NITERÓI
O FUTURO É AGORA
SEPLAG

Plano de Segurança de Informação

2023

COMITÊ ESTRATÉGICO DE TECNOLOGIA DA INFORMAÇÃO - CETI

FICHA TÉCNICA

Prefeito Municipal de Niterói
Axel Grael

Vice-Prefeito Municipal de Niterói
Paulo Roberto Bagueira

Secretária de Planejamento Orçamento e Modernização da Gestão
Ellen Benedetti

Escritório de Gestão de Projetos
Katherine Azevedo

Secretaria Municipal de Fazenda
Marília Ortiz

Secretaria Municipal de Administração
Luiz Vieira

Secretaria Municipal de Ciência & Tecnologia e Inovação
Valéria Braga

Subsecretário de Modernização da Gestão
Marcelo Zander Vaiano

EQUIPE RESPONSÁVEL PELO PSI

EQUIPE DE ELABORAÇÃO
Ana Clara Magella da Silva Tayão
David da Silva Figueiredo
Marcelo Zander Vaiano
Nayara Aparecida de Oliveira Silva

DIAGRAMAÇÃO
Laís Cândida de Oliveira Dias
Matheus Oliveira Ataliba Cézar

PLANO DE SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I

DISPOSIÇÕES INICIAIS E DEFINIÇÕES

Art. 1º Regulamentar o Plano de Segurança da Informação que tem por finalidade estabelecer critérios que permitam aos Empregados da Prefeitura Municipal de Niterói (PMN) seguir padrões de comportamento no tocante à Segurança da Informação, adequados às necessidades de negócio e de proteção legal da PMN.

Art. 2º Todos os processos de contratação de produtos e serviços devem ser analisados quanto aos aspectos relacionados à Segurança da Informação de forma que, sempre que pertinente, estejam sujeitos aos requisitos de conformidade a este plano e às suas normas complementares.

CAPÍTULO II

DEFINIÇÕES

DADOS	Trata-se da informação não processada
INFORMAÇÃO	É um ativo composto por um conjunto de dados ou elementos que tem valor relevante e, consequentemente, necessita ser adequadamente protegido de alteração, destruição e divulgação não autorizadas, quer seja acidental ou intencional
CONFIDENCIALIDADE	Propriedade que garante que a informação só está disponível a indivíduos ou processos autorizados

GRAU DE SENSIBILIDADE	É a classificação adotada para limitar o acesso à Informação de acordo com sua natureza e importância para o negócio da PMN. A Informação poderá ser identificada e classificada como: • Crítica - Informação restrita que, caso seja divulgada erroneamente, afetará a continuidade de um ou mais processos de negócio dos órgãos/entidades da PMN; • Média - Informação interna que, caso seja divulgada erroneamente, poderá difamar a imagem da instituição ou causar prejuízos indiretos; • Normal - Informação irrestrita em termos de divulgação e que poderá ser de conhecimento público.
ÁREA DE TECNOLOGIA DA INFORMAÇÃO	É a área responsável pela administração da infraestrutura de TIC dentro do órgão/entidade da PMN, cumprindo as regras especificadas pelo Gestor da Informação
GESTOR DA INFORMAÇÃO	É o empregado ou entidade da hierarquia da PMN responsável pelo teor e pela classificação da Informação
EMPREGADO	É todo empregado que, por uma finalidade específica, venha a ter acesso a Informações da PMN. • Empregado de outras instituições a serviço da PMN - Parceiro, estagiário ou outra pessoa que terá acesso a Informações da PMN, desde que comprovada à necessidade e conveniência para a PMN, após análise e aprovação da Área de Tecnologia da Informação.
TECNOLOGIA DA INFORMAÇÃO	É o patrimônio composto por elementos de hardwares, softwares, licenças e demais componentes necessários para a execução dos sistemas e processos do órgão/entidade

REDE CORPORATIVA	É o conjunto de recursos de infraestrutura, serviços e aplicações de Tecnologia da Informação, mantidos pela Área de Tecnologia da Informação e que tem por objetivo prover interconexão e disponibilizar informações para que sejam suportados os processos organizacionais do órgão/entidade
EQUIPAMENTO	É o conjunto de instrumentos necessários ao desenvolvimento de atividades informatizadas (micro, impressora, periférico, acessórios)
SERVIDOR CORPORATIVO	É o equipamento centralizador, destinado ao armazenamento de Informações Corporativas
SISTEMA/APLICATIVO	É todo o sistema de computação e software que abrange procedimentos e documentação relativa à sua operação
CRIPTOGRAFIA	É a aplicação de um sistema/aplicativo para tornar incompreensível um conjunto de dados, voz ou imagem, com observância de normas especiais consignadas numa cifra ou num código
PLANO DE CONTINGÊNCIA E CONTINUIDADE	É o plano que tem o objetivo de não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos
SENHA	É o meio de validação da identidade e, consequentemente, de estabelecimento dos direitos de acesso para os recursos ou serviços de processamento da informação dentro de um sistema ou ambiente

Para os fins do disposto neste Plano, a segurança da informação abrange:

- A segurança cibernética;
- A defesa cibernética;

- A segurança física e a proteção de dados organizacionais;
- As ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

CAPÍTULO III

ORIENTAÇÕES GERAIS DE SEGURANÇA DA INFORMAÇÃO

Artº 3 Os mecanismos, procedimentos e equipamentos de segurança adotados pelos órgãos e entidades da PMN deverão ser praticados e/ou operados quando da utilização dos recursos de Tecnologia da Informação.

Artº 4 A Área de Tecnologia da Informação deverá manter equipamentos/sistemas/aplicativos de segurança para controlar o acesso aos recursos de Tecnologia da Informação e para interligar a Rede Corporativa a outras redes.

Artº 5 Serão aplicados recursos de segurança de grau de complexidade compatível com o nível de importância definido para a Informação.

Artº 6 A identificação e a classificação do nível de importância da Informação para o órgão/entidade serão definidas pelo gestor da Informação, responsável por gerar e/ou armazenar a Informação.

Artº 7 O Gestor da Informação deverá analisar periodicamente a classificação da Informação em termos de valor e impacto para o órgão/entidade, pois a aquisição de novos ativos e a manipulação de novas Informações poderão mudar a prioridade de implementação dos controles de segurança.

Artº 8 Na classificação da Informação, deverá se buscar, sempre que possível, o grau de segurança menos restritivo que não comprometa a Informação, visando otimizar e agilizar o processo de tratamento da Informação e, ao mesmo tempo, reduzir os seus custos de proteção.

Artº 9 Para a Informação classificada como “crítica”, deverá ser preservado o seu registro histórico, com a identificação inequívoca do usuário que a acessou, de forma a permitir a execução do processo de Auditoria Interna, a ser viabilizada pelo Comitê Estratégico de Tecnologia da Informação (CETI), caso necessária.

Artº 10 Ao classificar uma Informação como “crítica” ou “média”, deverão ser indicados as pessoas, os grupos de trabalho, os órgãos e as organizações que têm permissão de acesso a ela.

Artº 11 A Informação que não possuir uma classificação explícita quanto a sua confidencialidade deverá ser considerada como “normal”.

Artº 12 A implantação de sistema/aplicativo e/ou Informação Corporativa deverá ser precedida da definição de procedimentos de segurança, monitoração e contingência.

Artº 13 A Informação Corporativa será armazenada de forma centralizada pela Área de Tecnologia da Informação, que será responsável por manter mecanismos de segurança com o objetivo de impedir a violação e a quebra de sigilo, garantir sua disponibilidade e proteger contra perda ou dano do original.

Artº 14 Toda Informação gerada, armazenada ou veiculada no órgão/entidade é de propriedade do órgão/entidade, reservando-se a este o direito de monitorar e registrar o uso da mesma.

Artº 15 A divulgação de Informação em nome da PMN somente poderá ser feita por Empregado devidamente autorizado.

Artº 16 O usuário será responsável pela segurança das Informações armazenadas no seu equipamento, arcando com o ônus da perda ou dano dos dados.

Artº 17 A instalação de aplicativos antivírus e sua atualização sistemática nos equipamentos do órgão/entidade serão de responsabilidade da Área de Tecnologia da Informação.

Artº 18 Para evitar a disseminação de vírus, o usuário deverá utilizar os meios de armazenamento portátil (pen drive, CD, DVD) somente no equipamento instalado no respectivo órgão/entidade de lotação.

§ 1º O meio de armazenamento portátil de origem externa ao ambiente do usuário deverá ser examinado e descontaminado previamente pelo sistema/aplicativo antivírus adotado pelo órgão/entidade.

Artº 19 A responsabilidade pela Segurança da Informação deverá ser atribuída na fase de admissão do Empregado no órgão/entidade e prevista no contrato individual de trabalho.

Artº 20 O Empregado, em qualquer nível hierárquico, na sua esfera de competência, será responsável em cumprir e fazer cumprir a aplicação eficaz das normas e princípios da Segurança da Informação, no compromisso com os critérios legais e éticos que envolvem o órgão/entidade. É de sua responsabilidade qualquer prejuízo ou dano que vier a sofrer ou causar a PMN ou a terceiros, em decorrência de não obediência às diretrizes e normas acima referidas.

Artº 21 O Empregado será responsável pela confidencialidade de qualquer senha que lhe tenha sido concedida para acesso ou uso da Informação do órgão/entidade, sendo a senha de caráter pessoal e intransferível, não podendo ser compartilhada em nenhuma hipótese.

§ 1º Será também de responsabilidade do Empregado o uso de Senha segura, devendo alterá-la conforme periodicidade determinada pelo órgão/entidade.

Artº 22 Quando o Empregado tomar atitudes ou ações contrárias às diretrizes deste Plano ou às normas correlatas, estará sujeito às penalidades estabelecidas em normas disciplinares da PMN ou em contrato de prestação de serviço específico.

Artº 23 Deverão ser previstas, nos contratos de prestação de serviços de terceiros, cláusulas que contemplem as responsabilidades no cumprimento do Plano de Segurança da Informação da PMN e de suas normas e procedimentos.

Artº 24 O usuário externo, ao executar serviços autorizado pela Área de Tecnologia da Informação ou pelo órgão/entidade detentor de equipamento de informática, deverá evitar ao máximo utilizar os meios de armazenamento portátil de sua propriedade em equipamento instalado no órgão/entidade.

§ 1º O empregado que acompanhar a execução dos serviços deverá fiscalizar o cumprimento desta norma de segurança e, em caso de necessidade de utilizar meios de armazenamento portátil, deverá solicitar o exame e a descontaminação prévios.

Artº 25 Será terminantemente proibido ao Empregado utilizar a Informação e o Ativo de Tecnologia da Informação para outros fins que não os estritamente profissionais, associados às atribuições de sua contratação específica, e contrários aos critérios estabelecidos neste Plano ou em outros Atos Normativos que tratem do assunto, especialmente em situação de pirataria, pornografia, cassino, incitação à violência ou racismo, estando sujeito a penalidades internas e a responder civil e criminalmente por seus atos.

Artº 26 Todo o Incidente de Segurança que afetar a Informação deverá ser reportado ao Comitê Estratégico de Tecnologia da Informação (CETI), que tem atribuição de criar normas e padrões técnicos a serem observados pelos órgãos e pelas entidades, validar e aprovar os instrumentos instituídos pela EGD e promover a governança da tecnologia da informação e comunicação, bem como estabelecer diretrizes de segurança da informação no âmbito da Prefeitura Municipal de Niterói e suas entidades vinculadas, caracterizando-se como a entidade mais adequada para tratar do assunto.

CAPÍTULO IV

ACESSO

Artº 27 O acesso à Rede Corporativa será disponibilizado pela Área de Tecnologia da Informação de acordo com o nível de acesso estabelecido pela titular de cada órgão de nível mínimo gerencial.

Artº 28 Não será permitido acesso individual a outras redes interligadas à Rede Corporativa.

Artº 29 O acesso será controlado por equipamentos e sistemas/aplicativos com o objetivo de identificar e registrar a solicitação de acesso do usuário aos recursos de Tecnologia da Informação, bem como impedir o acesso não autorizado à rede interna do órgão/entidade em geral e, em especial, aos bancos de dados corporativos.

Artº 30 O usuário dos serviços da Rede Corporativa será cadastrado e terá um identificador individual e único, de acordo com os procedimentos operacionais definidos pela Área de Tecnologia da Informação.

Artº 31 O Acesso à Rede Corporativa do órgão/entidade se dará através de senha pessoal e intransferível, cuja guarda e sigilo é de responsabilidade do usuário.

§ 1º O usuário deverá manter o sigilo da sua senha, sendo de sua responsabilidade o uso indevido, inclusive quando utilizada por terceiros.

Artº 32 Será registrado o acesso à Informação identificada e classificada, quanto ao seu grau de sensibilidade, como “crítica” e “média”.

Artº 33 A Informação classificada como “crítica” será criptografada e protegida por senha de acesso pessoal, de responsabilidade de cada usuário.

Artº 34 Será vedado o uso de equipamento de informática de propriedade particular no âmbito das instalações dos órgãos/entidades da PMN.

§ 1º Será permitida a utilização de equipamento particular se for comprovada a necessidade e conveniência para a PMN, após análise e aprovação da Área de Tecnologia da Informação do órgão/entidade.

Artº 35 As configurações das estações de trabalho não deverão ser alteradas pelo usuário.

Artº 36 Deverá ser desconectado da rede o equipamento que seja definido pelo usuário e/ou pelos padrões do órgão/entidade como detentor de Informações que devam estar protegidas com segurança total e que devam ter acesso físico especial.

Artº 37 As salas dos servidores corporativos deverão ter controle de acesso físico, sendo proibida a entrada de pessoas não autorizadas.

Artº 38 Os serviços de Correio Eletrônico Interno e Internet deverão garantir a identidade do emitente e, quando necessário, deverão ser compactados as mensagens e arquivos enviados.

Artº 39 Ao acessar a Rede Corporativa, internamente ou externamente, o usuário não poderá, em hipótese alguma, deixar sua conexão ativa, seja em que ambiente for. Ao descumprir esta determinação, o usuário implicitamente será responsável pelo uso indevido do acesso à Rede que venha a ser feito a partir de sua chave de acesso.

Artº 40 O acesso externo às Informações de uso restrito por meio da INTERNET, como aplicações específicas a determinadas áreas do órgão/entidade, deverá ser solicitado à Área de Tecnologia da Informação pelo titular de cada órgão de nível mínimo gerencial.

Artº 41 Para utilização da Rede Corporativa fora das dependências do órgão/entidade por meio de equipamentos e dispositivos móveis de propriedade dos mesmos, deverão ser observados os critérios estabelecidos nas normas aplicáveis a equipamentos fixos, como também:

- Somente realizar o trabalho quando houver certeza de que o local é seguro.
- Jamais deixar o equipamento desassistido ou sob a guarda de pessoas estranhas.

Artº 42 Os registros de eventos ocorridos na rede (log) devem ser protegidos adequadamente contra adulteração e destruição, para que não percam sua característica de evidência legal.

Artº 43 A PMN se reservará ao direito de produzir e manter trilhas de auditoria, registrando o uso de recursos e serviços da Rede Corporativa de maneira geral, bem como as exceções e outros eventos de segurança relevantes, a fim de auxiliar investigações futuras e a monitoração de acesso.

Artº 44 O desligamento de Empregados, empregados de outras instituições a serviço da PMN, estagiários ou o encerramento do serviço prestado à PMN por prestadores de serviço deverá ser comunicado à Área de Tecnologia da Informação imediatamente após a sua saída, para que o direito de acesso seja desativado.

Artº 45 A transferência de Empregado deverá ser comunicada à Área de Tecnologia da Informação imediatamente, para que seu direito de acesso seja revisto.

Artº 46 A validade do acesso dos prestadores de serviço não poderá ultrapassar o limite estabelecido nas instruções operacionais na INTRANET, ocasião em que o acesso será automaticamente suspenso ou renovado, quando necessário.

Artº 47 Toda Informação disponibilizada a um Empregado ou grupo de Empregados será de uso restrito e confidencial, a menos que o Gestor da Informação a torne disponível explicitamente para outros usuários ou grupos de usuários.

Artº 48 O acesso à Informação deverá ficar restrito aos Empregados e demais Empregados autorizados para tanto, observando-se a classificação da Informação.

CAPÍTULO V

DISPONIBILIDADE

Artº 49 Será elaborado um Plano de Contingência e Continuidade do negócio, que deverá ser implementado e testado periodicamente e que deve definir, no mínimo:

- As ações, os procedimentos e a programação de testes com o objetivo de restabelecer o funcionamento dos recursos essenciais de Tecnologia da Informação;
- Os meios alternativos de funcionamento dos recursos de Tecnologia da Informação;
- Instruções para manter armazenada a configuração padrão dos equipamentos, com o objetivo de permitir a sua restauração imediata em caso de falhas.

Artº 50 As Informações dos órgãos/entidades da PMN deverão ser protegidas por uma cópia de segurança, para que possa ser utilizada em caso de perda ou dano do original.

- Diariamente deverão ser feitas cópias de segurança de todas as Informações armazenadas nos servidores corporativos.
- No primeiro dia útil de cada mês, deverá ser feita uma cópia de segurança de todos os dados dos servidores corporativos, que será guardada em uma instalação distante do local onde estarão guardadas as cópias diárias.
- A área detentora de Informações que necessitem de uma agenda específica deverá combinar sua programação especial com a Área de Tecnologia da Informação do seu órgão/entidade.
- A definição da periodicidade para produção de cópia de segurança de Informações não corporativas será do titular do órgão de nível mínimo gerencial, que deverá objetivar uma recuperação de dados que permita a continuidade dos serviços.

NITERÓI

O FUTURO É AGORA

SEPLAG