ÓRGÃO CENTRAL DO
SISTEMA MUNICIPAL DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO DE SÃO PAULO – SMTIC

ORIENTAÇÃO TÉCNICA - 013
TECNOLOGIA DA INFORMAÇÃO DA COMUNICAÇÃO

Das Diretrizes Básicas de Segurança da Informação

2018

SUMÁRIO

INTRODUÇÃO

O presente documento estabelece diretrizes técnicas, gerais e específicas, para os Órgãos Setoriais da Prefeitura do Município de São Paulo (PMSP) no tocante a critérios gerais de gestão de aplicações.

Essa Orientação Técnica (OT-013/CMTIC) faz parte do conjunto de Orientações Técnicas (OT) que foram estabelecidas como instrumento de Governança de Tecnologia da Informação e Comunicação – TIC no Decreto Municipal 57.653, de 07 de abril de 2017, que define a Política Municipal de Tecnologia da Informação e Comunicação.

Esta Orientação Técnica contém diversas recomendações e sugestões.

Uma **recomendação** é uma diretriz definida pelo Conselho Municipal de Tecnologia da Informação e Comunicação – CMTIC, e estabelece regras, procedimentos ou critérios a serem seguidos por padrão. Desta forma, a sua não adoção deverá ser justificada tecnicamente.

Uma **sugestão** é uma boa prática validada pelo CMTIC e possui um caráter não vinculante, mostrando alternativas ou conhecimentos que poderão ser úteis na busca de soluções.

Sendo a Tecnologia da Informação e Comunicação temática dinâmica e de soluções em constante evolução e transformação, essa Orientação Técnica poderá ser objeto de revisões posteriores, visando a estar atualizada de acordo com os conhecimentos mais atuais e alinhada ao contexto da Prefeitura do Município de São Paulo.

Em caso de dúvidas, o Portal de Governança de TI (http://tecnologia.prefeitura.sp.gov.br/) é o local principal em que elas poderão ser expostas, discutidas e solucionadas, de forma a fomentar o aumento e melhoria de conhecimentos e procedimentos, bem como a sua disseminação.

Além do Portal, o Órgão Central do Sistema Municipal de Tecnologia da Informação e Comunicação está à disposição para dirimir eventuais dúvidas advindas desta Orientação.

Órgão Central - Coordenadoria de Gestão de Tecnologia da Informação e Comunicação (CGTIC): cgtic@prefeitura.sp.gov.br

OBJETIVO

O objetivo desta iniciativa é padronizar procedimentos e processos básicos de tomada de decisão, bem como disseminar conhecimentos e estimular boas práticas para que os Órgãos Setoriais possam conduzir suas iniciativas de forma embasada e de acordo com o seu grau de maturidade.

Fazem parte do escopo desse documento as diretrizes básicas a respeito da segurança da informação.

Diretrizes mais específicas poderão ser dispostas em outras Orientações Técnicas, sem prejuízo da revisão desta Orientação.

Não fazem parte do escopo desta OT questões como segurança patrimonial, disponibilização de termos de referência e definição de ferramentas padrão de segurança da informação.

CONSIDERAÇÕES INICIAIS

0.1. A Segurança da Informação deve permear todos os campos de conhecimento em termos de Tecnologia da Informação e Comunicação, sendo calcada em três grandes pilares, quais sejam: **pessoas**, **políticas/procedimentos** e **mecanismos** tecnológicos.

0.2. Além disso, ela compreende diversas dimensões que influenciam, em todo ou em parte, as diversas iniciativas em Tecnologia da Informação e Comunicação. Para fins desta Orientação Técnica, são adotadas as seguintes dimensões, sem prejuízo de outras possibilidades a serem estabelecidas por cada Órgão Setorial para consecução de seus processos de negócio:

I. **Confidencialidade**: propriedade de não estar disponível ou não ser revelado para indivíduos, entidades ou processos não autorizados;

II. **Integridade**: propriedade de completude e fidedignidade;

III. **Disponibilidade**: propriedade de estar acessível e usável para atender tempestivamente à demanda de uma pessoa, processo, ou entidade autorizada;

IV. **Autenticidade**: propriedade de que uma pessoa, organização, entidade, documento ou informação é de fato o que ela diz ser;

V. **Irretratabilidade**: também conhecida como não-repúdio, é a capacidade de provar a ocorrência de determinado evento ou ação, bem como provar a sua autoria ou responsabilidade;

VI. **Rastreabilidade**: capacidade de detectar a ocorrência de determinado evento ou ação, prover caracterização adequada do fato e determinar a sua autoria;

VII. **Confiabilidade**: propriedade de obter comportamentos e resultados de forma prevista e consistente;

VIII. **Utilidade**: propriedade de agregar ou gerar valor em termos organizacionais; e

IX. **Consciência**: ato e estado de conhecimento, internalização e adoção de determinada informação como tendo valor relevante em termos pessoais e/ou organizacionais.

0.3. Em termos de gestão, a Segurança da Informação é baseada em **Elementos Fundamentais** e dividida em diversas **Áreas de Gestão**.

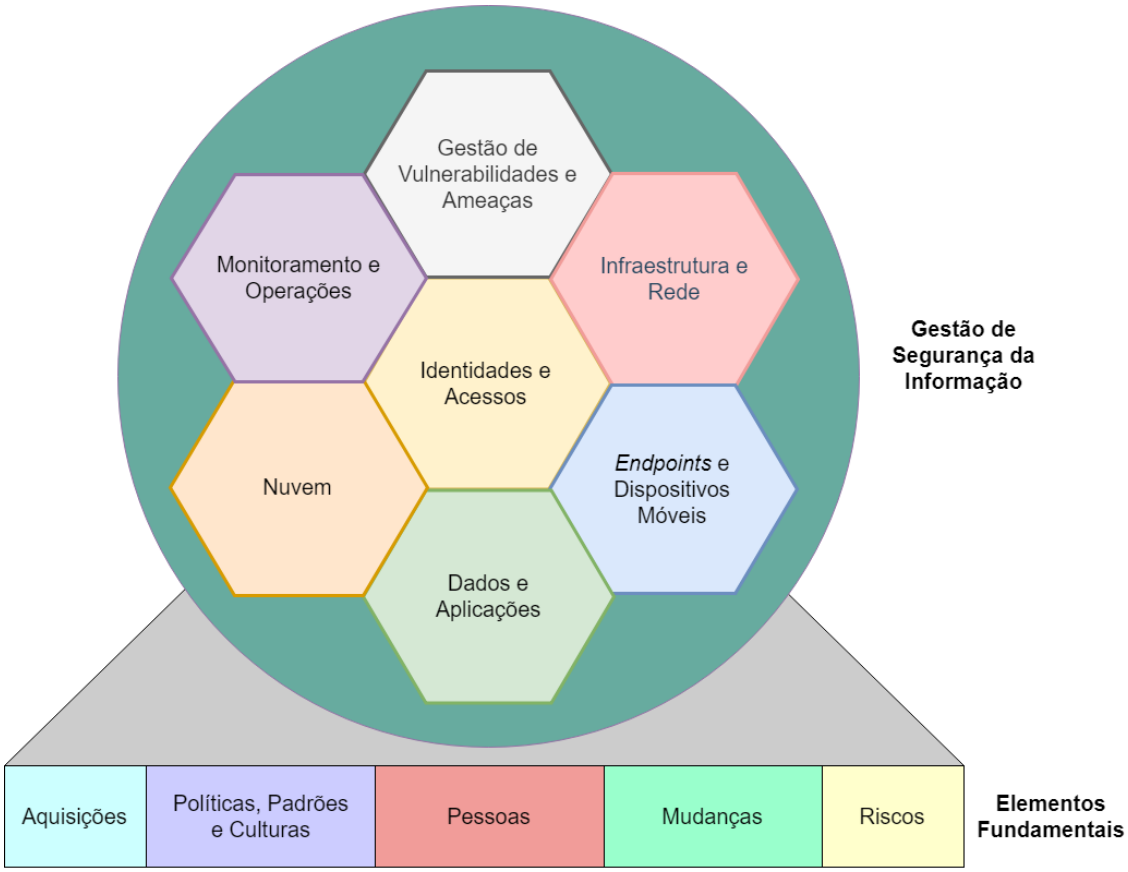

Figura 1: Elementos Fundamentais e Áreas de Gestão de Segurança da Informação. (adaptado do Gartner)

0.4. Os **Elementos Fundamentais** são:

I. Aquisições
II. Políticas, Padrões e Culturas
III. Pessoas
IV. Mudanças
V. Riscos

0.5. As **Áreas de Gestão** são:

I. Gestão de Vulnerabilidades e Ameaças
II. Monitoramento e Operações
III. Infraestrutura e Rede
IV. Identidades e Acessos
V. Nuvem
VI. *Endpoints* e Dispositivos Móveis
VII. Dados e Aplicações

1 Elementos Fundamentais de Segurança da Informação

1.1. 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.

1.2. 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.

I. 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.

II. 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.

III. 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.

IV. 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.

1.3. 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.

I. 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.

II. 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.

III. 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 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.

1.4. 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 rastrebailidade da mudança.

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

II. A gestão da mudança contempla naturalmente as questões de segurança.

1.5. 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.

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

II. 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.

III. 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.

Recomendações:

- 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.
- 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 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.

Sugestões:

- Se a gestão da mudança não incluía 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.

2 Áreas de Gestão de Segurança da Informação

2.1. A **Gestão de Vulnerabilidades e Ameaças** é uma prática básica em termos de Segurança da Informação, visto que uma das atuações mais intuitivas na área seria exatamente a identificação de ameaças, a eliminação de vulnerabilidades e o uso de controles para mitigar ameaças residuais.

I. A priorização de iniciativas de mitigação ou remediação é parte da gestão.

II. A busca por ameaças mais específicas e avançadas é algo a ser considerado por Órgãos Setoriais com maior nível de Maturidade.

2.2. A área de **Monitoramento e Operações** envolve a parte operacional da implementação de controles e detecção/eliminação/mitigação de ameaças.

I. A avaliação da qualidade das operações é uma atividade relevante, uma vez que não há uma ferramenta única capaz de mitigar todas as possibilidades e certamente nenhuma ferramenta é capaz de eliminar todas as ameaças.

II. O processo de monitoramento poderá começar como sendo pontual, para então passar para ocasional/periódico e chegar enfim ao estado desejado, que é o monitoramento contínuo.

2.3. A **Infraestrutura e Rede** contêm frequentemente os ativos mais valiosos em termos de tecnologia da informação e comunicação e, portanto, necessitam de proteção adequada, especialmente se o Órgão Setorial possuir um *data center* ou similar.

I. A segurança da rede envolve a proteção de ambientes virtualizados como IaaS e outras formas de acesso remoto.

2.4. O controle de **Identidades e Acessos** é, muitas vezes, um dos objetivos mais claros e imediatos de Segurança da Informação e permeia todas as demais áreas, direta ou indiretamente.

2.5. A **Nuvem** precisa ser tratada de forma diferenciada em termos de Segurança da Informação, uma vez que existem diversas formas de contratação e uso, impactando na implementação e operação dos controles de segurança.

I. A contratação e/ou uso da nuvem traz consigo questões não técnicas, especialmente questões de caráter legal/regulatório, que precisam ser levadas em consideração.

2.6. Os ***Endpoints* e Dispositivos Móveis** são um elemento de extrema relevância em qualquer arquitetura ou infraestrutura de tecnologia da informação e comunicação.

I. A questão do BYOD (*Bring Your Own Device*) é um desafio a ser tratado, considerando-se por um lado a sua conveniência e baixo custo, e por outro lado os riscos de se ter dados do Órgão Setorial em equipamentos e ambientes fora do seu controle direto.

2.7. A segurança das **Aplicações** trata tanto da segurança em termos de desenvolvimento quanto de execução, incluindo a proteção dos Dados que utilizam. Os **Dados** propriamente ditos são geralmente os ativos mais valiosos a serem protegidos e medidas devem ser tomadas para sua proteção, para fins de inserção/atualização/exibição/eliminação, processamento, armazenamento e transmissão/transferência.

Recomendações:

- Observar as Orientações Técnicas e correlatas e normativos em vigor afeitos para entender e atender, dentro do que for pertinente, as respectivas Recomendações e Sugestões.

3 Políticas Básicas de Segurança da Informação

Esta Orientação Técnica estabelece uma política básica de Segurança da Informação em três níveis: o Nível 0 é voltado aos Órgãos Setoriais que não possuem nenhuma política de Segurança da Informação, o Nível 1 se dirige aos que já implantaram o Nível 0 e, por fim, o Nível 2 é voltado aos Órgãos Setoriais que já alcançaram o Nível 1.

Deve-se ressaltar que a política descrita nesta Orientação se limita apenas ao que se entende ser o mínimo indispensável, estando muito longe ainda do ideal. É fundamental que cada Órgão sempre busque enriquecer, expandir e aprimorar a Segurança da Informação dentro da sua organização, para além do disposto nesta Orientação Técnica.

Nível 0:

O Nível 0 é voltado aos Órgãos Setoriais que não possuem maturidade suficiente para desenvolver atividades mais específicas de Segurança da Informação,

seja por falta de conhecimento, seja por falta de equipe, ou ainda por ser um Órgão Setorial recém-criado e, portanto, ainda em processo de estruturação.

Nesse caso, é importante que o responsável pela Tecnologia da Informação e Comunicação tenha pelo menos algumas informações rudimentares em mãos. Naturalmente, isso está longe de ser suficiente, necessitando que haja esforços para aumentar a maturidade do Órgão Setorial em termos de Tecnologia da Informação, de forma a avançar nos níveis da Segurança da Informação.

O Nível 0 exige as seguintes medidas:

Área de Gestão	Medidas a serem implementadas
Gestão de Vulnerabilidades e Ameaças	-o-
Monitoramento e Operações	-o-
Infraestrutura e Rede	1. Limitar o uso de contas de administrador ou similares, bem como privilégios administrativos de acesso/execução, de forma que apenas as pessoas que realmente precisem tenham acesso a essas contas e/ou privilégios. 2. Alterar todas as senhas padrão de infraestrutura e de rede para uma senha mais segura, gerido pelo responsável pela tecnologia da informação e comunicação do Órgão Setorial.
Identidades e Acessos	3. Implantar e manter processos de gestão de identidades e acessos, incluindo a parte de provisionamento, alteração e exclusão. 4. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que são aplicados critérios de senha, para se ter senhas adequadamente fortes. 5. Restringir as contas privilegiadas de usuário, tais como as contas de administrador, *root* e equivalentes, para que apenas os usuários que necessitam tais contas por necessidade de serviço, ou usuários que sejam servidores de carreira ou especialização em tecnologia da informação, possam ter permissão de uso de tais contas. 6. Definir processos de concessão e revogação de acesso, podendo incluir a necessidade de assinatura de um termo de responsabilidade.
Nuvem	7. Considerar, como padrão, que os dados na nuvem devem estar armazenados em território brasileiro.
Endpoints e Dispositivos Móveis	8. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que está acontecendo a aplicação de *patches* do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas. 9. Verificar, junto ao Integrador Estratégico e/ou ao prestador de

	serviços de infraestrutura, que há a proteção de *endpoints*, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos um antivírus. 10. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que foram implantados para rede *wireless*, configurando no mínimo o protocolo WPA2. 11. Alterar todas as senhas padrão das contas de administrador ou equivalentes para uma senha mais segura, gerida pela equipe de tecnologia da informação e comunicação do Órgão Setorial. 12. Implantar um sistema de gestão de ativos para gerir os *endpoints*.
Dados e Aplicações	13. Localizar onde estão os dados mais críticos armazenados pelo Órgão Setorial e, se estiverem armazenados em equipamentos pessoais, ter pelo menos uma cópia atualizada periodicamente em um repositório corporativo do Órgão. 14. Implantar infraestrutura e rotinas básicas de *backup* de dados, considerando a Orientação Técnica sobre o tema. 15. Verificar, junto ao Integrador Estratégico e/ou ao prestador de serviços de infraestrutura, que há controles de acesso às bases de dados do Órgão Setorial, de forma que o acesso seja estritamente em função das necessidades de serviço.

Nível 1:

O Nível 1 se destina aos Órgãos Setoriais que já iniciaram um processo de desenvolvimento e amadurecimento da sua equipe de Tecnologia de Informação e Comunicação. O objetivo é começar a munir a equipe com conhecimentos e ferramentas para atuarem de forma mais presente.

Além do Nível 0, o Nível 1 exige também as seguintes medidas:

Área de Gestão	Medidas a serem implementadas
Gestão de Vulnerabilidades e Ameaças	-o-
Monitoramento e Operações	-o-
Infraestrutura e Rede	16. Implantar medidas de segurança física para proteger no mínimo a infraestrutura principal de tecnologia da informação e comunicação do Órgão Setorial, incluindo[1]: a. Porta com chave/cadeado que esteja efetivamente

[1] Por "infraestrutura principal" entende-se o ambiente que se designa informalmente como a "sala de servidores", contendo os servidores e/ou os ativos de rede principais. Excluem-se os *data centers* (salas-cofre e infraestrutura associada), pois as exigências nesse caso são diferenciadas e muito mais rigorosas.

	operacional. b. Claviculário ou equivalente para guardar as chaves, incluindo as chaves dos *racks.* c. Limitação do acesso físico à infraestrutura principal apenas às pessoas que efetivamente trabalham com os ativos localizados na mesma.
Identidades e Acessos	17. Definir papéis para padronizar os conjuntos de permissões de acesso, ao invés de definir acessos para cada usuário, documentando os papéis definidos e mantendo a documentação no repositório de dados corporativo do Órgão Setorial. 18. Aplicar critérios de senha, para se ter senhas adequadamente fortes.
Nuvem	-o-
Endpoints e Dispositivos Móveis	19. Gerir a aplicação de *patches* do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas. a. Avaliar também a possibilidade de utilizar o servidor WSUS do Integrador Estratégico ou até mesmo ter um servidor WSUS interno ao Órgão Setorial, de forma a evitar congestionamento de rede. 20. Implantar a proteção de *endpoints*, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos: a. Anti-*malware*, incluindo antivírus; b. *Firewall*; c. Filtro para navegação Web, que pode ser implantado tanto por meio de uma solução centralizada quanto por meio de *add-ons* de navegadores; d. Detector de comportamento suspeito/anômalo. 21. Implantar e manter mecanismos de segurança para rede *wireless*, configurando no mínimo o protocolo WPA2.
Dados e Aplicações	22. Implantar controles de acesso às bases de dados do Órgão Setorial, de forma que o acesso seja estritamente em função das necessidades de serviço. 23. Se o Órgão realizar o desenvolvimento de aplicações, incluir como requisito não funcional a exigência de não inserir segredos (senhas, *tokens* etc.) no código-fonte, exceto para fins meramente de testes. 24. Se o Órgão realizar o desenvolvimento de aplicações, implantar controle de versão e gestão de repositório de código. 25. Se o Órgão realizar o desenvolvimento de aplicações, incluir no desenvolvimento a geração de logs de auditoria.

Nível 2:

O Nível 2 deve incorporar, ainda que em parte, da abordagem baseada em riscos. Para que isso possa ser realizado, o Órgão Setorial deverá ter pelo menos uma pessoa da equipe de tecnologia de informação e comunicação que tenha recebido

capacitação formal em análise e gestão de riscos, preferencialmente o líder da equipe de tecnologia de informação e comunicação.

Além do Nível 1, o Nível 2 exige também as seguintes medidas:

Área de Gestão	Medidas a serem implementadas
Gestão de Vulnerabilidades e Ameaças	26. Utilizar ferramentas automatizadas para conduzir, de forma periódica, avaliação básica de vulnerabilidade em sistemas de alto valor que o Órgão disponibiliza na internet.
Monitoramento e Operações	27. Definir e documentar processos básicos de continuidade de negócios e recuperação de desastres para pelo menos um evento negativo de impacto crítico.
Infraestrutura e Rede	28. Implantar mecanismos de detecção de ativos não identificados e/ou não autorizados na rede interna. 29. Implantar e manter um ou mais *firewalls* para controlar o tráfego de rede, especialmente se o Órgão Setorial tiver um *link* direto para a internet. 30. Implantar e manter uma ou mais VPNs (rede privada virtual), especialmente se o Órgão Setorial utilizar acesso remoto, incluindo a conexão a algum ambiente IaaS. 31. Implantar e manter um sistema de detecção e/ou prevenção a intrusões de rede, preferencialmente como parte de um *firewall* ou de um produto de gestão unificada de ameaças (UTM). 32. Planejar, implantar e documentar a segmentação/zoneamento de rede.
Identidades e Acessos	-o-
Nuvem	33. Investir em capacitação para ganhar conhecimento na avaliação do melhor modelo de contratação/implantação, além de conhecimentos para realizar a contratação em si. 34. Considerar, como padrão, que os dados na nuvem devem estar armazenados em território brasileiro. a. No caso do Órgão Setorial ter um líder de TI com capacitação formal em Gestão de Riscos e/ou uma unidade formalmente constituída de Segurança da Informação, o Órgão poderá armazenar seus dados na nuvem fora do território nacional, mediante análise de risco e justificativa.
Endpoints e Dispositivos Móveis	35. Implantar um sistema e/ou um processo de gestão de licenças de software, incluindo um processo contínuo de adequação e atualização planejada das licenças. 36. Realizar um processo de *hardening* (melhoria de robustez dos *endpoints*) de acordo com boas práticas conhecidas, tais como: a. Utilizar guias, *checklists* ou *benchmarks* amplamente utilizadas pelo mercado para ter um ponto de partida

	de realização de *hardening*[2]; b. Utilizar imagens atualizadas para instalar nos *endpoints*, se possível já após um processo de *hardening* da imagem; c. Limitar os privilégios das contas de administrador ou root local e/ou as pessoas com acesso a essas contas.
Dados e Aplicações	37. Se o Órgão realizar o desenvolvimento de aplicações, mapear as dependências da segurança da aplicação em termos de infraestrutura. 38. Se o Órgão realizar o desenvolvimento de aplicações, incorporar um mecanismo ou processo de teste de segurança de aplicações dentro da etapa de testes do ciclo de desenvolvimento de aplicações. 39. Se o Órgão disponibiliza aplicações para a internet que são hospedadas dentro da sua própria infraestrutura, implantar uma WAF (*Web Application Firewall*).

Para o caso específico do Nível 2, o líder da unidade formalmente constituída para gerir a tecnologia de informação e comunicação do Órgão Setorial poderá estabelecer um plano de adoção gradual das medidas descritas, considerando-se questões de caráter técnico, de pessoal e orçamentário/financeiro.

Em caso de ter alguma prática ou controle listados acima que exijam tecnologia e/ou processo que o Órgão Setorial ainda não detém, o líder poderá realizar e executar um planejamento, refletido no Plano Diretor Setorial de Tecnologia da Informação e Comunicação e limitado à disponibilidade orçamentária, para adquirir e/ou desenvolver tal tecnologia, bem como desenvolver e internalizar os processos necessários.

Em termos de Escala de Maturidade, a aplicação comprovada da política em Nível 1 habilita o Órgão Setorial a pleitear a medalha de bronze em Política de Segurança da Informação.

Recomendações:

[2] Alguns exemplos possíveis:
https://nvd.nist.gov/ncp/repository
https://iase.disa.mil/stigs/Pages/a-z.aspx
https://github.com/nsacyber/Windows-Secure-Host-Baseline
http://www.buffalo.edu/content/dam/www/ubit/docs/guidance-documents/appendix-a-server-security-checklist.pdf

- Para um Órgão Setorial sem nenhuma política de Segurança da Informação publicada ou publicizada, implantar a política em Nível 0 desta Orientação, seguindo-se o checklist disponível no Anexo.
- Para um Órgão Setorial que já implantou a política em Nível 0, buscar a implantação do Nível 1.
- Para um Órgão Setorial que já implantou a política em Nível 1, buscar a implantação planejada e gradual do Nível 2, considerando-se as capacidades e necessidades técnicas, de pessoal e de orçamento.
- Se o Órgão já alcançou o Nível 2, buscar aprimorar e expandir os seus controles de segurança para melhor gestão da Segurança da Informação.

Sugestões:

- Automatizar os procedimentos de dimensionamento e alocação de infraestrutura.
- Incorporar os requisitos de segurança dentro do processo de desenvolvimento ou do termo de referência de aquisição da aplicação.

4 Quando as recomendações passam a valer?

Os procedimentos descritos nesta Orientação Técnica (OT-013/CMTIC) deverão ser aplicados nos procedimentos atuais e futuros, bem como nos contratos futuros e nas prorrogações contratuais, ainda que de contratos assinados antes do início da vigência desta OT.

Esta Orientação Técnica entrará em vigor a partir da sua aprovação pelo CMTIC.

REFERÊNCIAS

Wonham, Mike. *Building the Foundations for Effective Security Hygiene.* Gartner, 2018. Publicado em 08 de agosto de 2018.

Anexo - Checklist Nível 0

Item	Ok?
As contas padrão de usuário **não** são contas de administrador, nem de administrador local ou equivalente.	
As contas de administrador dos servidores ou dos computadores que atuam como tal são geridas apenas pela equipe de Tecnologia de Informação e Comunicação do Órgão Setorial.	
Restringir as contas privilegiadas de usuário, tais como as contas de administrador, root e equivalentes, para que apenas os usuários que necessitam tais contas por necessidade de serviço, ou usuários que sejam servidores de carreira ou especialização em tecnologia da informação, possam ter permissão de uso de tais contas.	
As contas de acesso para os ativos de infraestrutura e de rede são geridas apenas pela equipe de Tecnologia de Informação e Comunicação do Órgão Setorial, pelo Integrador Estratégico ou pelo prestador de serviços de infraestrutura.	
Todas as senhas padrão dos ativos de infraestrutura e de rede que estiverem sob a gestão da equipe de Tecnologia de Informação e Comunicação do Órgão Setorial estão alteradas para uma senha não padrão, preferencialmente com o uso de caracteres e números no mínimo.	
Todas as senhas padrão dos ativos de infraestrutura e de rede que estiverem sob a gestão da equipe de Tecnologia de Informação e Comunicação do Órgão Setorial são alteradas periodicamente, pelo menos a cada três anos ou sempre que for necessário, para uma outra senha não padrão, preferencialmente com o uso de caracteres e números não utilizados na senha anterior.	
Existe um aceite formal dos servidores, admitido o uso de meio eletrônico/digital, explicitando o conhecimento e a concordância com as Políticas de Segurança implantadas no Órgão Setorial.	
É executada uma varredura periódica, no mínimo anualmente, para identificar os usuários que não são mais utilizados (ex: usuários dos servidores que já foram exonerados).	
É executado um procedimento periódico, no mínimo anualmente, para bloquear e/ou eliminar os usuários inativos, isto é, os usuários que não são mais exonerados.	
Existe um documento corporativo (ou equivalente) atualizado periodicamente com os sistemas utilizados no Órgão Setorial e os respectivos procedimentos para solicitação de acesso.	
O documento corporativo (ou equivalente) atualizado com os sistemas está armazenado em um repositório corporativo, e não pessoal, do Órgão Setorial.	
Existe um procedimento corporativo para concessão de permissões de acesso a usuários, registrando-se os pedidos de concessão, preferencialmente por meio eletrônico.	
Existe um procedimento corporativo que define formalmente quem é o autorizador da concessão de permissão de acesso, sendo que o autorizador não pode ser o próprio usuário, salvo no caso do Secretário, Secretário Adjunto, Subprefeito, Chefe de Gabinete e equivalentes.	
Existe um procedimento corporativo que define formalmente os critérios de exclusão de permissão de acesso, incluindo no mínimo os casos de bloqueio/exclusão do usuário e a remoção em caráter fático do servidor.	
É executada uma varredura e adequação periódicas das permissões concedidas a cada usuário, excluindo-se as permissões que não sejam estritamente necessárias ao cumprimento das atividades atuais do usuário.	

Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que são adotados critérios e procedimentos para se ter senhas adequadamente fortes para os usuários e ativos do Órgão Setorial que são geridos pelas entidades supra.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que são adotados políticas de aplicação de *patches* do sistema operacional e de outras aplicações, para eliminar vulnerabilidades conhecidas.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para a proteção dos *endpoints* do Órgão Setorial geridos pelos mesmos, seja por meio de uma solução integrada ou por meio de um conjunto de soluções, incluindo pelo menos um antivírus.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para a proteção da rede wireless do Órgão Setorial gerida pelos mesmos, configurando no mínimo o protocolo WPA2 para segurança.	
Existe um sistema de gestão de ativos implantado, operacional e em utilização no Órgão Setorial para gerir os ativos de microinformática (essencialmente desktops, notebooks e similares).	
Existe um procedimento corporativo, de preferência formal, que permite à equipe de Tecnologia de Informação e Comunicação do Órgão Setorial localizar e copiar para o repositório corporativo, de ofício, os dados corporativos armazenados em equipamentos pessoais, especialmente para o caso de remoção, aposentadoria e/ou exoneração iminente do servidor.	
Existe um procedimento corporativo implantado, junto com a infraestrutura necessária, para a execução de rotinas *básicas* de backup de dados, considerando a Orientação Técnica sobre o tema.	
Existe um documento formal do Integrador Estratégico e/ou do prestador de serviços de infraestrutura, admitido o uso de documento eletrônico/digital, explicitando que existem medidas para limitar o acesso direto à base de dados do Órgão Setorial, de forma que o acesso seja realizado estritamente em função das necessidades de serviço.	