Elementos Fundamentais

- Elementos Fundamentais
- Quais são as nossas recomendações?
- Quais são as sugestões?

Elementos Fundamentais

A boa gestão das aquisições é um componente essencial também em termos de Segurança da Informação, pois permite benefícios como:

- **I. mitigação de vulnerabilidades de segurança;**
- **II. redução de complexidade e heterogeneidade em equipamentos e endpoints;**
- **III. maior estabilidade nos componentes de TI;**
- **IV. menores custos de suporte;**
- **V. tempos menores de resposta e resolução.**

O estabelecimento e a implementação de um programa de Segurança da Informação, com a definição de políticas e padrões, assim como o fomento de uma cultura positiva em termos de Segurança da Informação, é crucial para a efetividade das iniciativas.

A geração de consciência positiva nas pessoas envolvidas fortalece um dos três grandes pilares da Segurança da
Informação, possibilitando inclusive uma redução de custos, financeiros e/ou administrativos, na implementação de mecanismos de Segurança da Informação, além de naturalmente mitigar potenciais vulnerabilidades.

A promoção de cultura corporativa de Segurança da Informação é fundamental e contempla iniciativas originárias dos níveis hierárquicos mais altos (top-down), incluindo o suporte da Alta Administração e o seu protagonismo como bons exemplos, e iniciativas com origem nas bases (grassroot), que engloba a conscientização e educação da força de trabalho.

DIRETRIZES BÁSICAS DE SEGURANÇA DA INFORMAÇÃO

A estabilidade e o insight são fatores relevantes para a efetividade da Segurança da Informação. Estabilidade significa que as mudanças ao ambiente são bem pensadas, racionais e sob alguma forma de governança que a controle. Já o insight permite que a organização conheça, compreenda e reaja aos componentes e atividades dentro do ambiente, tais como pessoas, aplicações e sistemas.

A prática de arquitetura empresarial (Enterprise Architecture) como framework estratégico para os processos é interessante, inclusive, em termos de Segurança da Informação, para dar previsibilidade e estabilidade ao ambiente e se tornar subsídio para a definição de padrões e para desenvolvimento consistente e repetível, bem como a elaboração de mapas de caminho.

As pessoas são fatores fundamentais para a efetividade da Segurança da Informação, de forma que se torna necessário ter um ambiente propício à adoção de comportamentos adequados em termos de Segurança da Informação.

A conscientização é a chave para o sucesso da Segurança da Informação. É importante estimular o engajamento das pessoas de forma adequada e com visibilidade das iniciativas. Nesse contexto, é interessante trabalhar com líderes para dar o exemplo e comunicar o que se espera das pessoas, assim como obter colaboração para coletar e disseminar informações.

A Segurança da Informação preconiza que as pessoas precisam ter não só a liberdade e autonomia necessárias para executar o serviço, mas também o conhecimento para tomar decisões mais corretas.

A Segurança da Informação prescreve que há a necessidade das pessoas terem a liberdade de falhar, ao mesmo tempo em que elas devem reconhecer, se apropriar e responder rapidamente a essas falhas. Uma cultura que ajude [OT 013] as pessoas que contribuam ao programa de Segurança da Informação permite detecção mais rápida de problemas e fornece oportunidades para evitar que eventuais problemas aumentem de tamanho/complexidade.

A gestão apropriada da mudança é primordial para se manter a estabilidade, especialmente em um contexto de mudanças extremamente rápidas, como é o caso da tecnologia da informação e comunicação, objetivando, entre outras coisas, evidenciar a aprovação e a rastreabilidade da mudança.

No âmbito desta Orientação Técnica, define-se mudança como uma alteração de processo/procedimento e/ou de arquitetura de software.

A gestão da mudança contempla naturalmente as questões de segurança.

A gestão apropriada de riscos é imprescindível para a Segurança da Informação, pois baliza a tomada de decisões, inclusive em termos de apetite de risco.

A gestão de riscos envolve iniciativas como análise de contexto, avaliação, tratamento e monitoramento dos riscos,
comunicação e revisão dos mecanismos implantados.

Em um primeiro nível, a gestão de riscos especifica a necessidade de adoção de controles, com a subsequente definição
de níveis aceitáveis e de processos de controle.

Para fins desta Orientação Técnica, a gestão de riscos engloba também a gestão de incidentes, que compreende
processos como:

- **a. plano para determinar quais sensores dos controles estão sendo usados para detectar incidentes, quando e como;**
- **b. processo gerencial de resposta para deter, recuperar e mitigar um incidente;**
- **c. processo de revisão para, no mínimo, evitar que o problema ocorra novamente ou, pelo menos, melhorar a resposta e mitigação em caso de nova ocorrência.**

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.

Quais são as sugestões?

- Se a gestão da mudança não incluír inicialmente as questões de segurança, começar com abordagens pontuais, simples e fáceis de serem adotadas.
- Estabelecer pontes com outras atividades e unidades da organização, tais como: recursos humanos, administrativo/financeiro e as unidades responsáveis pelos processos de negócio do Órgão Setorial. Construir relacionamentos com outras unidades facilita angariar suporte a desenvolvimentos futuros de boa gestão integrada de riscos, bem como o fomento mais rápido das práticas fundamentais em termos de Segurança da Informação.
- Planejar e executar um programa de conscientização de Segurança da Informação, de maneira a estimular comportamentos aceitáveis dos usuários em termos de Segurança da Informação.
- Definir questões relativas à autoridade e ownership de riscos e informações para que a Alta Administração do Órgão Setorial realize a sua implantação.

> Os dados em dispositivos de armazenamento removível (disco rígido externo, pendrive, etc...) devem ser criptografados para prevenir o acesso não autorizado em caso de perda ou roubo.