Quais são as nossas recomendações?

DIRETRIZES BÁSICAS DE SEGURANÇA DA INFORMAÇÃO

- Definir e publicizar, no mínimo, no âmbito do próprio Órgão Setorial, políticas internas que descrevam uso aceitável, entendido como sendo a diligência do usuário em compreender que os ativos de informática da Prefeitura são ativos corporativos (e não pessoais) e atuar para que haja adequada distinção no uso e armazenamento dos dados corporativos e pessoais, bem como requisitos básicos de segurança para, posteriormente, desenvolver mais padrões e especificações como parte da melhora do processo de gestão de riscos.
- Investir em capacitações técnicas de Segurança da Informação atualizadas e apropriadas para o corpo técnico de tecnologia da informação e comunicação, inserindo-as no planejamento de capacitação em tecnologia da informação e comunicação do Órgão Setorial.
- Aprimorar a gestão de ativos de microinformática, com a implantação de um inventário atualizado, preferencialmente de modo automatizado, e seguindo o disposto em outras Orientações Técnicas.

> Criptografar os dados sensíveis nos equipamentos utilizados pelos usuários finais (endpoint). Computadores, notebooks e dispositivos móveis (smartphone, tablet, etc...) devem utilizar ferramentas de criptografia para a proteção dos dados sensíveis.

> Criptografar os dados sensíveis em repouso armazenados nos servidores físicos (próprios ou contratados), virtuais ou em nuvem.

- Aprimorar a gestão de redes corporativas sem fio, protegendo adequadamente por meio de mecanismos como autenticação de usuários e criptografia de tráfego.
- Aprimorar a gestão de sistemas, incluindo-se eventuais nuvens e ambientes de IoT (internet das coisas), e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de licenças e patches de software, com a implantação de um inventário atualizado, preferencialmente de modo automatizado, e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de licenças e patches de software, com a implantação de um inventário atualizado, preferencialmente de modo automatizado, e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de dados, incluindo códigos-fonte, com a implantação de repositórios apropriados e métodos de classificação de informações, e seguindo o disposto em outras

Orientações Técnicas.

- Aprimorar a gestão de usuários e permissões de acessos, com a implantação e execução do ciclo de vida de usuários e acessos, e seguindo o disposto em outras Orientações Técnicas.
- Aprimorar a gestão de aquisições, buscando inclusive obter maior padronização dos ativos, em compasso com o inciso I do Artigo 15 da Lei 8.666/1993, e seguindo o disposto em outras Orientações Técnicas.
- Realizar a gestão da qualidade da Segurança da Informação, com o desenvolvimento e aplicação de indicadores, bem como avaliação periódica de ambientes e sistemas chaves em termos de Segurança da informação.
- Incluir questões de segurança na gestão da mudança.
- Estabelecer controles e definir os respectivos processos de controle, incluindo a definição de níveis de aceitação.
- Considerar necessidades de compliance regulatório por força de outros normativos, tais como a Lei Federal 13.709/2018 (Lei Geral de Proteção de Dados) e a Lei Federal 12.965/2014 (Marco Civil da Internet), e refleti-las nos controles adotados.

Revision #6
Created 2025-11-14 16:47:47 UTC by Arthur
Updated 2026-01-23 14:02:13 UTC by Loyd Hiroki Kozawa