Prefeitura Municipal de Maricá

Instituto de Ciência, Tecnologia e Inovação de Maricá

Anexo IV - Norma para Padrões de Segurança da Informação

Maricá, abril de 2025

Presidente

Cláudio de Souza Gimenez

Diretor de Infraestrutura

Laércio Aguiar da Rocha

Equipe Técnica

Emerson Lacerda Alencar

Giovanni Di Carlo

Márcio Santarém Nogueira

Histórico de Revisões

Versão	Data	Histórico	Autor	Revisor
1.0	abril de 2025	Versão inicial	Emerson L. Alencar Márcio S. Nogueira	Laércio A. Rocha

Sumário

1. PREMISSAS

1.1. É fundamental que todos os servidores públicos, diretorias, fornecedores, prestadores de serviços e demais parceiros vinculados compreendam o seu papel crucial no contexto da Segurança da Informação (SI). É um dever seguir rigorosamente as diretrizes e orientações estabelecidas na Política de Segurança da Informação (PSI) do ICTIM, a fim de evitar exposição indevida das informações e dos recursos de processamento a situações adversas, tais como comprometimento, alteração, furto e desvio.

1.2. Fica estabelecido que a Assessoria de TI da Diretoria de Infraestrutura, fornecedora de TI responsável por administrar a rede do ICTIM, será doravante denominada Responsável. Todos os demais fornecedores e prestadores de serviços serão denominados Terceiros.

2. CONCEITOS

2.1. Este documento reúne diretrizes de forma a estabelecer claramente o que Responsável e Terceiros precisam contemplar em seus serviços, para estarem em conformidade com as melhores práticas de Segurança da Informação.

2.2. Frente à crescente evolução tecnológica, caracterizada pela rapidez e diversidade dos recursos para acesso à informação, os fornecedores e prestadores de serviços de TIC devem possuir a habilidade de antecipar possíveis cenários e estar constantemente preparados para eventualidades. Isso implica adotar uma postura preventiva e preemptiva, que não se baseia mais na possibilidade de algo acontecer, mas sim na certeza de que acontecerá e na preparação para quando e como isso ocorrerá.

2.3. Um aspecto crucial, diante desse ritmo acelerado de evolução, é que a defasagem tecnológica resultante pode expor a infraestrutura e a segurança de TIC a vulnerabilidades, acarretando em inúmeras consequências, tais como ineficiência operacional, descontentamento tanto de colaboradores quanto de clientes, além de retardar e tornar ineficaz o processo decisório.

2.4. Os equipamentos podem apresentar falhas devido a defeitos de fabricação, instalação inadequada ou uso incorreto, bem como devido a quebras ou danos nos componentes, resultantes de uma conservação inadequada. Da mesma forma, os sistemas podem enfrentar falhas técnicas, vulnerabilidades de segurança e problemas causados pelo mau uso ou pela negligência na gestão das credenciais de acesso.

2.5. A falta de controles e processos adequados para identificar esses casos pode comprometer um ou mais dos princípios da Segurança da Informação em diferentes níveis de gravidade.

3. DIRETRIZES

IMAGEM OFICIAL PARA INSTALAÇÃO DE COMPUTADORES

3.1. Para garantir o acesso aos recursos do domínio do ICTIM, os equipamentos devem ser instalados usando imagens oficiais mantidas e gerenciadas pelo RESPONSÁVEL, que ficará encarregado de configurar todos os acessos, privilégios e garantir a conformidade. Dessa forma, será estabelecido um padrão homogêneo e garantida a entrada correta dos equipamentos na rede do ICTIM.

3.2. As imagens conterão no mínimo o seguinte conjunto de softwares:

a. Sistema operacional de uso difundido;

b. Navegador para uso da internet e acesso ao correio eletrônico institucional;

c. Sistema de detecção e mitigação de malwares (antivírus);

d. Pacote base de aplicativos de escritório (editor de textos, planilha eletrônica etc.);

e. Programa leitor de Portable Document Format (PDF), quando não incluso no próprio sistema operacional;

f. VMware Horizon Client para uso dos sistemas corporativos;

ACESSO A REDE E INTERNET

Compete ao Responsável seguir e/ou implementar as seguintes diretrizes:

3.3. Todos os usuários que possuem acesso à rede e aos sistemas devem ser designados com uma identificação de login única, a qual estará associada à Diretoria onde estão realizando suas atividades. Essa identificação incluirá as permissões pertinentes e solicitadas pelo(a) Diretor(a) da área;

3.4. Devem existir procedimentos formais que contemplem todas as atividades ligadas à administração de acessos, desde a criação de um usuário novo, passando pela administração de privilégios e senhas, alteração de setor e desativação de usuários;

3.5. O acesso aos serviços computacionais deve ser sempre realizado por meio de um procedimento seguro, utilizando comunicações criptografadas, onde o usuário se conecta a um sistema ou rede específicos. Este processo deve ser cuidadosamente planejado para reduzir ao máximo as chances de acessos não autorizados. As senhas podem ser alteradas pelo usuário conforme as diretrizes estabelecidas na Norma para Utilização de Credenciais e Senhas.

3.6. Contas inativas (sem login nas estações de trabalho ou webmail) há mais de 2 (dois) meses, deverão ser bloqueadas e a chefia imediata do usuário notificada, preservando o conteúdo já existente na caixa de e-mail do usuário. Elas poderão ser reativadas mediante solicitação;

3.7. Contas inativas há mais de 3 (três) meses serão consideradas elegíveis à remoção, com perda de todo conteúdo associado àquela conta, incluindo mensagens existentes na sua caixa de e-mail. Este procedimento só poderá ser realizado mediante envio de comunicação à chefia imediata, que deverá autorizar ou solicitar a manutenção da conta mediante justificativa e/ou amparo legal que fundamente esta solicitação;

3.8. O uso de redes externas de comunicação (Internet, redes privadas etc.) obrigatoriamente deve ser realizado empregando tecnologias de ponta, com as devidas segregações e segmentações de redes, obrigatoriamente empregando servidores de firewalls, servidores de acesso à internet e ferramentas contra malwares e lixo eletrônico (Spam);

3.9. Deve ser formalizado aos usuários, em seu primeiro acesso, que o ICTIM mantém rastreamento de acesso à internet a fim de permitir o monitoramento do correto uso da tecnologia (nome do usuário e endereço acessado são informações obrigatórias no rastreamento);

3.10. O usuário que efetuar qualquer acesso a sites com material indevido deverá ter sua conta bloqueada;

3.11. Todo usuário desligado do ICTIM deve ter sua conta imediatamente inativada, mediante comunicação dos Recursos Humanos;

3.12. Todo servidor deverá assinar o Termo de Responsabilidade relativo ao uso do computador institucional.

SERVIÇOS DE E-MAIL

Compete ao Responsável seguir e/ou implementar as seguintes diretrizes:

3.13. Formalizar aos usuários, em seu primeiro acesso, que todas as informações veiculadas em e-mail institucional pertencem ao ICTIM, podendo este monitorar, auditar e ter acesso de uso a qualquer tempo;

3.14. As contas de e-mail deverão estar relacionadas com o AD do domínio de forma a automatizar tarefas de inclusão, desativação e exclusão de contas, bem como uma melhor gestão por parte dos administradores;

3.15. Cada usuário deve ter uma única conta de e-mail vinculada a seu login de domínio. Eventuais necessidades acima deste limite devem ser realizadas pela disponibilização de um grupo de e-mail, ou alternativa equivalente para esta finalidade, evitando que um usuário tenha múltiplas contas, assim reduzindo diversos problemas de gerenciamento de e-mails.

3.16. Todo o tráfego de dados que passa pelos servidores de e-mail deve obrigatoriamente ser verificado de forma automática por solução end point completa (antivírus, antispam, filtragem web e mail, alertas, firewall, etc), capaz de identificar e filtrar Spam e combater:

a. Vírus

b. Bots

c. Adwares

d. Trojan Horses

e. Worms

f. Ramsonwares

g. Híbridos e variantes

3.17. A ferramenta de e-mail deve oferecer o informativo de orientação de uso da informação, de acordo com as recomendações de melhores práticas de mercado. Exemplo: “Este e-mail pertence ao ICTIM e as informações contidas não devem ser divulgadas fora do escopo desta tratativa”.

CONTROLE DE HARDWARE E SOFTWARE

Compete ao Responsável cumprir as seguintes diretrizes:

3.18. Oferecer uma ferramenta para inventário de hardware, que inclua um agente de monitoramento capaz de automatizar essa tarefa pela rede. Este agente será responsável por identificar e relatar o conjunto de softwares instalados em cada equipamento, possibilitando o

dimensionamento e monitoramento do parque computacional. Isso visa facilitar uma gestão eficiente da infraestrutura.

3.19. Fornecer um catálogo de sistemas claro e funcional, abrangendo todos os sistemas em uso, os descontinuados e aqueles planejados para implantação futura. Este catálogo será de fácil consulta, destacando as funcionalidades e o propósito de cada sistema dentro do ICTIM.

3.20. Utilizando os recursos mencionados anteriormente, será possível monitorar e gerar relatórios de segurança para os gestores responsáveis do ICTIM. Esses relatórios destacarão todos os casos que possam representar potenciais riscos para a segurança da informação.

3.21. É importante notificar a gestão das diretorias afetadas e a área responsável pela Governança de TI do ICTIM sobre a presença de software e/ou hardware descontinuados, que não recebem atualizações dos fabricantes e representam riscos à segurança. Dessa forma, as medidas necessárias podem ser tomadas para mitigar esses riscos.

FUNCIONALIDADES DE BACKUPS

Compete ao Responsável, bem como aos Terceiros que venham a prestar serviços de backup para o ICTIM, as diretrizes a seguir:

3.22. Implementar e manter uma política de backups clara, eficiente e bem documentada, permitindo que os usuários compreendam e sigam as diretrizes estabelecidas na Norma para Procedimentos de Backup.

3.23. Os recursos de armazenamento designados para backup dos usuários, integrantes dos Repositórios Oficiais, devem estar em total conformidade com as diretrizes estabelecidas na Norma para Repositório Oficial de Arquivos.

3.24. É obrigatório contar com redundância nos backups, além de manter uma cópia fisicamente separada em serviços de nuvem, datacenters externos ou em meios similares, devidamente comprovados em eficácia e capazes de garantir uma rápida recuperação dos dados quando necessário.

3.25. O escopo do backup é definido pelo setor de Governança de TI do ICTIM conforme as demandas de cada diretoria.

3.26. Os backups devem ser unidirecionais, ou seja, a infraestrutura de produção não tem capacidade de alterar backups já realizados.

3.27. Os backups poderão ser recuperados de maneira transparente independentemente de ser segmentado de forma full, incremental ou

diferencial, com periodicidade e retenção apropriadas à perda máxima de dados definida para a solução.

FUNCIONALIDADES DE BACKUPS

Compete ao Responsável seguir e/ou implementar as seguintes diretrizes:

3.28. Quando próprios do ICTIM, todos os equipamentos de informática deverão ser inventariados pela Diretoria de Infraestrutura/Informática e previamente registrados pela Coordenação de Patrimônio do ICTIM antes de serem conectados à rede corporativa do Instituto;

3.29. A instalação de equipamentos, adição ou a substituição de peças, periféricos ou outros elementos físicos de informática, que integram o patrimônio do ICTIM, somente poderá ser efetuada pelo Responsável e eventuais Terceiros contratados para tal finalidade.

3.30. Quando locados, a taxonomia de nomenclatura dos equipamentos deve seguir o padrão definido pela empresa prestadora do serviço;

3.31. A manutenção dos equipamentos locados somente poderá ser efetuada pela própria empresa CONTRATADA, na qual é a prestadora do serviço.

3.32. Instalações devem ser realizadas somente através das imagens oficiais mencionadas nesta norma;

3.33. As manutenções em equipamentos que armazenem informações devem ser acompanhadas por um representante do setor sempre que esse equipamento estiver em uso, ou logado com a credencial do servidor que necessita do suporte;

3.34. Manutenções via acesso remoto devem ser feitas por ferramenta e procedimentos seguros aprovados pela equipe de Segurança da Informação do Responsável;

3.35. Todo o conteúdo armazenado em unidades de armazenamento (HDD, SDD, M2, etc.) de qualquer equipamento que seja doado, cedido, devolvido, vendido ou descartado deverá ter todas as suas informações armazenadas apagadas, empregando métodos que realmente tornem as informações irrecuperáveis. CD’s, DVD’s, fitas ou pen drives descartados devem ser fisicamente destruídos;

CRIAÇÃO E USO DE CREDENCIAIS COM PERFIL ADMINISTRATIVO

Compete ao Responsável seguir e/ou implementar as seguintes diretrizes:

3.36. Definir os profissionais de seu quadro funcional que, para o exercício de suas funções, recebem credenciais de administrador;

3.37. Contas regulares de usuário, que por padrão são restritivas, não podem ser promovidas e receber permissões administrativas;

3.38. Quando da necessidade de conceder credencial de administrador a um usuário, uma solicitação da chefia imediata desse deverá ser feita por meio de formalização justificada e autorizada pela equipe de Governança de TI do ICTIM.

3.39. Uma requisição de criação de novo usuário deve obrigatoriamente conter:

a. Identificação do demandante

b. A justificativa da necessidade

c. O período de duração estimado.

d. Demais dados que a Diretoria de Infraestrutura e o Responsável venham a definir.

3.40. A taxonomia para contas de administrador deverá seguir o formato de conta de usuário no AD;

3.41. Para Terceiros que venham a prestar serviços, que justificadamente necessitem perfil de administrador, deverá ser criado um usuário novo com data de expiração correspondente a requisição de usuário.

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

3.42. É de competência do Responsável implementar e publicar um Plano de Resposta a Incidentes de acordo com a Norma para Plano de Resposta a Incidentes, de forma a manter a operação do ICTIM segura contra eventuais situações que a comprometam.