

 ICTIM <small>INSTITUTO DE CIÊNCIA TECNOLOGIA E INOVAÇÃO DE MARICÁ</small>	DIRETORIA DE INFRAESTRUTURA	NI-INFRA-001	REV. N° 04
		ELABORADA EM ABR/2025	PÁGINA 1 de 6

SUMÁRIO

- 1 Objetivo**
- 2 Campo de Aplicação**
- 3 Responsabilidade**
- 4 Documentos de Referência**
- 5 Conceitos**
- 6 Definições**
- 7 Diretrizes Gerais**

	DIRETORIA DE INFRAESTRUTURA	NI-INFRA-001	REV. N° 04
		ELABORADA EM ABR/2025	PÁGINA 2 de 6

1 OBJETIVO

Esta Norma estabelece os procedimentos e rotinas para Garantir a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das informações necessárias para a realização dos negócios do Instituto de Ciência, Tecnologia e Informação de Maricá - ICTIM.

2 CAMPO DE APLICAÇÃO

Esta Norma se aplica a todos os administradores, funcionários, estagiários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento, ou com acesso a informações que pertençam ao Instituto de Ciência, Tecnologia e Informação de Maricá - ICTIM.

Todo e qualquer usuário de recursos computacionais deste Instituto tem a responsabilidade de proteger a segurança e a integridade das informações e dos equipamentos de informática..

3 RESPONSABILIDADE

A responsabilidade pela revisão e cancelamento desta Norma é da Diretoria de Infraestrutura.

4 DOCUMENTOS DE REFERÊNCIA

Normativo	Do que se refere
Lei nº 13.709/2018	A Lei Geral de Proteção de Dados Pessoais (LGPD)
Decreto Municipal nº 840, de 05 de abril de 2022 (Prefeitura de Maricá)	Regulamenta a aplicação da Lei Federal Nº 13.709, de 14 de agosto de 2018 - Lei Geral De Proteção de Dados Pessoais (LGPD) – no âmbito da Administração Municipal Direta e Indireta do Município de Maricá/RJ.

5 CONCEITOS

A segurança da informação é aqui caracterizada pela preservação dos seguintes conceitos:

- **Confidencialidade:** Garante que a informação seja acessível somente pelas pessoas autorizadas, pelo período necessário;
- **Disponibilidade:** Garante que a informação esteja disponível para as pessoas autorizadas sempre que se faça necessário;
- **Integridade:** Garante que a informação esteja completa e íntegra e que não tenha sido modificada ou destruída de maneira não autorizada ou acidental durante o seu ciclo de vida.

	DIRETORIA DE INFRAESTRUTURA	NI-INFRA-001	REV. N° 04
		ELABORADA EM ABR/2025	PÁGINA 3 de 6

6 DEFINIÇÕES

- **Informação:** resultado do processamento e organização de dados (eletrônicos ou físicos) ou registros de um sistema.
- **Ativos de Informação:** conjunto de informações, armazenado de modo que possa ser identificado e reconhecido como valioso para a empresa.
- **Sistemas de informação:** de maneira geral, são sistemas computacionais utilizados pela empresa para suportar suas operações.
- **Segregação de funções:** consiste na separação entre as funções de autorização, aprovação de operações, execução, controle e contabilização, de tal maneira que nenhum funcionário, estagiário ou prestador de serviço detenha poderes e atribuições em desacordo com este princípio.
- **Grupo Gestor da Segurança da Informação:** grupo composto por administradores do Instituto de Ciência, Tecnologia e Informação de Maricá - ICTIM com o objetivo de avaliar a estratégia e diretrizes de segurança da informação seguidas pela empresa.

6.1 SIGLAS

- **ICTIM-** Instituto de Ciência, Tecnologia e Inovação de Maricá
- **NI** - Norma Interna
- **LGPD** - Lei Geral de Proteção de Dados Pessoais
- **TI** – Tecnologia da Informação
- **DI** – Diretoria de Infraestrutura

6.2 CLASSIFICAÇÃO DA INFORMAÇÃO

Toda informação produzida no desenvolvimento das atividades da empresa deve ser classificada de acordo com os níveis de confidencialidade abaixo:

- **Pública:** É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral. Por exemplo: informações disponíveis na página da Internet do Instituto de Ciência, Tecnologia e Informação de Maricá
- **Interna:** É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização. Exemplo: boletim semanal.
- **Confidencial:** É toda informação que pode ser acessada por usuários da organização e por parceiros da organização especificamente autorizados. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro. Exemplo: propostas comerciais.
- **Restrita:** É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização. Exemplo: dados da folha de pagamento são de acesso restrito apenas ao setor de RH.

6.3 RESPONSABILIDADES

De forma geral, cabe a todos os administradores, funcionários, estagiários e prestadores de serviços:

	DIRETORIA DE INFRAESTRUTURA	NI-INFRA-001	REV. N° 04
		ELABORADA EM ABR/2025	PÁGINA 4 de 6

- Cumprir fielmente a Política de Segurança da Informação do Instituto de Ciência, Tecnologia e Informação de Maricá - ICTIM;
- Proteger as informações contra acessos, modificação, destruição ou divulgação não autorizados pela ICTIM;
- Assegurar que os recursos tecnológicos, as informações e sistemas à sua disposição sejam utilizados apenas para as finalidades aprovadas pela ICTIM;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Não compartilhar informações confidenciais de qualquer tipo;
- Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

É dever de todos dentro do Instituto de Ciência, Tecnologia e Informação de Maricá - ICTIM:

- Considerar a informação como sendo um ativo da organização, um dos recursos críticos para a realização do negócio, que possui grande valor para o Instituto de Ciência, Tecnologia e Informação de Maricá – ICTIM e deve sempre ser tratada profissionalmente.
- É de responsabilidade do Gerente/Supervisor de cada área classificar a informação (relatórios, documentos, modelos, procedimentos, planilhas) gerada por sua área de acordo com o nível de confidencialidade estabelecido neste documento.

São boas práticas:

- Bloquear o acesso ao computador sempre que sair da sua mesa de trabalho, mesmo que por alguns minutos;
- Manter mesas organizadas e documentos com informações confidenciais trancados, quando não os estiver utilizando.

6.4 GRUPO GESTOR DA SEGURANÇA DA INFORMAÇÃO DO INSTITUTO DE CIÊNCIA, TECNOLOGIA E INFORMAÇÃO DE MARICÁ - ICTIM

Missão

- Ser o gestor do processo de segurança e proteger as informações da organização, catalisando, coordenando, desenvolvendo e/ou implementando ações para esta finalidade.

Grupo Gestor	
Nome	Cargo/Lotação
Laércio Rocha	Diretor de Infraestrutura
Emerson Alencar	Assessor de TI

	DIRETORIA DE INFRAESTRUTURA	NI-INFRA-001	REV. N° 04
		ELABORADA EM ABR/2025	PÁGINA 5 de 6

7 DIRETRIZES GERAIS

7.1 DADOS PESSOAIS DE FUNCIONÁRIOS

- O Instituto De Ciência, Tecnologia e Informação De Maricá – ICTIM se compromete em não acumular ou manter intencionalmente dados pessoais de funcionários além daqueles relevantes na condução do seu negócio. Todos os dados pessoais de funcionários serão considerados confidenciais.
- Os dados pessoais de funcionários sob a responsabilidade do Instituto de Ciência, Tecnologia e Informação de Maricá - ICTIM não serão usados para fins diferentes daqueles para os quais foram coletados.
- Dados pessoais de funcionários não serão transferidos para terceiros, exceto quando exigido por Autarquia superior, e desde que tais terceiros mantenham a confidencialidade dos referidos dados.

7.2 PROGRAMAS ILEGAIS

- É terminantemente proibido o uso de programas ilegais (software pirata) no ICTIM. Os usuários não podem, em hipótese alguma, instalar este tipo de programa nos equipamentos deste ICTIM.
- Periodicamente, o Grupo Gestor da Segurança da Informação do Instituto de Ciência, Tecnologia e Informação de Maricá - ICTIM fará verificações nos dados dos servidores e/ou nos computadores dos usuários, visando garantir a correta aplicação desta diretriz.

7.3 ADMISSÃO/DEMISSÃO DE SERVIDORES / COLABORADORES

- O setor de RH do Instituto de Ciência, Tecnologia e Inovação de Maricá - ICTIM deverá informar toda e qualquer movimentação de temporários e/ou estagiários, e admissão/demissão de colaboradores, para que os mesmos possam ser cadastrados ou descadastrados nos sistemas do ICTIM. O RH deverá questionar ao setor responsável pela contratação quais sistemas e repositórios de arquivos de trabalho o novo colaborador deverá ter direito de acesso. Essas informações deverão ser registradas e encaminhadas para o Grupo Gestor da Segurança da Informação através do “Formulário para concessão e revogação de acessos aos recursos computacionais do Instituto de Ciência, Tecnologia e Inovação de Maricá - ICTIM”,
- O Grupo Gestor da Segurança da Informação do Instituto de Ciência, Tecnologia e Inovação de Maricá - ICTIM fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, que deverá ser trocada pelo usuário no seu primeiro acesso.
- No caso de desligamento, o setor de RH deverá comunicar o fato na mesma data ao Grupo Gestor da Segurança da Informação, por meio do “Formulário para concessão e revogação de acessos aos recursos computacionais do Instituto de Ciência, Tecnologia e Inovação de Maricá - ICTIM” para que todos os acessos concedidos sejam revogados.
- Cabe ao setor de RH dar conhecimento e obter as devidas assinaturas de concordância dos novos contratados em relação à Política de Segurança da Informação do Instituto de Ciência, Tecnologia e Inovação de Maricá - ICTIM.

	DIRETORIA DE INFRAESTRUTURA	NI-INFRA-001	REV. N° 04
		ELABORADA EM ABR/2025	PÁGINA 6 de 6

7.4 POLÍTICA DE SENHAS

- Recomendamos que as senhas tenham sempre no mínimo de 8 (oito) caracteres alfanuméricos, contendo pelo menos uma letra maiúscula e um caractere especial;
- Recomendamos que as senhas também sejam ser trocadas pelos usuários a cada 3 meses, não devendo se repetir as senhas definidas nos últimos 12 meses;
- Sempre que um usuário é desligado da organização, todas as suas senhas e acessos são revogados no mesmo dia.

HISTÓRICO DE ELABORAÇÃO E QUADRO DE APROVAÇÃO

Quadro de Aprovação		
	Nome	Cargo/Lotação
Elaborado por:	Emerson Alencar	Assessor de TI / DI
	Márcio Santarém	Analista TI / DI
Aprovado por:	Laércio Rocha	Diretor / DI