tecnologia a serviço da cidade
procempa

Política de Segurança da Informação

Setembro, 2022

Sumário

Apresentação

A Revolução Digital consolidada nas últimas décadas tornou possível um enorme avanço: a coleta, contabilização e processamento de quantidades significativas de informações do turbilhão de eventos que ocorrem todos os dias na sociedade. Hoje podemos extrair mais facilmente dessas informações dados que servem como farol orientador importantíssimo para tomada de decisões e identificação de oportunidades.

Na medida em que as informações são usadas para decisões importantes, seu valor é reconhecido e deve ser preservado. Algumas informações não devem cair nas mãos erradas. Adulterações e indisponibilidade podem levar a decisões erradas ou falta de ação. O grande valor atrai grandes ameaças. Ouvimos notícias quase que diariamente sobre vazamentos de dados, espionagem, ransomware e ataques hacker em todo tipo de organização. Importante ressaltar que a Segurança da Informação não deve atuar apenas sobre os sistemas digitais e sim em todos os meios onde a informação reside.

Estas são as bases e justificativas para a Segurança da Informação, que visa a manutenção da Confidencialidade, Integridade e Disponibilidade dos dados e informações. E o instrumento importante de Governança é a Política de Segurança da Informação (PSI), um conjunto de diretrizes, normas, procedimentos e padrões que devem ser seguidas pela instituição como um todo, para que sejam assegurados seus recursos computacionais e suas informações.

As diretrizes estabelecidas nesta política a serem observadas pelo corpo técnico e gerencial, colaboradores em geral, terceiros e fornecedores. A responsabilidade é de todos. De forma especial, a Equipe de Segurança da Informação da PROCEMPA é guardiã da aplicação desses princípios. Emite pareceres e contribui para elaboração de termos de referência quanto a segurança em projetos, contratações e aquisições, sem de forma alguma impedir a inovação com o controle totalitário da informação. Mas sim, deve orientar o uso das melhores práticas, controlar e monitorar o fluxo das informações, como forma de evitar incidentes indesejados, adicionando capacidade de predizer ataques, identificando vulnerabilidades e as preliminares que ocorrem antes dos incidentes.

Da mesma forma, a Equipe de Proteção de Dados da PROCEMPA, supervisionada pelo Encarregado de Tratamento de Dados Pessoais, atua em relação a preservação da privacidade, direito fundamental definido na Constituição Federal e na conformidade com a Lei Geral de Proteção de Dados Pessoais.

Ambas as equipes devem colaborar para garantir que os empregados tomem conhecimento da existência e sigam as políticas e normas expressas nesta PSI e documentos relacionados, oferecendo treinamentos e campanhas de conscientização oportunamente.

As mudanças no mundo digital ocorrem rápido demais para impedir todos os possíveis ataques, portanto é preciso também investir em resiliência, sistemas redundantes, tolerantes a falhas e dar respostas rápidas para ocorrências de comprometimento e limitação de impactos. Para isso, é preciso um time de resposta rápida a incidentes, como uma brigada de incêndio, cuja organização é definida na Politica de Resposta a Incidentes, uma das normas subordinadas a esta PSI.

Espera-se que esse trabalho possa ajudar a PROCEMPA a aprimorar a Segurança da informação, contribuindo para sempre colocar a tecnologia a serviço da cidade.

Definições e Referências

- LGPD – Lei Federal nº 13.709/2018, a Lei Geral de Proteção de Dados Pessoais.
- LAI – Lei Federal nº 12.527/2014, a Lei de Acesso a Informação.
- Marco Civil da Internet, Lei Federal nº 12.965/2014
- SGSI – Sistema de Gerenciamento de Segurança da Informação, tratado pela família de normas técnicas ISO 27000, no Brasil publicadas pela Associação Brasileira de Normas Técnicas (ABNT), sob a nomenclatura NBR ISO/IEC 27000.
- Confidencialidade – propriedade de que o dado ou informação não seja disponibilizado ou revelado a sistema ou pessoa (física ou jurídica), não autorizada e credenciada.
- Integridade – propriedade de que o dado ou informação não seja modificado, excluído ou adulterado – intencionalmente ou não – por pessoas, sistemas, defeitos, acidentes ou forças da natureza, mantendo sua confiabilidade e consistência.
- Disponibilidade – propriedade de que o dado ou informação possa ser acessado por pessoa ou sistema autorizado, quando solicitado, em tempo razoável para sua utilização.
- Autenticidade – registro da fonte da informação, garantida pela Integridade, possibilitando identificar a identidade da pessoa, entidade ou sistema que a presta.
- Dado Pessoal – dado ou informação relacionada a pessoa natural identificada ou identificável.
- Dado Pessoal Sensível – dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde, ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural, conforme definido pela LGPD.
- Dados Confidenciais – todos aqueles que devem ter acesso restrito e aos quais se aplica o princípio da Confidencialidade.
- DPO – Encarregado pelo Tratamento de Dados Pessoais, com atribuições definidas na LGPD.

Diretrizes

Estes são os princípios básicos que regem a Política de Segurança da Informação da PROCEMPA, estabelecidos de acordo com as necessidades da instituição. Violações a essa PSI devem ser mitigadas e podem sujeitar os responsáveis às penalidades aplicáveis, que serão definidas de acordo com a gravidade da ocorrência, podendo envolver advertência, suspensão, rescisão contratual por justa causa ou outras medidas cabíveis, de acordo com o Código de Conduta e Integridade da PROCEMPA.

1. Além das informações organizacionais, à PROCEMPA é atribuída a guarda de informações de seus clientes diretos e indiretos, fornecedores, empregados, terceiros e estagiários. Portanto, a criação de um ambiente que garanta a Segurança da Informação, com a devida confidencialidade, integridade e disponibilidade, bem como o respeito e proteção da privacidade é essencial para a continuidade de negócio da companhia. Para isso, devem ser utilizados mecanismos e controles de Segurança da Informação, balanceando fatores de risco, tecnologia e custo, buscando formas de compatibilizar o desenvolvimento tecnológico, livre iniciativa e a inovação, respeitando a autodeterminação informativa, o direito a informação, a liberdade de expressão, o direito a opinião, a inviolabilidade da honra e da imagem, o livre desenvolvimento da personalidade e a cidadania.

2. Toda a informação deverá ser classificada formalmente quanto à sua confidencialidade e ter tratamento de acordo com a sua classificação, independente da sua forma de armazenamento, digital ou não, seguindo orientações da Política de Acesso e Classificação de Dados. Deve-se garantir a proteção adequada das informações e dos sistemas contra acesso indevido, cópia, leitura, modificação, destruição e divulgação não autorizados. Que sejam utilizados apenas para as finalidades aprovadas pela companhia, estando sujeitos à monitoração, rastreabilidade e auditoria.

3. Os sistemas em produção devem estar identificados, inventariados, documentados e classificados quanto a sua criticidade, registrada em inventário. Em especial, deve-se assegurar a existência de procedimentos de continuidade de negócios documentados para todos os sistemas críticos da companhia e de seus clientes. Para sistemas que tratam dados pessoais, deve-se ter os dados categorizados e inventariados. Sempre que possível, devem ter também Relatório de Impacto de Proteção de Dados, de acordo com os princípios da LGPD.

4. Dados Pessoais, sensíveis ou não, são considerados confidenciais, e devem ser protegidos de acordo com a LGPD em sua redação vigente. Cuidados redobrados devem ser tomados em relação a Dados Pessoais Sensíveis, aqueles que podem revelar origem racial, étnica, opinião política, convicção religiosa, filosófica, filiação sindical, dados genéticos ou biométricos, relacionados a saúde, vida sexual ou orientação sexual.

5. As informações, dados e registros devem ter o ciclo de vida programado. Cumprido o ciclo de vida, se consideradas confidenciais, quando não mais necessárias, devem ser destruídas. O descarte ou reutilização de mídias, digitais ou não, que as contém ou contiveram deve ser feito de forma a impossibilitar recuperação das mesmas.

6. A Segurança da Informação e a Privacidade devem ser tratadas sempre em todas as etapas de projetos e por todo o ciclo de vida dos serviços e produtos da PROCEMPA.

7. Caso o produto ou serviço ofereça alternativas opcionais para o usuário final, devem ser indicadas, sugeridas e escolhidas por padrão as alternativas que se acredita serem as que oferecem mais segurança e privacidade para o usuário.

8. Controles de segurança devem ser adotados em conformidade com a legislação e normas vigentes, suportando o desenvolvimento tecnológico e inovação, conforme definições de gestão de riscos e vulnerabilidades. Em especial, devem ser implantados os Controles de Segurança da Informação Críticos.

9. Todos os equipamentos da companhia ou instalados em suas dependências deverão estar inventariados e identificados de forma individual, protegidos, com documentação atualizada e de acordo com as cláusulas contratuais, regulamentação e legislação em vigor, permitindo a sua localização a qualquer tempo, bem como a identificação dos responsáveis por sua utilização.

10. Identificações, credenciais ou senhas de sistemas da PROCEMPA são individuais, não compartilháveis e intransferíveis. O usuário é responsável por todas as atividades desenvolvidas com sua identificação e senha, por isso deve manter a senha em sigilo e trocá-la periodicamente.

11. Os recursos, sistemas, produtos e serviços colocados em produção devem ser testados anteriormente para a verificação de possíveis impactos no processo produtivo.

12. A contratação de produtos ou serviços de tecnologia deve considerar os pareceres da Segurança da Informação e Privacidade. Os trabalhadores, diretos, terceiros ou estagiários, durante a vigência e após o término do contrato de trabalho ou prestação de serviço, não podem se apropriar de informações confidenciais.

13. Todo o trabalhador conhecendo qualquer incidente, desvio, falha ou violação das normas relacionadas a Segurança da Informação, deve notificar imediatamente seu superior e a Equipe de Segurança da Informação. Se há mera possibilidade de impacto a Dados Pessoais, sensíveis ou não, deve ser notificado também o DPO, que de acordo com as leis e regulamentações deve ter condições de verificar a obrigação de comunicar incidentes aos titulares dos dados pessoais envolvidos, autoridades competentes e tomar outras providências.

Normas relacionadas a PSI

Conforme as melhores práticas, a PSI da PROCEMPA é dividida de forma hierárquica, e se relaciona com uma série de documentos mais específicos, que refletem as diretrizes apresentadas aqui. Eventuais desvios ou exceções em relação a estas Políticas devem ser documentados e mitigados dentro de prazos razoáveis.

- Política de Segurança Física – mitigação de riscos e ataques diretos a equipamentos e infraestrutura nas dependências da companhia.
- Política de Mesas e Telas Limpas – normas para evitar a exposição de dados e informações em ambiente de escritório.
- Política de Uso Geral da Rede e Equipamentos – descreve as regras e melhores práticas para utilização segura da rede, credenciais, serviços, sistemas e equipamentos fornecidos pela companhia para fins de trabalho, ou trazidos pelo usuário (BYOD).
- Política de Acesso e Classificação de Dados – estabelece as políticas de acesso e classificação de informação nas bases de dados da PROCEMPA.
- Política de Produtos, Serviços e Servidores – com regras para produtos, serviços e servidores disponíveis na rede.
- Política de Cópias de Segurança – referência para cuidados e obrigações quanto a cópias de segurança (backups) dos dados e sistemas da companhia.
- Política de Retenção de Registros – definição do ciclo de vida para registros (logs) de acesso e sistemas.
- Plano de Resposta a Incidentes – fornece meios de resposta rápida a incidentes de segurança e privacidade
- Política de Privacidade – descreve e estabelece regras para o tratamento de dados pessoais feito pela companhia