Norma para Padrões de Segurança da Informação

PREFEITURA

Mais **cidade**. Mais **vida**.

Normativa para Padrões de Segurança da Informação da Prefeitura Municipal de Porto Alegre

Secretaria Municipal de Planejamento e Assuntos Estratégicos CGTI-SMPAE

Versão 1.0

Última atualização 9 de Fevereiro de 2023

PREMISSAS

Todos os servidores públicos, secretarias, órgãos, fornecedores, prestadores de serviço e demais parceiros vinculados devem ter conhecimento de seu importante papel no contexto de **Segurança da Informação (SI)** sendo um dever seguirem as diretrizes e orientações contidas na **Política de Segurança da Informação (PSI)** em sua íntegra, assim evitando expor a informação e os recursos de processamento a situações adversas como comprometimento, alteração, furto e desvio.

Fica estabelecido que a **PROCEMPA**, fornecedor de TI responsável por administrar a rede da **PMPA,** será doravante denominada **RESPONSÁVEL.** Todos os demais fornecedores e prestadores de serviços serão denominados **TERCEIROS.**

CONCEITOS

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.

Diante de uma evolução tecnológica cada vez mais rápida e diversa em número de recursos para o acesso à informação, os fornecedores e prestadores de serviços de TIC precisam ter a capacidade de antever as situações possíveis e estarem sempre preparados para o pior cenário, adotando uma postura preventiva e preemptiva que não trabalha mais com o “se pode acontecer”, mas sim “quando e como vai acontecer”.

Fator importante, diante desta velocidade de evolução, a consequente defasagem tecnológica pode tornar vulnerável a infraestrutura e a segurança de TIC, gerando consequências como ineficiência operacional, insatisfação de colaboradores e clientes, morosidade e ineficácia do processo decisório.

Equipamentos estão sujeitos a defeitos de fabricação, de instalação ou de utilização incorreta, à quebra ou à queima de componentes e à má conservação. Sistemas estão sujeitos a falhas técnicas, a vulnerabilidades de segurança, ao mau uso e à negligência na guarda de *credencias* de acesso.

A ausência de controles e processos que permitam identificar estes casos pode comprometer um ou mais dos princípios da **SI** nos mais diversos graus de severidade.

DIRETRIZES

IMAGEM OFICIAL PARA INSTALAÇÃO DE COMPUTADORES

- Equipamentos, para terem acesso ao domínio da **PMPA**, devem ser instalados através de imagens oficiais mantidas e gerenciadas pelo **RESPONSÁVEL**, que fará todas as configurações de acessos, de privilégios e de conformidade. Desta maneira será assegurado um padrão homogêneo e a correta entrada de equipamentos na rede da **PMPA.**
- Conforme o artigo 19 da sessão VI da OS 007/2018 as imagens conterão no mínimo o seguinte conjunto de software:

  I – Sistema operacional de uso difundido.

  II – Navegador para uso da internet e acesso ao correio eletrônico institucional.

  III – Sistema de detecção e mitigação de malwares (antivírus).

  IV – Pacote base de aplicativos de escritório de uso gratuito (editor de textos e de planilha eletrônica).

  V – Programa leitor de *Portable Document Format* (PDF), quando não incluso no próprio sistema operacional.

ACESSO A REDES E INTERNET

Compete ao **RESPONSÁVEL** seguir e/ou implementar as seguintes diretrizes:

- Todos os usuários com acesso à rede e sistemas devem ter uma única identificação de *login*, a qual estará vinculada ao órgão em que estiver exercendo suas atividades, com as respectivas permissões, independentemente do seu órgão de origem.
- 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.
- O acesso a serviços computacionais deve ocorrer sempre através de um procedimento seguro (criptografado), pelo qual o usuário se conecta a um determinado sistema ou rede, que deve ser planejado para minimizar as oportunidades de acessos não autorizados. As senhas poderão ser alteradas pelo usuário a qualquer tempo, conforme a Norma para Utilização De Credencias e Senhas.

- Contas inativas (sem *login* nas estações de trabalho ou *webmail*) há mais de três 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.
- Contas inativas há mais de doze meses serão consideradas elegíveis à remoção, com perda de todo conteúdo associado àquela conta, incluindo mensagens existentes na sua caixa de *e-mai*. 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.
- 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 f*irewalls*, servidores de acesso à internet e ferramentas contra *malwares* e lixo eletrônico (Spam).
- Deve ser formalizado aos usuários, em seu primeiro acesso, que a **PMPA** 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).
- O usuário que efetuar qualquer acesso a *sites* com material indevido deverá ter sua conta bloqueada.
- Todo usuário desligado da **PMPA** ou órgãos vinculados deve ter sua conta imediatamente inativada.

SERVIÇOS DE E-MAIL

Compete ao **RESPONSÁVEL** seguir e/ou implementar as seguintes diretrizes:

- Formalizar aos usuários, em seu primeiro acesso, que todas as informações veiculadas em e-mail pertencem a **PMPA,** podendo esta monitorar, auditar e ter acesso de uso a qualquer tempo.
- 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.
- 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.
- 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:

- Vírus
- Bots
- Adwares
- Trojan Horses
- Worms
- Ramsonwares
- Híbridos e variantes

- A ferramenta de e-mail deve oferecer a funcionalidade de classificação da informação (público, restrito, sigiloso) bem como o informativo de orientação de uso da informação, de acordo com as recomendações de melhores práticas de mercado. Exemplo: “Este e-mail pertence à **PMPA** e as informações contidas não devem ser divulgadas fora do escopo X”.

CONTROLE DE HARDWARE E SOFTWARE

Compete ao **RESPONSÁVEL** cumprir com as seguintes diretrizes:

- Disponibilizar ferramenta para inventário de hardware, com agente de monitoramento capaz de automatizar esta tarefa pela rede, que informe o conjunto de software instalados em cada equipamento, de forma a permitir o dimensionamento e monitoramento da situação do parque computacional para uma gestão eficiente.
- Disponibilizar catálogo de sistemas claro e funcional com todos os sistemas em utilização, descontinuados e em previsão de implantação, devendo ser de fácil consulta de funcionalidades e propósito dentro da **PMPA**.
- Através dos recursos acima, deve monitorar e gerar relatórios de segurança para os gestores responsáveis da **PMPA**, apontando todos os casos que representem potencial risco para a segurança da informação.
- Notificar a gestão dos órgãos impactados e a área responsável pela Governança de TI da **PMPA** sobre a presença de software e/ou hardware descontinuados, sem a garantia de atualizações dos fabricantes, que representem risco a segurança, de forma que estes tomem as providências necessárias.

FUNCIONALIDADES DE BACKUPS

Compete ao **RESPONSÁVEL,** bem como aos **TERCEIROS** que venham a prestar serviços de backup para a **PMPA**, as diretrizes a seguir:

- Adotar e manter uma política de backups clara, eficiente e documentada, de forma que os usuários tenham a condição de compreender e seguir o que é descrito na Norma para Procedimentos de Backup.
- Os recursos de armazenamento destinados aos usuários para backup, que compõe os **Repositórios Oficiais,** devem estar em conformidade com a Norma para Repositório Oficial de Arquivos.
- Obrigatoriamente deve existir redundância de backup, bem como cópia fisicamente separada em nuvem, datacenter externo ou meio semelhante, comprovadamente eficiente e que permita uma recuperação de dados no menor tempo possível.
- O escopo do backup deverá ser definido junto ao setor de Governança de TI da **PMPA** conforme as demandas de cada órgão.
- Backup deve ser unidirecional, ou seja, a infraestrutura de produção não tem capacidade de alterar backups já realizados.
- Backup deve ser não cumulativo. O backup poderá ser recuperado de forma transparente independentemente de ser segmentado de forma incremental, com periodicidade e retenção apropriadas à perda máxima de dados definida para a solução.

INSTALAÇÃO E MANUTENÇÃO DE COMPUTADORES

Compete ao **RESPONSÁVEL** seguir e/ou implementar as seguintes diretrizes:

- Todos os equipamentos de informática deverão ser inventariados e previamente registrados pela área de patrimônio antes de serem conectados na rede da **PMPA**.
- A taxonomia de nomenclatura de máquinas deve seguir o padrão “PA” seguido do número de patrimônio do equipamento e “LC” seguido do número de patrimônio do equipamento, quando de equipamentos locados.
- Instalações devem ser realizadas somente através das imagens oficiais mencionadas nesta norma.
- Deve ser feita a instalação de criptografia de disco padrão nativa do sistema operacional com

habilitação de gestão de chaves via hardware. Esta instalação deverá ser habilitada somente se a máquina tiver suporte de gestão de chaves criptográficas via hardware (TPM 2.0).

- A instalação de equipamentos, adição ou a substituição de peças, periféricos ou outros elementos físicos de informática, que integram o patrimônio do Município, somente poderá ser efetuada pelo **RESPONSÁVEL** e eventuais **TERCEIROS** contratados pela **PMPA** para tal finalidade.
- 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 funcionário que necessita do suporte.
- Manutenções via acesso remoto devem ser feitas por ferramenta e procedimentos seguros aprovados pela equipe de Segurança da Informação do **RESPONSÁVEL.**
- 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 pendrives descartados devem ser fisicamente destruídos.

CRIAÇÃO E USO DE CREDENCIAIS COM PERFIL ADMINISTRATIVO

É de competência do **RESPONSÁVEL** seguir e/ou implementar as seguintes diretrizes:

- Definir os profissionais de seu quadro funcional que, para o exercício de suas funções, recebem credenciais de administrador.
- Contas regulares de usuário, que por padrão são restritivas, não podem ser promovidas e receber permissões administrativas.
- Quando da necessidade de conceder credencial de administrador, um novo usuário deverá ser criado com os acessos necessários, por meio de formalização justificada (requisição de usuário) e autorizada pela equipe de Segurança da Informação do **RESPONSÁVEL**.
- Uma requisição de usuário deve obrigatoriamente conter:
    - Identificação do demandante.
    - A justificativa da necessidade.
    - O período de duração estimado.
    - Demais campos que a **PMPA** e o **RESPONSÁVEL** venham a definir.
- A taxonomia para contas de administrador deverá seguir o formato: “ADM.” + conta de usuário no AD (conta regular).
- 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.
- A taxonomia para criação de contas de administrador para **TERCEIROS** deverá seguir o formato: “3RD.” + “Nome da Empresa” + “Nome e Sobrenome”, limitados a quinze caracteres. A senha será mantida no Sistema de Gerenciamento de Senhas centralizado pelo **RESPONSÁVEL**, e deverá ser modificada semanalmente.

PLANO DE RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

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 da PMPA segura contra eventuais situações que a comprometam.

Como parte complementar a viabilização deste plano, o **RESPONSÁVEL** conjuntamente à Governança de TI do Município deverá estabelecer o Plano de Recuperação de Desastres (DRP).

Histórico de Revisões

Versão	Data	Alterações	Autor	Revisor
1.0	09/02/2023	Versão inicial	(CGTI-SMPAE) Eduardo Hoppe Fernando Delazeri	(CGTI-SMPAE) Eduardo Hoppe