DECRETO Nº 4134/2024.

DISPÕE SOBRE A APROVAÇÃO DA NORMA COMPLEMENTAR PARA GESTÃO DE ATIVOS DE TIC DO MUNICÍPIO DE RIO DAS OSTRAS.
O PREFEITO DO MUNICÍPIO DE RIO DAS OSTRAS, Estado do Rio de Janeiro, no uso de suas atribuições legais, em consonância ao Processo Administrativo nº 44568/2024;

DECRETA:

CAPÍTULO I
DA NORMA COMPLEMENTAR PARA GESTÃO DE ATIVOS DE TIC

Seção I
Da Introdução

Art. 1º Esta Norma Complementar tem por objetivo estabelecer as normas relativas ao inventário e mapeamento de ativos de tecnologia da informação no âmbito do Município de Rio das Ostras.

CAPÍTULO II
DO PROPÓSITO

Art. 2º O objetivo desta normativa é garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.
Art. 3º Para manter a segurança e continuidade do negócio do Município, em sua missão é fundamental mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização. Auxiliando também na recuperação de incidentes.

CAPÍTULO III
DOS TERMOS E DEFINIÇÕES

Art. 4º Esta Norma Complementar estabelece os termos e definições, da seguinte forma:

I- ATIVOS DE INFORMAÇÃO: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
II- INCIDENTE: interrupção não planejada ou redução da qualidade de um serviço, ou seja, ocorrência, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;
III- GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO: processo de natureza permanente, estabelecido, direcionado e monitorado pela alta administração, que contempla as atividades de identificação, avaliação e gerenciamento de potenciais eventos que possam afetar a organização, destinado a fornecer segurança razoável quanto à realização de seus objetivos;
IV- INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

CAPÍTULO IV
DA REFERÊNCIA LEGAL E DE BOAS PRÁTICAS

Art. 5º Esta Norma apresenta a referência legal e de boas práticas, no quadro seguinte:

Orientação	Seção
Decreto Municipal Nº 4060/2024 – Política de Segurança da Informação	Em sua íntegra
Lei Nº 13.709/2018 – Lei Geral de Proteção de Dados	CAPÍTULO VII - Seção I – Art. 46, Seção II Art. 50
Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança – Sistemas de gestão de segurança da informação - Requisitos;	A.8 (A.8.1., A.8.2., A.8.3.)
CIS - Center for Internet Security	Em sua íntegra
MITRE ATT&CK	Em sua íntegra

CAPÍTULO V
DAS DISPOSIÇÕES GERAIS

Seção I
Da Gestão de Ativos

Art. 6º A norma complementar de Gestão de Ativos de informação deve estar alinhada com a Política de Segurança da Informação vigente.
Art. 7º A Política de Gestão de Ativos de informação deve estar alinhada com uma gestão de continuidade de negócios em nível organizacional.
Art. 8º O processo de mapeamento de ativos de informação deve estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças nos aspectos relativos à segurança da informação.
Art. 9º As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.
Art. 10. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.
Art. 11. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter:
I- os responsáveis (proprietários e custodiantes) de cada ativo de informação;
II- as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação;

III- as interfaces de cada ativo de informação e as interdependências entre eles.

Art. 12. O Município empregará o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.
Art. 13. Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:
I- ativos físicos;
II- bancos de dados;
III- dispositivos móveis;
IV- hardwares;
V- níveis de permissões;
VI- serviços;
VII- softwares.

Art. 14. O Município utilizará controles técnicos em todos os ativos para garantir que apenas software autorizado seja executado, sendo estes reavaliados semestralmente ou com mais frequência.
Art. 15. O Município utilizará controles técnicos para garantir que apenas bibliotecas e scripts autorizados, e assinados digitalmente tenham permissão para serem executados.
Art. 16. O Município utilizará de scripts e protocolos de segurança para o acesso e administração dos ativos de informação.
Art. 17. O Município deverá elaborar e manter diagramas e demais documentações da arquitetura de rede da organização. A revisão destas documentações deverá ser realizada de forma periódica ou quando ocorrerem mudanças significativas, que possam impactar tais artefatos.
Art. 18. O Município deverá garantir que a infraestrutura de rede da organização esteja atualizada. Deverá ser realizada uma revisão das versões de software de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da organização.
Art. 19. O inventário também deverá incluir atualizações ou remoções dos softwares, bem como dos sistemas de informação.
Art. 20. As atualizações e novas versões de softwares devem ser avaliadas e aprovadas antes da instalação.

Seção II
Das Diretrizes

Art. 21. A Gestão de Tecnologia da Informação definirá a estratégia para o Processo de Inventário e Mapeamento de Ativos para cada ciclo de execução, que incluirá:
I- o escopo de coleta;
II- o conjunto mínimo de informações de cada ativo e a identificação de seus responsáveis;
III- a caracterização dos contêineres;
IV- a definição dos requisitos de segurança da informação e comunicações.

Art. 22. O Processo de Inventário e Mapeamento de Ativos de Informação é composto pelas seguintes etapas:
I- coleta de informações gerais dos ativos de informação;
II- detalhamento dos ativos de informação;
III- caracterização dos contêineres dos ativos de informação;
IV- definição dos requisitos de segurança da informação e comunicações.

Art. 23. A Coleta de Informações Gerais dos Ativos de Informação consiste na definição dos responsáveis pela coleta e na utilização de um conjunto essencial de informações para cada ativo de informação.
Art. 24. O detalhamento do ativo deve contemplar informações que determinem com clareza e objetividade o conteúdo do ativo de informação, os responsáveis e respectivos requisitos de segurança da informação.
Art. 25. O contêiner é o local onde “vive” o ativo de informação e, assim, recomenda-se que tal contêiner seja caracterizado, no mínimo, com a lista de todos os recipientes em que um ativo da informação é armazenado, transportado ou processado, e respectiva indicação dos responsáveis por manter estes recipientes.
Art. 26. Os requisitos de segurança da informação e comunicações devem ser definidos por meio de critérios que atendam a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.
Art. 27. Os critérios devem ser categorizados, no mínimo, em 5 categorias de controle:
I- tratamento da informação;
II- controles de acesso físico e lógico;
III- gestão de risco de segurança da informação e comunicações;
IV- tratamento e respostas a incidentes em redes computacionais;
V- gestão de continuidade dos negócios nos aspectos relacionados à segurança da informação e comunicações.

Seção III
Da Padronização

Art. 28. Todo ativo de TIC deve seguir padronização de configuração definida pela Gestão de Tecnologia do Município.
Art. 29. Os requisitos básicos de configuração para cada tipo de ativo podem ser encontrados no portal GovTIC, na área específica de documentação técnica.

CAPÍTULO VI
DA CLASSIFICAÇÃO DE NÍVEL DE ACESSO DAS INFORMAÇÕES

Art. 30. Todos os ativos de informação devem ser classificados de acordo com seu nível de acesso, a fim de assegurar o direito fundamental de acesso à informação, bem como dispor sobre a devida restrição de acesso sobre informações sigilosas, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e demais normas aplicáveis.
Art. 31. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação do Município, independentemente de seu formato e suporte, devem ser classificadas segundo seu nível de acesso, de acordo com a legislação pertinente, sobretudo com as disposições da LAI, do Decreto nº 7.724, de 16 de maio de 2012, e orientações ou normas complementares editadas por órgãos competentes.
Art. 32. A classificação de nível de acesso das informações deve observar às diretrizes constantes na LAI, Decreto nº 7.724, de 16 de maio de 2012 e outros normativos complementares.
Art. 33. As informações devem ser classificadas conforme os seguintes níveis de acesso:
I- PÚBLICA: com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;

II- RESTRITA: quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso;
III- SIGILOSA CLASSIFICADA EM GRAU DE SIGILO: nos termos do art. 23 da Lei nº 12.527/2011, subdividida nos graus ultrassecreto, secreto ou reservado.

Art. 34. Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de nível de acesso de informações usados pela organização.

CAPÍTULO VII
DAS VIOLAÇÕES, PENALIDADES E SANÇÕES

Art. 35. Cabe à área responsável pela gestão de TIC no âmbito do Município definir os aspectos relacionados à plataforma tecnológica, gestão operacional, forma de autenticação e sustentação do domínio de rede corporativa.
Art. 36. As ocorrências de mau uso do acesso aos recursos disponíveis na rede e sistemas corporativos não previstas nesta norma e os casos omissos serão encaminhados para a área responsável pela gestão de TIC no âmbito do Município para análise e pronunciamento.
Art. 37. O descumprimento dessa Norma poderá resultar em sanções administrativas, civis e criminais, na forma da Lei.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 38. Orientações e devidas documentações técnicas a respeito da gestão de ativos TIC estão disponíveis no Portal GovTIC: https://www.riodasostras.rj.gov.br/govtic/.
Art. 39. Este Decreto entra em vigor na data de sua publicação, aprovando a Norma Complementar para Gestão de Ativos de TIC.

Rio das Ostras, 22 de novembro de 2024.

MARCELINO CARLOS DIAS BORBA
Prefeito do Município de Rio das Ostras

DECRETO Nº 4135/2024

DISPÕE SOBRE A APROVAÇÃO DA NORMA COMPLEMENTAR PARA GESTÃO DE INCIDENTES DE TIC DO MUNICÍPIO DE RIO DAS OSTRAS.
O PREFEITO DO MUNICÍPIO DE RIO DAS OSTRAS, Estado do Rio de Janeiro, no uso de suas atribuições legais, em consonância ao Processo Administrativo nº 44568/2024;

DECRETA:

CAPÍTULO I
DA NORMA COMPLEMENTAR PARA GESTÃO DE INCIDENTES DE TIC

Seção I
Da Introdução

Art. 1º Esta Norma Complementar tem por objetivo estabelecer as diretrizes para o Serviço de Tratamento de Incidentes de tecnologia da informação no âmbito do Município de Rio das Ostras.

CAPÍTULO II
DO PROPÓSITO

Art. 2º Esta Norma complementar se aplica a todos os usuários de serviços de tecnologia da informação institucionais, tais como:
I- servidores do quadro permanente;
II- comissionados;
III- cedidos;
IV- requisitados;
V- terceirizados;
VI- discentes;
VII- estagiários;
VIII- prestadores de serviços;
IX- usuário de unidade/setor; e
X- pessoal de associação temporária que usam serviços de tecnologia da informação do Município de Rio das Ostras com acesso restrito, ou acesso autenticado.

Art. 3º O Processo de Gerenciamento de Incidentes de TIC é responsável em gerenciar o ciclo de vida de todos os incidentes.
Parágrafo único. Na terminologia ITIL, um “incidente” pode ser definido como uma interrupção não planejada ou redução da qualidade em um Serviço de TIC.
Art. 4º É também responsabilidade do Processo de Gerenciamento de Incidentes de TIC restaurar a operação do serviço à sua normalidade o mais rapidamente possível e minimizar os impactos adversos para as áreas de Negócio, assegurando que a qualidade dos níveis de serviço acordados sejam mantidos.
Art. 5º Principais objetivos:
I- assegurar que métodos e procedimentos padronizados sejam utilizados para atuar de forma rápida e eficiente na resposta aos incidentes;
II- reduzir o impacto nas áreas de Negócio causados por indisponibilidades não programadas;
III- monitorar o ambiente de TIC a fim de reduzir possíveis incidentes garantindo rápida atuação por parte da Central de Serviços e dos Grupos Solucionadores;
IV- alinhar as atividades deste processo com as prioridades das áreas de Negócio;
V- manter a satisfação dos usuários com a qualidade dos Serviços de TIC.

CAPÍTULO III
DOS TERMOS E DEFINIÇÕES