o processo e a tomada de decisões, principalmente na comunicação do incidente.

(ii) Superintendente Administrativo, Financeiro e de TI. Na estrutura da SP Regula, a Gestão de Tecnologia e Informação está atualmente subordinada a esta Superintendência, com as seguintes atribuições: (I) disponibilizar e administrar recursos de tecnologia da informação e infraestrutura; (II) desenvolver e manter sistemas de apoio às áreas de negócios da SP Regula; (III) implementar sistemas de

apoio à gestão do SP Regula; (IV) promover a segurança da informação; (V) implementar um processo de transformação digital e uma cultura de inovação contínua; (VI) exercer outras atribuições relacionadas à sua área de atuação que lhe sejam delegadas. Além disso, a Superintendência é responsável pela Secretaria Executiva, gestão de recursos públicos e de pessoas dentro da Agência.

(iii) A área de TI, composta pelo Gerente de TI, Analista de Sistemas de TI; Analista de Suporte de TI; São os principais intervenientes em todas as fases que envolvem o plano de resposta a incidentes, prevenção, planeamento, avaliação, deteção, contenção, análise.

Os membros da área de TI devem participar de todo o processo de resposta a incidentes, divulgar a importância de comunicar qualquer percepção de ameaça e informar como detectar uma ameaça, como prestar atenção aos sistemas que atuam lentamente; tráfego de rede excepcionalmente intenso; desativação de softwares antivírus, entre outros que devem ser informados em treinamentos para todos os servidores. Os membros da área de TI devem participar de todo o processo de resposta a incidentes, receber informações sobre ameaças ou incidentes, verificar as informações do Sistema, detectar se há ameaça ou violação no sistema, identificar o tipo de ataque, confirmar se a violação é específica ou é generalizado, verifique quais sistemas foram afetados.

Superintendente Jurídico para análise de vazamentos de dados sigilosos, de ilegalidades, de contratos e observações de processos propostos na legislação;

(iv) A Superintendente Jurídica auxiliará na tomada de medidas judiciais, prestando apoio técnico-jurídico, de acordo com suas atribuições de: realizar atividades de consultoria e assessoria jurídica; pronunciar-se sobre assuntos de natureza jurídica ou administrativa, emitindo pareceres jurídicos; opinar previamente, por meio de assessoria técnica, sobre como cumprir decisões judiciais.

(V) A atual Superintendência de Controle Interno Responsável pela Proteção de Dados Pessoais (DPO) é responsável, dentro de suas atribuições legais, por orientar e monitorar os procedimentos e ações relacionadas à proteção de dados individuais, para atendimento à LGPD; orientar as unidades no atendimento às demandas dos órgãos de controle; orientar as unidades no cumprimento dos seus deveres de transparência ativa e passiva; orientar e acompanhar o fluxo de resposta às solicitações de informações relativas ao Regulamento SP ou serviços delegados, e colaborar na interação com

órgãos e entidades da Administração Pública Municipal, demais esferas administrativas e sociedade civil.

A LGPD prevê no art. 41, § 2º, as atividades que competem ao Encarregado de Proteção de Dados Pessoais: (i) acolher reclamações e comunicações dos titulares dos dados, prestar esclarecimentos e tomar providências; (ii) receber comunicações da autoridade nacional e adotar medidas; (iii) orientar os empregados e contratados da entidade quanto às práticas a serem adotadas em relação à proteção de dados pessoais; e (iv) exercer outras atribuições determinadas pelo controlador ou estabelecidas em norma complementar.

O Encarregado de Proteção de Dados Pessoais é um ator fundamental na estrutura de compliance, sendo responsável por: a) auxiliar no compliance por meio da implementação de ferramentas de responsabilização; b) auxiliar na avaliação do impacto da Proteção de Dados Pessoais; c) auxiliar em auditorias; d) atuar como intermediário entre os interessados – ANPD; titular dos dados e áreas da organização; (e) monitorar o cumprimento da LGPD: (coletar informações para identificar as atividades de tratamento; analisar e verificar o cumprimento das atividades de tratamento; emitir conselhos e recomendações ao controlador e operador; auxiliar na realização da DPIA e notificação de dados pessoais; priorizar atividades e esforços baseados no risco; manter registros das atividades de processamento de dados.

5) Preparação: Caso hipotético para treinamento da equipe de Incidente de Resposta

Atualmente um dos serviços mais críticos dentro da Agência é o serviço funerário. Essa percepção ocorre por diversos motivos, tanto na estruturação da área e no estabelecimento de fluxos e processos consistentes para gestão de serviços e fiscalização das concessionárias, quanto pelo tratamento de dados sensíveis acessados e compartilhados entre a SP Regula e os 38 órgãos de atendimento. funeral, e ausência de cláusulas estabelecidas nos termos da LGPD, e desconhecimento de como esse tratamento é realizado pelas Agências.

Para efeitos deste projeto e exercício de treinamento da equipe de resposta a incidentes, é simulado o seguinte: um ataque de malware ao sistema de serviço funerário, para que a equipe de atendimento responda a perguntas.

O serviço é prestado por 4 concessionárias que realizam o atendimento por meio de 38 agências espalhadas por diversas regiões da cidade. A SP Regula é responsável pela regulamentação e fiscalização do serviço.

Não existem políticas ou procedimentos em termos de violação de dados, nem plano de resposta a incidentes. As medidas preventivas estão em fase de implementação. E a equipe de resposta recebe um e-mail da área de comunicação da Agência: “A equipe de comunicação da Agência recebe um e-mail de um jornalista. Pedido de comentários/reação da Agência sobre fuga de dados pessoais.

Para a direção,

Sou jornalista da conceituada publicação "Veja SP". Este jornalista tem conhecimento de alguns casos de suposto vazamento de dados de pessoas cadastradas em lista de beneficiários de programas sociais. Tenho conhecimento de vários outros casos relacionados com denúncias de serviços funerários.

Agradeceria se a Agência pudesse fornecer alguma contribuição ou reagir sobre estes casos que serão publicados em um artigo para nossa próxima publicação, o mais tardar amanhã.

Agradecemos antecipadamente a cooperação. O jornalista"

A equipe de comunicação solicita informações do diretor do DPO no CC sobre como reagir.

DPO recebe uma chamada de

Em cada etapa considere, entre outros, os seguintes pontos: Como agimos?

1) Quais ações são necessárias? Por quem?

2) Que recomendações daríamos?

3) Quais são os riscos? Para quem?

4) Quando devem ser tomadas medidas?

A primeira medida a tomar é detectar se existe um incidente de segurança: Identifique o incidente de segurança, qual é o incidente? Quando ocorreu o incidente? Quem causou isso? Onde? O gestor de TI junto com sua equipe deve agir imediatamente para isolar os sistemas, detectar os dispositivos afetados e analisar o incidente. Identificar a ameaça antecipadamente pode impedir o acesso para dados ou sistemas. Se detectado em tempo hábil, o hacker pode ter acesso à infraestrutura, mas não ter tempo de acessar o banco de dados.

Juntos, vocês devem atuar e designar um dos membros da equipe de TI para comunicar o incidente ao operador do sistema e às concessionárias sobre o incidente para realizar testes e verificar se há alguma outra ameaça ou violação detectada e informar as ferramentas que devem ser utilizadas para detecção. É importante que esta comunicação seja realizada pela equipe de TI para informar tecnicamente o incidente e informar as medidas que julga necessárias serem investigadas no momento.5) Avalie: Trata-se de uma violação de dados pessoais?

6) Quais dados pessoais foram violados? Criticidade dos dados, dados sensíveis?

7) Qual é o impacto provável da violação para as pessoas afetadas?

8) Qual é o número de pessoas afetadas?

9) Quando ocorreu a violação (antes da detecção)?

10) Temos que notificar a autoridade competente? Quais autoridades devem ser notificadas do incidente de violação internamente na Prefeitura e externamente? Que informações devem ser notificadas às autoridades nomeadas?

A ANPD só precisa ser notificada sobre incidente de segurança que possa causar riscos ou danos significativos aos titulares dos dados. Portanto, não é qualquer incidente que precisa ser relatado. Por isso, há necessidade de analisar todas as fases, para só reportar o incidente se for necessário e causar algum dano. Caso a avaliação seja de que pode resultar em risco ou dano relevante, o Encarregado de Proteção de Dados Pessoais deverá notificar a pessoa com as informações jurídicas exigidas pela LGPD.

A LGPD dispõe em seu art. 48 que: "O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa causar risco ou dano significativo aos titulares. § 1º A comunicação será feita em prazo razoável, definido pela autoridade nacional, e deverá mencionar, no mínimo: (I) a descrição da natureza dos dados pessoais afetados; (II) informações sobre os titulares envolvidos; (III) indicação das medidas técnicas e de segurança utilizadas para proteção dos dados, observados os segredos comercial e industrial; (IV) os riscos relacionados ao incidente; (V) os motivos do atraso, caso a comunicação não tenha sido imediata; e (VI) as medidas que foram ou serão adotadas para reverter ou mitigar os efeitos da perda. § 2º A autoridade nacional verificará a gravidade do incidente e poderá, se necessário para salvaguardar os direitos dos titulares, ordenar ao controlador a adoção

de medidas, tais como: (I) ampla divulgação do fato na mídia; e (II) medidas para reverter ou mitigar os efeitos do incidente.

Para preservar os direitos dos titulares e tentar reduzir os possíveis prejuízos que um incidente de segurança possa causar, a ANPD recomenda que a comunicação seja feita o mais breve possível, em até 2 (dois) dias úteis após o conhecimento do fato. No caso do GDPR, o DPA deve ser comunicado se houver probabilidade de riscos aos direitos e liberdades individuais no prazo de 72 horas após o conhecimento da violação.

O diretor designado informará as demais autoridades, Prefeito, Controlador Geral do Município de São Paulo; Delegacia de polícia. Temos que comunicar com os titulares dos dados? Avaliação dos riscos para os direitos e liberdades dos titulares dos dados

Que meios de comunicação serão utilizados para relatar o incidente?

Como será avaliada a gravidade dos dados violados? Ao avaliar o risco do incidente, devemos considerar, entre outros aspectos: natureza, categoria e número de titulares de dados afetados, categoria e quantidade de dados afetados, consequências concretas e prováveis; os potenciais danos materiais, morais e reputacionais que possam ser causados aos titulares; as medidas mitigadoras adotadas pelo controlador após o incidente. Se a violação puder causar consequências significativas ao titular dos dados, como discriminação, risco financeiro, danos materiais, problemas psicológicos.

Que medidas serão tomadas para mitigação? Quem será designado para relatar o incidente de violação e as ações tomadas à equipe? Isolar o sistema afetado, alterar senhas, garantir que o sistema esteja fora de perigo (corrigir problema); documente tudo no caminho. Tome medidas corretivas, como criptografia, treinamento.

Elaborar documentação com a avaliação interna do incidente, medidas tomadas e análise de riscos, para efeito de atendimento ao princípio da responsabilidade e prestação de contas (Art. 6º, X da LGPD).

6) Detecção: Lista com ferramentas que serão utilizadas para detectar eventual violação.

Atualmente a rede é protegida por firewall e o controle de acesso ocorre através de um proxy. Há proteção de endpoint/antivírus. Os sistemas são atualizados automaticamente. A Agência possui uma política de senhas fortes, com alterações

mensais. E são utilizados o sistema WSUS (Windows Serve Update Services), navegador de Internet e pacote office. As atualizações ocorrem a partir de um servidor local. Não existe software na Agência.

Há controle de acesso realizado por áreas e pastas departamentais. Dados de mercado que possam ser de interesse comercial das concessionárias, como os existentes na área de saneamento ambiental, para esses dados há uma auditoria de quem pode solicitar esses relatórios, e quem acessou os dados. Esses dados ficam armazenados em um sistema, um data center que possui diversos mecanismos de segurança, fica em uma rede separada e só se comunica através de um servidor web, da impressora (instalada recentemente) com controle de acesso e de uma pasta com nome para impressão de documentos.

As atuais ferramentas disponíveis na Agência para detecção de ataque cibernético, que seriam utilizadas pela área de TI, são: (i) Endpoint System; (ii) LOGs do sistema; (iii) Análise de tráfego de dados (gráficos); (iv) Sistema de controle de acesso aos equipamentos, com verificação de relatórios, para identificação da máquina ou máquinas que possuem alto tráfego/consumo); (v) Análise de segurança dos LOGs do firewall, para verificar se a rede da Agência está sendo atacada.

Além das ferramentas de segurança disponíveis, os servidores se perceberem qualquer atividade suspeita deve relatar a atividade, pois o usuário é capaz de detector e relatar algo suspeito antes mesmo do alerta de sofisticadas ferramentas de segurança, daí se percebe a importância do treinamento dos agentes no tema, pois tem papel fundamental na segurança da informação e segurança cibernética da Agência.

Conforme dito na introdução, o teste de verificação de vulnerabilidade (pentest) está sendo contratado pela Agência SP Regula; Sistema de backup completo; Sistema Security Operation Center (SOC), com telas e monitoramento de pessoas 24 horas por dia, firewall, monitoramento de máquinas e fluxo de dados, inbound e outbound, e Sistema de Gerenciamento de Informações e Eventos de Segurança (SIEM), para monitoramento de LOGs e eventos de Agência. Essas ferramentas ajudarão a detectar qualquer incidente ou violação.

7) Análise: Identificação de incidente e priorização de incidente no âmbito da SP Regula

O primeiro passo para analisar se o incidente é um ataque cibernético é verificar o que está sendo impactado e determinar o escopo da violação. Analisar se se trata de: (i) um ataque cibernético; (ii) falha processual; (iii) erro humano; (iv) se o incidente está sendo causado internamente; ou se estiver sendo causado por agente externo; (v) se há acesso à rede por agente externo; (vi) se há acesso ou tentativa de acesso por agente externo; (vi) se o serviço é executado por agente externo; (vii) se houver incidente de segurança, o que está sendo afetado, se o acesso foi à infraestrutura ou se houve acesso a alguma informação confidencial ou restrita, ou se houve acesso a dados pessoais; (viii) se houver uma violação de dados que possa afetar a confidencialidade, integridade ou disponibilidade; (ix) se houver "destruição, perda, alteração acidental ou ilegal, divulgação ou acesso não autorizado a dados ou informações"; (x) se houver tratamento ilegal de dados, mas esse tratamento não tiver ocorrido em decorrência de incidente de segurança .

Caso a ameaça seja confirmada, ela deverá ser analisada antes de qualquer ação ser tomada, para confirmar se se trata de um incidente de segurança. Nesse sentido, como vimos nos módulos anteriores, os alertas devem ser analisados para verificar se há alguma ação a ser tomada, pois os incidentes podem ser válidos, mas não significa necessariamente que esteja acontecendo um ataque cibernético.

Se for detectada a ocorrência de um incidente de segurança, a extensão do ataque deve ser analisada para tomar medidas oportunas para reduzir e eliminar os danos. Para isso, é necessário verificar o impacto na organização e nos indivíduos, e verificar o potencial de propagação, e se pode impactar a confiabilidade, integridade e disponibilidade. Devem também ser avaliados o tipo de impacto e a sua avaliação (baixo, médio, alto), se o impacto é funcional ou informativo e o tempo de recuperação do impacto e se é ou não recuperável ou não. Nesse sentido, quanto maior o impacto, mais rapidamente a equipe deverá estar preparada para agir e responder ao ataque, observando as medidas técnicas, legais e políticas necessárias.

Nesse sentido, caso ocorra mais de um ataque ao mesmo tempo e dependendo do ataque, o impacto poderá ser maior para a Agência, assim como seria um ataque de ransomware, em que o acesso a informações e alterações, perda ou roubo de dados poderia ocorrem em dimensões inimagináveis que poderiam impactar jurídica, financeira e politicamente a Agência e a Prefeitura de São Paulo. Este tipo de ataque deve ser priorizado e evitado devido ao potencial de causar danos sem precedentes,

incluindo danos à reputação, tempo e recursos necessários para a recuperação do incidente.

Todos os ataques devem ser considerados para fins de prevenção. O malware também pode causar danos, mas com os atuais sistemas de proteção da Agência poderá ser identificado mais facilmente do que um ataque de ransomware. Embora existam ferramentas e proteções que dificultariam a entrada de malwares, a falta de conhecimento por parte dos servidores sobre segurança da informação, e até mesmo a utilização de dispositivos pessoais sem uma rede separada para uso, poderiam facilitar a entrada deste tipo. de ataque.

O ataque DDoS dentro da Agência, por não haver serviços disponíveis no site da Agência, causaria um impacto menor, pois as informações disponíveis podem ser encontradas em outros sites como Prefeitura, delegados, outros órgãos públicos e até mesmo em comunicados do Agência. imprensa.

Além disso, todas as informações sobre incidentes devem ser documentadas e utilizadas para ações preventivas, para conformidade legal e para informações a serem utilizadas em processos judiciais. Por este motivo, todas as ações realizadas e medidas tomadas devem constar do documento.

8) Contenção:

Após identificar que há um ataque, para evitar que o ataque se espalhe ainda mais, cabe ao departamento de TI desligar a rede e isolar o problema offline, desligando sistemas e redirecionando componentes. A equipe de TI deve identificar se o incidente está ocorrendo em uma máquina, em várias máquinas ou se todas as máquinas estão sendo atacadas e isolar a máquina ou máquinas que estão sob ataque. O gestor de TI junto com sua equipe deve agir imediatamente para detectar os dispositivos afetados, analisar o incidente e realizar backups caso seja necessário utilizá-los em processos judiciais antes de conter a ameaça. No caso da Agência, não há necessidade de manter o serviço disponível para manter as medidas de contenção de ataques.

Portanto, a área de TI deve atuar utilizando Sistema de Proteção contra Intrusão para barrar IPS específicos ou fonte/filtro de ataque; desligue os servidores afetados por malware; Identificar e informar o fornecedor do Sistema sobre o ataque; Adicionar capacidade; Prevenir a reinfecção.

Entre os ativos mais atacados de qualquer organização estão as contas de usuários ou serviços e precisam ser desativados, redefinidos ou ter permissões revogadas caso sejam utilizados ou afetados por uma violação.

É necessário identificar a ameaça antecipadamente para impedir o acesso a dados ou sistemas. Se detectado em tempo hábil, o hacker pode ter acesso à infraestrutura, mas pode não ter tido tempo de acessar o banco de dados. Também se a ameaça pode ainda estar noutro dispositivo ou se pode ter afetado outros sistemas, como os sistemas dos delegados ou dos operadores de sistema da Agência.

Juntos, devem atuar para comunicar o incidente ao operador do sistema e concessionárias sobre o incidente para realizar testes e verificar se há outras ameaças ou violações detectadas e informar as ferramentas que devem ser utilizadas para detecção. É importante que esta comunicação seja realizada pela equipe de TI para informar tecnicamente o incidente e informar as medidas que julgar necessárias serem investigadas no momento. Etapa 7: Comunicação

De acordo com a Seção 4 das notas da Unidade 2, compile um plano de comunicação de crise cibernética detalhando as partes interessadas internas e externas com as quais sua organização precisaria se comunicar em caso de violação. Descreva quais canais de comunicação seriam usados para se comunicar com essas partes interessadas.

9) Comunicação:

Após identificar que há um ataque, para evitar que o ataque se espalhe ainda mais, cabe ao departamento de TI desligar a rede e isolar o problema offline, desligando sistemas e redirecionando componentes. A equipe de TI deve identificar se o incidente está ocorrendo em uma máquina, em várias máquinas ou se todas as máquinas estão sendo atacadas e isolar a máquina ou máquinas que estão sob ataque. O gestor de TI junto com sua equipe deve agir imediatamente para detectar os dispositivos afetados, analisar o incidente e realizar backups caso seja necessário utilizá-los em processos judiciais antes de conter a ameaça. No caso da Agência, não há necessidade de manter o serviço disponível para manter as medidas de contenção de ataques.

Portanto, uma área de TI deve atuar utilizando Sistema de Proteção contra Intrusão para barrar IPs específicos ou fonte/filtro de ataque; desligue os servidores

afetados por malware; identificar e informar o fornecedor do Sistema sobre o ataque; Adicionar capacidade; Prevenir a reinfecção.

É necessário identificar antecipadamente a ameaça para impedir o acesso a dados ou sistemas. Se detectado em tempo hábil, o hacker pode ter acesso à infraestrutura, mas pode não ter tido tempo de acesso ao banco de dados. Também se a ameaça pode ainda ser outro dispositivo ou se pode ter afetado outros sistemas, como os sistemas dos delegados ou dos operadores de sistema da Agência.

Juntos, devem atuar para comunicar o incidente ao operador do sistema e fornecer informações sobre o incidente para realizar testes e verificar se há outras ameaças ou descobertas detectadas e informar as ferramentas que devem ser utilizadas para detecção. É importante que esta comunicação seja realizada pela equipe de TI para informar técnicas sobre o incidente e informar as medidas que julgar possíveis serem investigadas no momento. Etapa 7: Comunicação

De acordo com a Seção 4 das notas da Unidade 2, compilamos um plano de comunicação de crise cibernética detalhando as partes interessadas internas e externas com as quais sua organização precisaria se comunicar em caso de violação. Descreva quais canais de comunicação seriam usados para comunicar essas partes interessadas.

10) Erradicação

Para realizar a erradicação, é necessário identificar o que causou o incidente dentro da Agência. A equipe de resposta a incidentes deve identificar a causa do ataque e o que foi feito para conter todos os dispositivos infectados. Além da limpeza que deve ser realizada, a identificação da ameaça, o interesse que ocorreu por trás dela e a vulnerabilidade são essenciais a serem considerados na erradicação.

A equipe de TI deve analisar os sistemas e verificar se ainda existe algum malware e removê-lo com ferramentas adequadas, como software antivírus. A caixa de ferramentas também é essencial para ajudar a conter o ataque e registrar informações. Além de conter os dispositivos que devem ser utilizados. Além do acima exposto, isolar e desabilitar contas e componentes violados, alterar senhas, remover privilégios de acesso de servidores que foram usados como meio de iniciar o ataque. Aplique patches e reconfigure firewalls. Depois que a ameaça for erradicada, o processo de recuperação poderá começar.

11) Recuperação

Diferentes partes interessadas de toda a organização (desde o departamento de TI, as unidades afetadas, e a diretoria) estão envolvidas no processo de recuperação. Estas partes interessadas podem estar diretamente envolvidas no processo de recuperação ou fornecer orientação sobre o processo a seguir e os prazos que devem ser respeitados. Devem ser priorizados os sistemas que são mais importantes para a atividade retomar as funcionalidades básicas. As interdependências entre sistemas também devem ser compreendidas, pois alguns sistemas só podem ser recuperados após outros.

Uma vez que o ataque possa ser atribuído a um grupo ou indivíduo específico, poderá ser mais fácil se recuperar do ataque, pois a equipe de resposta a incidentes terá uma melhor compreensão da motivação do ataque e dos métodos utilizados.

Durante a recuperação, os sistemas são reconstruídos, reinstalados ou restaurados pela equipe de recuperação de incidentes usando dados de backup. Os arquivos são substituídos por versões limpas e patches são instalados. É importante que os sistemas recuperados sejam testados e monitorizados para garantir que não ocorra reinfecção e que funcionem como deveriam. O processo de recuperação é uma oportunidade para aumentar a segurança com base nas vulnerabilidades descobertas durante as etapas de detecção e análise.

12) Análise pós incidente

As medidas preventivas citadas acima devem ser consideradas numa análise pós-evento de um incidente de segurança.

É necessário avaliar um ataque cibernético após a sua ocorrência para determinar se a resposta ao ataque foi suficiente ou não e para implementar as lições aprendidas. Esta etapa pode começar enquanto a recuperação ainda está em andamento, principalmente se demorar um pouco para que todos os sistemas sejam recuperados. O objetivo desta etapa é melhorar o plano de resposta a incidentes e fortalecer os sistemas para protegê-los de ataques futuros.

Após o incidente deve ser realizada uma reunião com todas as pessoas envolvidas no evento, o mais rápido possível, para análise das lições aprendidas. O

objetivo desta reunião é identificar quaisquer deficiências na forma como a detecção e erradicação do ataque foi tratada. Outra reunião sobre as lições aprendidas com o incidente também deve ocorrer após a recuperação dos sistemas. Isto destina-se a captar suficientemente lições sobre o processo geral de recuperação e sobre como a organização deve melhorar ainda mais a sua resiliência operacional.

Um relatório de incidente (também chamado de relatório post-mortem) deve ser compilado após a conclusão da reunião de lições aprendidas. Este relatório não servirá apenas como referência para planejar ataques futuros, mas também será útil como ferramenta de treinamento no futuro. Também pode ser usado como prova caso surja alguma questão legal devido ao ataque.

O relatório deve abordar: (i) O tipo e natureza do incidente; (ii) Se o incidente poderia ou não ter sido evitado; (iii) Como e quando o incidente foi detectado e se são necessárias melhorias nas ferramentas de detecção; (iv) Os sistemas afetados pelo ataque; (v) Como a organização respondeu ao ataque e o que poderia ter sido feito melhor durante o processo de resposta ao incidente; e (vi) Recomendações para melhorar o processo de resposta daqui para frente.

Todas as lições aprendidas com a análise pós-evento devem ser implementadas para reduzir o risco de ocorrência de incidentes futuros e para garantir que a organização esteja melhor preparada caso um ataque ocorra novamente. Pode ser necessário fazer alterações em políticas, processos e procedimentos, em ferramentas e equipamentos e até mesmo no comportamento das partes envolvidas no processo.

As melhorias devem ser categorizadas como de curto ou longo prazo. As melhorias a curto prazo podem ser feitas imediatamente, enquanto as melhorias a longo prazo estão relacionadas com mudanças estratégicas, como a reformulação completa de certos processos, que levarão mais tempo a implementar. Planos de ação que incluam partes responsáveis, prazos e resultados devem ser criados para garantir que todas as partes interessadas saibam o que se espera delas. O plano de resposta a incidentes atualizado e melhorado também deve ser testado antes de ser implementado para determinar se as melhorias introduzidas são suficientes.