POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Município de Santa Lúcia

2024

PREFEITURA MUNICIPAL
SANTA LÚCIA

Prefeitura Municipal de Santa Lúcia

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Fevereiro

2024

RESUMO

A Revolução Digital, que se fortaleceu nas últimas décadas, propiciou um avanço de forma extraordinária a capacidade de coletar, contabilizar e processar volumes significativos de dados provenientes da sucessiva efervescência de eventos na sociedade. Na atualidade, pode-se extrair com maior facilidade informações valiosas desses dados, as quais servem como uma orientação fundamental tanto para a tomada de decisões quanto para a identificação de oportunidades. Dado que os dados exercem um papel vital na tomada de decisões importantes, sendo assim seu valor é amplamente reconhecido e deve ser protegido. Todavia, esse valor substancial também atrai ameaças significativas, as quais devem ser evitadas para inibir que os dados caiam nas mãos erradas. Quanto a adulteração ou a falta de disponibilidade dos dados podem decorrer em decisões equivocadas. Contudo esses princípios fundamentais esclarecem a importância da segurança da informação, que foca assegurar a confidencialidade, integridade e disponibilidade das informações. Um instrumento essencial para alcançar esse objetivo é a implementação de uma Política de Segurança da Informação, cujo consiste em um conjunto de diretrizes, normas, procedimentos e padrões a serem seguidos por todos os usuários da infraestrutura do município de Santa Lúcia.

Palavras – chave: Revolução digital, avanço, coleta, processamento, dados, eventos, sociedade, informações, tomada de decisões, oportunidades, valor, reconhecido, preservado, ameaças, adulterações, indisponibilidade, confidencialidade, integridade, disponibilidade, segurança da Informação, política de segurança da Informação, diretrizes, normas, procedimentos, padrões, infraestrutura, companhia, município, Santa Lúcia.

ABSTRACT

The Digital Revolution, which has strengthened in recent decades, has provided an extraordinary advancement in the ability to collect, account and process significant volumes of data arising from the successive effervescence of events in society. Nowadays, valuable information can be more easily extracted from this data, which serves as fundamental guidance for both decision-making and identifying opportunities. Given that data plays a vital role in making important decisions, its value is widely recognized and must be protected. However, this substantial value also attracts significant threats, which must be avoided to prevent data from falling into the wrong hands. Tampering or lack of availability of data can result in mistaken decisions. However, these fundamental principles clarify the importance of information security, which focuses on ensuring the confidentiality, integrity and availability of information. An essential instrument to achieve this objective is the implementation of an Information Security Policy, which consists of a set of guidelines, norms, procedures and standards to be followed by all users of the infrastructure of the municipality of Santa Lúcia.

Keywords: Digital revolution, advancement, collection, processing, data, events, society, information, decision making, opportunities, value, recognized, preserved, threats, tampering, unavailability, confidentiality, integrity, availability, information security, information security policy , guidelines, norms, procedures, standards, infrastructure, company, municipality, Santa Lucia.

SUMÁRIO

CAPÍTULO 1

1.0 INTRODUÇÃO

A segurança da informação é uma preocupação essencial em um mundo cada vez mais digital e em constante modernização. A proteção dos dados corporativos contra ameaças tanto internas quanto externas é fundamental para assegurar a continuação dos negócios e a confiança dos clientes. Este documento determina as diretrizes e procedimentos principais para a implementação efetiva das políticas de segurança da informação no município de Santa lúcia. Contudo ao seguir estas orientações, pretendemos fortalecer nossa postura de segurança e amenizar os riscos associados à manipulação e compartilhamento de informações sensíveis.

CAPÍTULO 2

2.0 DEFINIÇÕES E REFERÊNCIAS

As definições e referências do projeto estarão destacadas logo abaixo:

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 à 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 seu uso.
- 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, dados tanto genético quanto 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.

CAPÍTULO 3

3.0 INSTRUÇÕES

Estes são os princípios básicos que regem a Política de Segurança de Santa Lúcia, estabelecidos de acordo com as necessidades da instituição, destacados logo abaixo.

À cidade de Santa Lúcia é atribuída a guarda de informações de seus clientes diretos e indiretos, fornecedores e empregados. Portanto, a criação de um ambiente que garanta a disponibilidade e proteção é fundamental para a continuação de negócio da instituição.

- Toda a informação deverá ser classificada formalmente quanto à sua confidencialidade, disponibilidade, integridade e ser tratada conforme a sua classificação, independente da sua forma de armazenamento, digital ou não.

- As informações e dados pessoais pertencentes a pessoa natural identificada, devem de forma obrigatória ser protegidos conforme a Lei Geral de Proteção de Dados (LGPD) e analisados confidencialmente quando não houver justificativa legitima em contrário. Atenção redobrada deve ser tomada em relação aos dados pessoais sensíveis, referente aqueles que podem revelar origem racial, étnica, convicção religiosa, opinião política, filosófica, dados genéticos ou biométricos, relacionados a saúde, vida e orientação sexual.

- Informações devem possuir um ciclo de vida de maneira programada. Onde as informações consideradas confidenciais não mais necessárias, devem ser destruídas através de mecanismos adequados, todavia esse descarte ou reutilização de mídias devem ser feitos de forma a impedir a recuperação das mesmas.

- O indivíduo que tenha acesso as dependências da prefeitura devem ser identificadas. Quanto ao acesso de terceiros em áreas onde exista o processamento físico ou digital de informações deverá ser fundamentado pela estrita necessidade e deverá acontecer constantemente com o acompanhamento responsável pelas informações no setor.

- A Companhia requer que todos os equipamentos sejam devidamente inventariados e identificados de maneira individual. Essa medida é primordial para assegurar o controle apropriado dos ativos e facilitar a gestão eficiente dos recursos tecnológicos.
- O usuário é responsável por todas as atividades desenvolvidas mediante ao seu cargo e realizar as ações de manutenção apropriadas, portanto deve zelar tanto por sua proteção quanto ao sigilo.
- É imprescindível que quaisquer alterações no âmbito de trabalho sejam meticulosamente planejadas, formalizadas por meio de processos padronizado, comunicadas, autorizadas e, sempre que possível, testadas em um ambiente apropriado antes de serem estabelecidas. Essas medidas possuem um foco em avaliar e diminuir os impactos potenciais nas operações, garantindo a estabilidade do ambiente produtivo.
- Durante e após o término do contrato de trabalho ou prestação de serviço, é proibido que colaboradores se apropriem tanto das informações quanto dos recursos tecnológicos da prefeitura, incluindo e-mail corporativo, planilhas, arquivos de dados, vídeos, mídias, equipamentos, componentes ou até mesmo acessórios associados a essas informações do instituto.
- É de responsabilidade de todos os funcionários garantir a segurança das informações. A prefeitura de Santa lúcia realizará treinamentos para promover a conscientização e preparo dos colaboradores nesse aspecto.

3.1 NORMAS E SEGURANÇA FÍSICA

Quaisquer violações das normas determinadas, incidentes, indício de um possível vazamento de dados ou até mesmo falhas de segurança devem ser comunicadas de imediato a diretoria da prefeitura.

Em relação a segurança física as diretrizes de segurança na prefeitura de Santa lúcia abrangem diversas medidas primordiais para assegurar a proteção dos ativos e informações da empresa, sendo assim isso inclui a obrigação da utilização de digital como identificação por todos os indivíduos que adentram as instalações, o controle do acesso de pessoas externas mediante autorização e acompanhamento, além da necessidade de uma documentação adequada para o ingresso e saída de equipamentos. Os prestadores de serviços do município também são responsáveis

pela integridade do patrimônio, prejuízos ocasionados por seus empregados ao patrimônio e pela confidencialidade das informações acessadas. Dessa maneira é exigido o descarte bem seguro de documentos e mídias que contenham informações particulares quando não forem mais necessários, além da entrega de documentos confidenciais somente mediante registro. Por fim, os equipamentos internos são periodicamente inventariados, e apenas funcionários autorizados podem realizar o remanejamento de equipamentos com foco na segurança e integridade dos ativos da empresa.

3.2 CREDENCIAIS

A segurança de acesso na prefeitura de Santa lúcia destaca a importância das credenciais individuais, identificações e senhas de acesso como elementos essenciais para a proteção dos sistemas e informações. É destacado que essas informações precisam ser mantidas em sigilo e de forma alguma nunca serem compartilhadas. Além do mais, os funcionários são instruídos a trocar constantemente suas senhas e a escolher senhas robustas, longas e complexas para assegurar a segurança dos dados. Também é salientado que as senhas devem ser exclusivas, não devendo ser usadas em nenhum outro sistema ou serviços não gerenciados da prefeitura, seja em contextos pessoal ou profissional, visando evitar comprometimentos de segurança.

CAPÍTULO 4

4.0 REDE E SUA UTILIZAÇÃO

A utilização da internet na prefeitura de Santa lúcia determina as diretrizes de maneira clara para garantir o uso adequado dos recursos online. O acesso à internet é oferecido para fins corporativos, embora acessos lícitos de natureza pessoal sejam permitidos em horários não comerciais, desde que não violem outras normas. É explicitamente proibido o acesso a conteúdo pornográfico, ou difamatório ofensivo. A Companhia reserva-se o direito pelo monitoramento e registro dos acessos à internet, podendo até mesmo a bloquear sites considerados inadequados. Além de tudo, a política restringe a utilização indevida do correio eletrônico, proibindo participações no envio de mensagens ofensivas, comerciais ou de spam. O compartilhamento de recursos e a conexão de equipamentos pessoais à rede da empresa são sujeitos a regulamentação e controle.

CAPÍTULO 5

5.0 PRESERVAÇÃO DE ESTAÇÕES

A política de proteção de estações na instituição planejada para 2025 e 2026 determina medidas para garantir a segurança dos sistemas. Incluindo a instalação de Firewall, ativação e atualização do antivírus na prefeitura e em todas as suas estações de trabalho, notebooks e computadores indicados pela equipe de administração do antivírus. Os usuários são proibidos de obstruir a operação e atualização do antivírus sem quaisquer autorizações. Contudo em casos de algum problema com o antivírus, os usuários devem comunicar de imediato aos responsáveis pela administração do antivírus para que as providências sejam tomadas.

5.1 POLÍTICA DE USO DOS PROGRAMAS

A política de software na organização determina diretrizes com clareza para a utilização e instalação de programas nos equipamentos disponíveis. As estações de trabalho são configuradas com o mínimo primordial de programas para suas funções básicas. A empresa reserva-se o direito de efetuar verificações periódicas no inventário dos equipamentos em desenvolvimento ao longo de 2025 dos hardwares e ao software, para assegurar o cumprimento das normas designadas.

CAPÍTULO 6

6.0 BACKUP

A política de backup na prefeitura determina as responsabilidades dos responsáveis pelos servidores no que diz respeito à segurança e proteção dos dados. Cada usuário é responsável por manter cópias de segurança de seus próprios arquivos, cujo devem ser armazenados em autorização pelo instituto. É proibida a cópia de dados confidenciais para serviços externos não autorizados. Esses mesmos dados confidenciais devem estar criptografados nos backups onde é recomendada sempre que possível, dessa forma os responsáveis pelos servidores devem assegurar a execução de backups de informações críticas, testando periodicamente os processos de restauração. Além do mais, os meios de armazenamento dever ser guardados em locais seguros, e a equipe responsável deve garantir a disponibilidade dos backups pelo tempo determinado por lei, juntamente com os equipamentos essenciais para sua recuperação quando necessário.

CAPÍTULO 7

7.0 SISTEMATIZAÇÃO E APLICAÇÃO

A política de segurança de dados no município determinara diretrizes rigorosas para proteção das informações sensíveis durante os anos de 2025 e 2026 em conformidade com a LGPD. Em relação ao desenvolvimento e manutenção dos sistemas, é obrigatório a utilização de software e controle de arquivos aprovados pelo instituto como modelos, documentos, diagramas, páginas web ou até mesmo fontes, sendo que cada desenvolvedor é responsável pela integridade dos arquivos e adesão às recomendações de segurança aplicáveis.

.

CAPÍTULO 8

8.0 AUDITORIA, DOCUMENTAÇÃO E SEGURANÇA SERVIDOR

A diretriz de segurança de servidores na prefeitura, tem como planejamento estabelecer procedimentos rigorosos entre o para assegurar a integridade e segurança dos sistemas. Incluindo a instalação padronizada de servidor com pacotes obrigatórios, seguidos por uma verificação adicional efetivadas pela equipe técnica. As atualizações de segurança devem ser adotadas pelo responsável do servidor, seguindo protocolos de backup, horário adequado e também plano de recuperação de falhas. O acesso remoto deve ser de maneira criptografada. Além do mais, a ativação de novos serviços de rede estará sempre sujeita a uma análise de riscos, com restrição à instalação de serviços não autorizados. Quanto ao tráfego de informações confidenciais deve ser realizado proteções, cujo os firewalls devem ser configurados para permissão de acesso meramente a redes ou máquinas autorizadas. Profissionais da área técnica ou segurança tecnológica podem utilizar ferramentas de detecção e prevenção de ameaças para identificação e registro referentes a tentativas de invasão.

A obrigação dos administradores é de habilitarem registros de segurança para auxilio no tratamento de recuperação de falhas, contabilização e auditorias. Contudo esses registros devem ser analisados frequentemente, seja por meios manuais ou até mesmo por processos automatizados, assegurando a eficiência do sistema de segurança e a detecção precoce de potenciais problemas. Abordando a documentação exigida na empresa pode-se destacar a importância de registrar que sistemas críticos tenham documentado o plano de continuidade de negócio ou recuperação de desastre para sistemas primordiais. Além de tudo, todas as atualizações e instalações devem ser corretamente documentadas pelo responsável, abarcando procedimentos de correções aplicadas, softwares instalados e atualizados, instalação, permissões de acesso, configurações implementadas, contatos para suporte e outras informações relevantes, visando garantir a transparência e a gestão eficaz dos sistemas.

Em relação a segurança física de servidores na empresa, determina ações para proteção a infraestrutura contra acessos não autorizados e garantir o funcionamento adequado dos equipamentos. Em relação ao acesso físico dos servidores e equipamentos é restrito exclusivamente a funcionários e terceiros autorizados, tendendo a segurança dos dados. Além do mais, os servidores e equipamentos devem atuar em ambientes que na qual cumpram às condições recomendadas pelo fabricante, incluindo temperatura, nível de poeira e umidade, para garantir o desempenho e a durabilidade dos sistemas.