

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 1/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Sumário

1. OBJETIVO	4
2. ABRANGÊNCIA.....	4
3. DEFINIÇÕES	4
4. DIRETRIZES	4
4.1. GESTÃO DE DISPOSITIVOS DE CLIENTE.....	4
4.1.1. DISPOSITIVOS DE CLIENTES SEGUROS	4
4.1.2. DISPOSITIVOS DE CLIENTES NÃO-SEGUROS	4
4.1.3. SMARTPHONES.....	5
4.1.4. CONEXÃO ÀS REDES DA SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA	5
4.1.5. UTILIZAÇÃO DE DISPOSITIVOS ADMINISTRADOS PELA SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA.....	5
4.1.6. CONFIGURAÇÃO DO DISPOSITIVO	6
4.1.7. PROTEÇÃO FÍSICA E AMBIENTAL.....	6
4.1.8. SOFTWARE.....	7
4.1.9. DESCARTE DE DISPOSITIVOS	7
4.1.10. EQUIPAMENTOS DE USUÁRIOS FINAIS	8
4.1.11. MANUTENÇÃO DOS DISPOSITIVOS.....	8
4.1.12. CRIPTOGRAFIA	8
4.2. UTILIZAÇÃO DOS SISTEMAS DE INFORMAÇÃO.....	9
4.2.1. INFORMAÇÕES CONFIDENCIAIS	9
4.2.2. USO PESSOAL DOS SISTEMAS DE INFORMAÇÃO.....	10
4.2.3. ATIVIDADES PROIBIDAS NOS SISTEMAS DE INFORMAÇÃO	10
4.2.4. MONITORAMENTO	11
4.2.5. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO.....	12
4.2.6. PROTEÇÃO DE REDE	12
4.2.7. CRIAÇÃO/CANCELAMENTO DE CONTAS E ATRIBUIÇÃO/REVOGAÇÃO DE PERMISSÕES	12
4.2.8. MUDANÇAS DE FUNÇÃO DO COLABORADOR.....	14
4.2.9. CANCELAMENTO/SUSPENSÃO DAS CONTAS	14
4.2.10. NORMAS PARA SENHAS DOS SISTEMAS DE INFORMAÇÃO.....	14
4.2.11. AUDITORIA DAS CONTAS	14
4.2.12. ACESSO REMOTO	15
4.2.13. E-MAIL.....	15
4.2.14. INTERNET.....	16

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 2/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.2.15.	MENSAGENS INSTANTÂNEAS.....	16
4.2.16.	SERVIÇOS DE E-MAIL DA INTERNET.....	16
4.2.17.	MÍDIAS DE ARMAZENAMENTO PORTÁTEIS.....	16
4.3.	GESTÃO PARA ACESSO REMOTO.....	16
4.3.1.	PADRÕES DE ACESSO REMOTO.....	16
4.3.2.	APROVAÇÃO.....	17
4.3.3.	AUTENTICAÇÃO.....	17
4.3.4.	CONTROLES DE ACESSO.....	17
4.3.5.	AMBIENTE DE TRABALHO REMOTO.....	18
4.4.	GESTÃO DE VULNERABILIDADE.....	18
4.4.1.	AUDITORIA DE AVALIAÇÃO DE VULNERABILIDADE.....	18
4.4.2.	AVALIAÇÕES DE VULNERABILIDADE NÃO-AUTORIZADAS.....	18
4.5.	GESTÃO DE MUDANÇAS.....	18
4.5.1.	PLANEJAMENTO DA MUDANÇA.....	19
4.5.2.	REGISTRO E CLASSIFICAÇÃO DAS MUDANÇAS EM SISTEMA DE SERVICE CENTER.....	19
4.5.3.	AUTORIZAÇÃO DA MUDANÇA PELO USUÁRIOS.....	19
4.5.4.	ANALISE DE VIABILIDADE DA MUDANÇA.....	19
4.5.5.	HOMOLOGAÇÃO EM AMBIENTE DE TESTE.....	20
4.5.6.	GESTÃO DE PATCH.....	20
4.5.7.	APROVAÇÃO DA GERÊNCIA DE TI.....	20
4.5.8.	EXECUÇÃO DAS MUDANÇAS.....	20
4.5.9.	REVERSÃO DA MUDANÇA.....	21
4.5.10.	ACEITE DO USUÁRIO.....	21
4.5.11.	DOCUMENTAÇÃO.....	21
4.5.12.	PLANOS DE CONTINUIDADE DOS NEGÓCIOS E DE RECUPERAÇÃO DE DESASTRES.....	21
4.6.	MONITORAMENTO DE SISTEMAS ELETRÔNICOS.....	21
4.6.1.	CRITÉRIOS DE MONITORIA.....	21
4.6.2.	PROCEDIMENTOS.....	22
4.7.	GESTÃO DE RECUPERAÇÃO DE DESASTRES.....	23
4.7.1.	ANÁLISE DO IMPACTO NOS NEGÓCIOS.....	23
4.7.2.	IDENTIFICAÇÃO DE SERVIÇOS CRÍTICOS.....	23
4.7.3.	INSTALAÇÕES DE PROCESSAMENTO ALTERNATIVAS.....	23
4.7.4.	BACKUP DE INFORMAÇÕES.....	24
4.7.5.	PROCEDIMENTOS DE RECUPERAÇÃO TÉCNICA.....	24
4.7.6.	EQUIPE DE RECUPERAÇÃO TÉCNICA.....	24
4.7.7.	DISPONIBILIDADE DE MATERIAL PARA RECUPERAÇÃO.....	24

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 3/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.7.8.	TESTE DO PLANO DE RECUPERAÇÃO	25
4.7.9.	MANUTENÇÃO DO PLANO DE RECUPERAÇÃO	25
4.7.10.	ALTERAÇÕES NAS NECESSIDADES DOS NEGÓCIOS	25
4.7.11.	CONTINUIDADE DOS NEGÓCIOS	25
4.8.	PROTEÇÃO AMBIENTAL E FÍSICA	26
4.8.1.	ÁREAS PROTEGIDAS	26
4.8.2.	PROTEÇÃO FÍSICA E AMBIENTAL DE ÁREAS PROTEGIDAS	26
4.8.3.	CABOS DE TELECOMUNICAÇÃO E DE ENERGIA	27
4.8.4.	PERDA OU ROUBO DE EQUIPAMENTOS	27
4.8.5.	MESA ORGANIZADA	27
4.8.6.	MATERIAIS PERIGOSOS	27
4.8.7.	EQUIPAMENTOS DE GRAVAÇÃO	27
4.8.8.	MOVIMENTAÇÃO DE EQUIPAMENTOS	27
4.8.9.	DESCARTE	27
4.8.10.	REPARO E MANUTENÇÃO	28
4.8.11.	ACESSO FÍSICO	28
4.8.12.	GERENCIAMENTO DE INCIDENTES	28
4.8.13.	BACKUP E ARMAZENAMENTO	28
4.8.14.	CERTIFICAÇÕES DE FORNECEDORES	28
4.8.15.	AUDITORIAS	28
5.	CONFORMIDADE	29
6.	ÍNDICE DE ANEXOS	29
	Anexo 1 - Definições utilizadas na Política Corporativa de TI	30
	Anexo 2 - Termo de Responsabilidade e Cautela de Equipamentos de TI	33
	Anexo 3 - Termo de Confidencialidade para Utilização de Sistemas de Informação	34
	Anexo 4 - Termo de Responsabilidade para Utilização de Contas com Privilégios	35

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 4/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

1. OBJETIVO

Estabelecer diretrizes, controles, responsabilidades e procedimentos para os processos da Tecnologia da Informação da Secretaria Municipal de Educação de Araruama.

2. ABRANGÊNCIA

Essa política se aplica a todos os componentes dos sistemas de informação da Secretaria Municipal de Educação de Araruama, incluindo, sem limitação, dispositivos-cliente (tais como equipamento móvel, desktops e notebooks), servidores, dispositivos de rede (como firewalls), programas de software e outros dispositivos de comunicação (tais como equipamentos de videoconferência).

3. DEFINIÇÕES

Todas as definições utilizadas nesse documento estão localizadas no [Anexo 1 - Definições utilizadas na Política Corporativa de TI](#).

4. DIRETRIZES

4.1. GESTÃO DE DISPOSITIVOS DE CLIENTE

O objetivo dessa política é garantir que os riscos associados ao uso de dispositivos-cliente sejam devidamente administrados. Esses riscos incluem:

- Exposição a códigos mal-intencionados;
- Softwares não-autorizados, tais como sniffers e ferramentas de hackers sendo utilizados nos sistemas de informação Secretaria Municipal de Educação de Araruama.

4.1.1. DISPOSITIVOS DE CLIENTES SEGUROS

Todos os dispositivos administrados pela Secretaria Municipal de Educação de Araruama são dispositivos de clientes seguros.

Os dispositivos seguros poderão ser fornecidos com acesso total às redes da Secretaria Municipal de Educação de Araruama.

Tal acesso poderá ser através de conexão com fio, sem fio ou remota, utilizando os mecanismos de acesso remoto autorizados pela Secretaria Municipal de Educação de Araruama.

4.1.2. DISPOSITIVOS DE CLIENTES NÃO-SEGUROS

Todos os dispositivos não-administrados pela Secretaria Municipal de Educação de Araruama são dispositivos de clientes não-seguros. Os dispositivos de cliente não-seguros não têm acesso total às redes da Secretaria Municipal de Educação de Araruama.

Os dispositivos de cliente não-seguros só têm acesso com ou sem fio às redes da Secretaria Municipal de Educação de Araruama nas seguintes hipóteses:

- A rede tiver a capacidade de distinguir os dispositivos não-administrados pela Secretaria Municipal de Educação de Araruama no momento da conexão;

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 5/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

- A rede puder restringir o acesso a uma área de quarentena da rede da Secretaria Municipal de Educação de Araruama;
- A área de quarentena deverá evitar:
 - Que códigos mal-intencionados sejam transmitidos ao resto da rede;
 - Acessos não-autorizados ao resto da rede;
 - Que aplicativos intrusivos ou não autorizados acessem o resto da rede.

Dispositivos de cliente não-seguros poderão ter acesso remoto a redes da Secretaria Municipal de Educação de Araruama utilizando mecanismos de acesso remoto autorizados pela Secretaria Municipal de Educação de Araruama. Os usuários de tais dispositivos deverão receber somente:

- Acesso a programas ou recursos seguros, específicos para cada usuário com base em suas necessidades e comerciais; e
- Acesso ao ambiente protegido da Secretaria Municipal de Educação de Araruama.

4.1.3. SMARTPHONES

Smartphones que não sejam administrados pela Secretaria Municipal de Educação de Araruama são dispositivos de cliente não-seguros.

A conexão desses dispositivos às redes da Secretaria Municipal de Educação de Araruama está sujeita aos requisitos do item **4.1.4. CONEXÃO ÀS REDES.**

4.1.4. CONEXÃO ÀS REDES DA SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA

Todos os dispositivos administrados pela Secretaria Municipal de Educação de Araruama são dispositivos cliente-seguro e poderão ser fornecidos com acesso total às redes da Secretaria Municipal de Educação de Araruama, dentro das restrições impostas pelas permissões existentes de acesso aos usuários.

Todos os dispositivos não administrados pela Secretaria Municipal de Educação de Araruama são dispositivos cliente-não-seguro e não terão acesso total às redes da Secretaria Municipal de Educação de Araruama. A conexão desses dispositivos à rede da Secretaria Municipal de Educação de Araruama deverá cumprir as exigências da Política para Dispositivos de Cliente Seguros. Qualquer exceção a isso deverá ser aprovada pela direção de Tecnologia e Operações.

Todos os equipamentos de clientes com conexão wireless ou a cabo, deverão ser aprovados pela área de TI antes de serem conectados à rede da Secretaria Municipal de Educação de Araruama. Isso inclui dispositivos que não sejam de propriedade da Secretaria Municipal de Educação de Araruama e a configuração dos mesmos.

4.1.5. UTILIZAÇÃO DE DISPOSITIVOS ADMINISTRADOS PELA SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA

Os dispositivos administrados pela Secretaria Municipal de Educação de Araruama são, em princípio, apenas para fins comerciais legítimos.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 6/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

O uso limitado para fins pessoais será permitido, desde que:

- Não viole qualquer condição do vínculo empregatício;
- Não utilize recursos de TI excessivamente, tais como largura de banda;
- Seja lícito;
- Não cause impacto no desempenho dos sistemas de informação da Secretaria Municipal de Educação de Araruama;
- Não cause impacto na realização dos trabalhos dos usuários ou em outros usuários;
- Não comprometa a segurança das informações e sistemas de informação;
- Não conflite com qualquer política, norma e orientação da Secretaria Municipal de Educação de Araruama;
- Não prejudique a imagem ou reputação da Secretaria Municipal de Educação de Araruama.

A Secretaria Municipal de Educação de Araruama não será responsável por qualquer perda ou inconveniência causada aos usuários em função de tal uso pessoal.

4.1.6. CONFIGURAÇÃO DO DISPOSITIVO

Os dispositivos administrados pela Secretaria Municipal de Educação de Araruama deverão estar de acordo com as configurações padrão para o dispositivo aprovadas pela área de TI.

Quando forem utilizados dispositivos não-administrados pela Secretaria Municipal de Educação de Araruama:

- A configuração padrão de segurança da Secretaria Municipal de Educação de Araruama exigida deverá estar instalada em todos os dispositivos;
- Qualquer software licenciado da Secretaria Municipal de Educação de Araruama instalado nos dispositivos deverá ser removido ao final do uso do dispositivo.
- Qualquer informação da Secretaria Municipal de Educação de Araruama armazenada nos dispositivos deverá ser completamente removida ao final do uso do dispositivo.
- Quando houver a necessidade de armazenamento de informação da Secretaria Municipal de Educação de Araruama nos dispositivos, a mesma deverá ser disponibilizada aos colaboradores pertinentes antes da remoção.
- Nenhum usuário ou administrador de sistema poderá alterar ou desabilitar as configurações de segurança nos dispositivos administrados pela Secretaria Municipal de Educação de Araruama.
- Alterações de software ou hardware nos dispositivos administrados pela Secretaria Municipal de Educação de Araruama somente poderão ser efetuadas com recursos autorizados da Tecnologia da Informação.

4.1.7. PROTEÇÃO FÍSICA E AMBIENTAL

Os usuários deverão manter suas mesas limpas e organizadas, sendo que todas as informações comerciais e confidenciais deverão ser guardadas com segurança, bem como documentos e mídias de armazenamento portáteis quando não estiverem sendo usadas, além dos documentos impressos.

Os usuários deverão garantir sempre a devida proteção física e do ambiente dos dispositivos-cliente esteja adequada o tempo todo.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 7/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Será necessária a autorização formal para remover os dispositivos administrados pela Secretaria Municipal de Educação de Araruama de suas dependências.

A autorização poderá ser concedida pela área de TI ou pelo Gerente da Área do usuário.

A perda ou roubo de qualquer hardware ou software de computador e de telefonia deverá ser comunicado a área de TI.

4.1.8. SOFTWARE

A área de TI deverá estabelecer e manter uma Lista de Tecnologias Implementáveis - DTL, que inclui o software que possa ser implementado nos dispositivos administrados pela Secretaria Municipal de Educação de Araruama.

Apenas os softwares autorizados incluídos na DTL poderão ser instalados nos dispositivos administrados pela Secretaria Municipal de Educação de Araruama.

Colaboradores e terceiros que necessitem de softwares não incluídos na DTL instalados nos dispositivos administrados pela Secretaria Municipal de Educação de Araruama deverão obter a aprovação da área de TI antes de sua instalação.

As situações a seguir estão proibidas para dispositivos administrados pela Secretaria Municipal de Educação de Araruama:

- Atropelar ou contornar qualquer sistema de segurança, ou instalar qualquer programa ou software que tenha esses efeitos;
- Copiar o software da Secretaria Municipal de Educação de Araruama para uso em dispositivos não-administrados pela Secretaria Municipal de Educação de Araruama;
- Copiar ou dar acesso ao software da Secretaria Municipal de Educação de Araruama para distribuição a contratados independentes, clientes ou terceiros;
- Modificar, revisar ou adaptar qualquer software da Secretaria Municipal de Educação de Araruama;
- Traduzir, aplicar engenharia reversa ou desmontar qualquer software residente na infraestrutura de Tecnologia da Informação da Secretaria Municipal de Educação de Araruama.
- Adquirir software diretamente.

Os equipamentos e softwares adquiridos diretamente pelos usuários finais deverão ser aprovados pela direção de Tecnologia da Informação antes de sua aquisição.

Todos os softwares em dispositivos administrados ou não pela Secretaria Municipal de Educação de Araruama deverão ser devidamente licenciados e de acordo com os contratos de licença.

4.1.9. DESCARTE DE DISPOSITIVOS

Os dispositivos que tenham que ser descartados deverão ter todas as informações completamente removidas pelo atual software de limpeza de dados. Os procedimentos referentes ao processo de aprovação para baixa de ativos deverão seguir os normativos em vigor.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 8/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.1.10. EQUIPAMENTOS DE USUÁRIOS FINAIS

Os equipamentos fornecidos pela área de TI aos usuários finais, tais como, computadores de mesa (desktop), computadores portáteis (laptop), aparelhos celulares, smartphones, monitores, placas de comunicação (GPRS), etc, devem possuir termo de responsabilidade assinado pelo usuário conforme *Anexo 2 – Termo de Responsabilidade e Cautela de Equipamentos de TI.*

Estes termos deverão ser revisados anualmente para constatar a guarda do equipamento pelo colaborador indicado no termo. A Gerência de TI deverá manter controle do fornecimento, troca e devolução dos equipamentos.

O usuário devolverá os equipamentos por ele utilizados ao final do seu contrato de trabalho e baixa do termo de responsabilidade no departamento Administrativo.

O usuário se responsabilizará pela guarda e posse do equipamento, respondendo perante a companhia no que diz respeito à má utilização ou qualquer dano causado ao mesmo, assumindo os encargos de fiel depositário, nos termos do artigo 627 e seguintes do Código Civil Brasileiro, na ocorrência de qualquer dos eventos acima ou arcar com os custos de eventuais consertos.

Em caso de roubo, furto, extravio e perda de bens portáteis, por exemplo, laptops ou aparelhos de celular, o usuário efetuará o registro do Boletim de Ocorrência numa delegacia policial e, de posse deste documento, contatar o departamento Administrativo para entregar cópia do mesmo.

4.1.11. MANUTENÇÃO DOS DISPOSITIVOS

Os usuários não deverão tentar reparar dispositivos administrados pela Secretaria Municipal de Educação de Araruama ou permitir que técnicos não-autorizados realizem qualquer suporte, reparo ou manutenção em dispositivos administrados pela Secretaria Municipal de Educação de Araruama.

Os usuários deverão contatar o centro de apoio ao usuário local, no caso a DITEI, quanto aos requisitos de suporte, reparo ou manutenção.

A manutenção dos dispositivos administrados pela Secretaria Municipal de Educação de Araruama somente poderá ser realizada com recursos autorizados pela DITEI.

4.1.12. CRIPTOGRAFIA

A área de TI deverá fornecer ou autorizar todas as soluções de criptografia.

O uso de qualquer forma de criptografia nos sistemas de informação da Secretaria Municipal de Educação de Araruama é proibido, a menos que autorizado especificamente pela área de TI.

Os usuários deverão garantir que todas as informações criptografadas da Secretaria Municipal de Educação de Araruama sejam disponibilizadas aos recursos apropriados da Secretaria Municipal de Educação de Araruama caso tenham que deixar a companhia ou mudar de cargo.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 9/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.2. UTILIZAÇÃO DOS SISTEMAS DE INFORMAÇÃO

Formalizar as responsabilidades dos usuários para proteger as informações e os sistemas de informação da Secretaria Municipal de Educação de Araruama, assim como as informações de terceiros hospedadas nos sistemas da Secretaria Municipal de Educação de Araruama de acordo com sua importância.

A política cobre as responsabilidades dos usuários nas seguintes áreas dos sistemas de informação da Secretaria Municipal de Educação de Araruama:

Gestão da Informação:

- Gestão de informações confidenciais;
- Propriedade de informações;
- Uso pessoal dos sistemas de informação da Secretaria Municipal de Educação de Araruama;
- Atividades proibidas;
- Monitoramento;

Gestão da Infraestrutura de Tecnologia da Informação:

- Proteção física e de ambiente;
- Equipamentos de clientes;
- Softwares;
- Acesso, contas e senhas de usuários;
- Proteção de rede;
- Recuperação de desastre;

Gestão de aplicações ou serviços específicos:

- Email;
- Internet;
- Comunicadores Instantâneos;
- Webmail;

4.2.1. INFORMAÇÕES CONFIDENCIAIS

Os usuários deverão garantir que compreendem a confidencialidade das informações administradas por eles e tratá-las de acordo. Isso se aplica às informações da Secretaria Municipal de Educação de Araruama e de terceiros.

Informações recebidas de terceiros deverão ser tratadas de acordo com qualquer norma ou exigência de gestão de informações que possam ter aplicabilidade a tais informações, como por exemplo, aquelas incluídas em acordos de sigilo ou de confidencialidade.

Nenhum conteúdo confidencial poderá ser armazenado em discos locais ou dispositivos móveis, a menos que possua segurança de proteção apropriada, como criptografia aprovada pela área de TI ou proteção por senha.

Os usuários serão responsáveis por fazer backup do conteúdo armazenado nos discos locais ou dispositivos móveis.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 10/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.2.2. USO PESSOAL DOS SISTEMAS DE INFORMAÇÃO

A Secretaria Municipal de Educação de Araruama não poderá garantir que o uso pessoal dos seus sistemas de informação, como o uso de comunicadores instantâneos, permanecerá privado. A Secretaria Municipal de Educação de Araruama não possui qualquer responsabilidade pela privacidade dessas informações.

A Secretaria Municipal de Educação de Araruama não aceitará nenhuma responsabilidade ou consequências por conta do uso pessoal dos sistemas de informação da Secretaria Municipal de Educação de Araruama.

Os sistemas de informação da Secretaria Municipal de Educação de Araruama são fundamentalmente destinados apenas ao uso comercial. Uso pessoal limitado é permitido, contanto que:

- Não viole nenhuma condição empregatícia;
- Não faça uso excessivo dos recursos de TI, como link de dados (internet);
- Seja lícito;
- Não afete o desempenho dos sistemas de informação da Secretaria Municipal de Educação de Araruama;
- Não afete o desempenho do trabalho dos usuários;
- Não comprometa a segurança das informações e dos sistemas;
- Não viole nenhuma política, norma e diretriz da Secretaria Municipal de Educação de Araruama;
- Não prejudique a imagem ou a reputação da Secretaria Municipal de Educação de Araruama;
- Não perturbe, intimide ou humilhe nenhuma pessoa em função de raça, sexo, religião, incapacidade e idade.

A Secretaria Municipal de Educação de Araruama não será responsável por qualquer prejuízo ou transtorno causado a usuários decorrente de tal uso pessoal.

Caso um usuário não esteja certo se um determinado uso pessoal dos sistemas SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA seja permitido ou não, esse uso deverá ser esclarecido junto à Gerencia da DITEI. A SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA se reserva o direito de restringir o uso pessoal de seus sistemas (como a internet) a fim de salvaguardar e proteger o ambiente de Tecnologia da Informação. Essas restrições poderão incluir limitação ao acesso de sites na internet, restrições de downloads na internet, ou limitação de horários para acesso à internet para uso pessoal.

4.2.3. ATIVIDADES PROIBIDAS NOS SISTEMAS DE INFORMAÇÃO

O uso dos sistemas de informação da Secretaria Municipal de Educação de Araruama, como internet ou e-mail, é proibido para os seguintes casos:

- Obter, armazenar, visualizar, distribuir ou exibir qualquer material pornográfico, obsceno ou semelhante;
- De forma a fazer discriminações injustas arbitrariamente a qualquer pessoa, como em função de raça, sexo, religião, incapacidade ou idade;
- De forma que possa ser razoavelmente esperada a perturbar, intimidar ou humilhar qualquer

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 11/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

- pessoa em função de raça, sexo, religião, incapacidade ou idade;
- Fazer propaganda ou realizar negócios pessoais.

O uso dos sistemas de informação da Secretaria Municipal de Educação de Araruama não deverá violar nenhuma lei ou regulamento aplicável.

Os usuários não deverão tentar acessar sistemas para os quais não tenham recebido direito de acesso, ou buscar falhas de segurança ou comprometer os sistemas.

Os usuários não poderão alterar nem desabilitar configurações de segurança, antivírus ou outros softwares de proteção ou monitoramento nos dispositivos gerenciados pela Secretaria Municipal de Educação de Araruama, a menos que possuam autorização da área de TI.

Os usuários não poderão desviar nem burlar nenhum sistema de segurança, ou instalar qualquer programa ou software que tenha esse objetivo.

Para proteger os seus sistemas, a Secretaria Municipal de Educação de Araruama se reserva o direito de retirar o acesso caso as exigências desta política não sejam observadas.

4.2.4. MONITORAMENTO

A Secretaria Municipal de Educação de Araruama monitorará o uso dos sistemas de informação:

- Caso haja suspeita de violação de alguma regra contida nesta política ou em outras políticas da Secretaria Municipal de Educação de Araruama;
- Caso haja suspeita de uso não autorizado;
- Caso haja suspeita de brecha contratual;
- Para prevenir ou detectar qualquer suspeita de crime ou descumprimento de qualquer legislação aplicável;
- Para cooperar com qualquer autoridade legal na detecção e prevenção de atividades ilegais ou qualquer atividade que possa constituir má conduta profissional;
- Para evitar ataques de códigos maliciosos;
- Para verificar o desempenho dos sistemas.

Quando necessário, a Gerência de TI da Secretaria Municipal de Educação de Araruama informará os funcionários da existência de sistemas de monitoramento e obterá o consentimento do funcionário conforme termo de confidencialidade.

Toda atividade de monitoramento será desempenhada de acordo com a legislação vigente.

A área de TI da Secretaria Municipal de Educação de Araruama se reserva o direito de acessar, monitorar, ler, filtrar, bloquear, excluir, usar e/ou tomar ações contra dados ou informações mantidos ou transmitidos através dos sistemas da Secretaria Municipal de Educação de Araruama.

Monitoramento não-invasivo será realizado por programas de software que monitoram e registram a atividade nos sistemas de informação da Secretaria Municipal de Educação de Araruama. Esse monitoramento inclui, entre outros:

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 12/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

- Uso da internet e extranet;
- Uso de e-mail;
- Criação, edição e exclusão de arquivos em pastas compartilhadas e pessoais na rede;
- Uso dos sistemas de informação da Secretaria Municipal de Educação de Araruama.

Monitoramento invasivo só será empregado caso:

- Haja motivo suficiente para justificar esse monitoramento;
- A área de TI autorize esse monitoramento. Caso considerem necessário, poderá ser envolvida uma empresa de Auditoria, conforme a Política de Monitoramento de Sistemas Eletrônicos.
- Caso acesso as informações eletrônicas de um usuário seja necessário por outro usuário na ausência daquele:
- Tal acesso só poderá ser fornecido mediante autorização da área de Compliance.
- O funcionário deverá ser notificado sobre o acesso.

A área de TI em conjunto com a área de Compliance da SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA avaliará periodicamente a conformidade dos usuários com esta política.

4.2.5. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Todos os incidentes de segurança deverão ser comunicados a gerência de TI.

4.2.6. PROTEÇÃO DE REDE

Redes wireless só poderão ser implantadas com a permissão prévia da área de TI.

Dispositivos de comunicação ou dispositivos de clientes que estejam conectados às redes da Secretaria Municipal de Educação de Araruama só poderão ser conectados às redes da Secretaria Municipal de Educação de Araruama com a permissão prévia da área de TI.

4.2.7. CRIAÇÃO/CANCELAMENTO DE CONTAS E ATRIBUIÇÃO/REVOGAÇÃO DE PERMISSÕES

O acesso a sistemas de informação da Secretaria Municipal de Educação de Araruama deve ser concedido exclusivamente a usuários identificados.

Os acessos podem ser concedidos a colaboradores, colaboradores temporários e terceiros (fornecedores).

Os usuários serão responsáveis por todas as atividades desempenhadas com suas contas de usuário pessoais.

A autorização deve ser concedida pela gerência do colaborador/temporário/terceiro de acordo com o cargo e funções a serem desempenhadas. Cabe a gerência o direito de revogar tal acesso, conforme as circunstâncias possam justificar. Em caso de concessão de acesso a terceiros, a gerência deverá justificar na solicitação o motivo e o prazo do acesso; Em casos de sistemas de informação específicos, o acesso deverá ser autorizado/revogado pelo responsável do sistema.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 13/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

O princípio do menor privilégio deverá ser aplicado a todo acesso concedido às informações e aos sistemas de informação da Secretaria Municipal de Educação de Araruama.

Os acordos de confidencialidade deverão ser estabelecidos entre as Unidades de Negócio da SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA e cada usuário conforme Anexo 3 – Termo de Confidencialidade para Utilização de Sistemas de Informação e Anexo 4 – Termo de Responsabilidade para Utilização de Contas com Privilégios.

As solicitações para cadastro/cancelamento/suspensão de usuários e/ou atribuição/revogação/alteração de permissões de acesso aos sistemas devem ser registrados em sistema adequado. Nos casos de cadastramento de usuários e atribuição/mudança de permissão nos sistemas deverá estar em anexo ao registro da solicitação a autorização formal assinada (digitalizada) ou uma cópia do e-mail identificando com clareza quem está autorizando.

Cada conta deverá ser atribuída a um único usuário, da mesma forma que cada usuário poderá ter um único acesso em cada sistema. O usuário não pode compartilhar sua conta e senha tampouco com outros colaboradores, temporários ou fornecedores. A conta deve ser criada de forma que o usuário possa ser identificado pelo nome/sobrenome. Em casos de homônimos, deverá ser identificada a melhor combinação possível.

A criação de contas genéricas deve ser evitada, mas quando indispensável deve ser justificada e atribuída a um usuário.

Contas padrão fornecidas com softwares de fornecedor deverão, quando possível, ser desabilitadas. As senhas padrão para essas contas deverão ser alteradas. Quando não for possível desabilitar, deverá ser atribuída para uso de um único colaborador, de forma que o mesmo possa ser responsabilizado pela conta.

Contas ou senhas de usuários não deverão ser codificadas nem armazenadas dentro de aplicativos.

Direitos de acesso concedidos a usuários deverão manter uma segregação de funções apropriada entre funções incompatíveis.

Contas criadas para terceiros ou pessoal temporário deverá ter data de validade limitada a data de validade do contrato ou no máximo 5 anos, após a qual todo o acesso será revogado.

As senhas deverão estar de acordo com as normas de senhas definidas nesta política.

As senhas deverão ser alteradas imediatamente caso se tornem de conhecimento de outras pessoas ou no caso de haver suspeita de que tenham sido divulgadas a outros.

Estações de trabalho abandonadas deverão ser bloqueadas, por exemplo, com o uso de proteção de tela com senha.

O mau uso de contas de usuário deverá ser comunicado ao setor de TI local.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 14/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.2.8. MUDANÇAS DE FUNÇÃO DO COLABORADOR

Caso haja mudança na natureza das funções de um usuário, seus direitos de acesso a sistemas de informação deverão ser atualizados de forma a corresponder corretamente à sua nova posição e responsabilidades.

4.2.9. CANCELAMENTO/SUSPENSÃO DAS CONTAS

Em caso de ausência do colaborador por períodos muito longos a gerencia deverá solicitar a suspensão da conta de acesso aos sistemas do colaborador.

Contas de usuário que não tenham sido usadas por 180 dias deverão ser desabilitadas, sendo que a reativação deverá ser solicitada como se fosse um novo acesso com aprovação do gestor.

Contas de usuários que tenham sido desabilitadas há 30 dias deverão ser excluídas permanentemente, exceto para aplicações que necessitem de auditoria, como por exemplo, sistemas financeiros.

Quando uma conta de usuário for excluída, os emails e dados associados à conta de usuário deverão ser retidos de acordo com as necessidades da gestão.

Todo acesso a sistemas de informação deverá ser cancelado na data de desligamento de um usuário.

4.2.10. NORMAS PARA SENHAS DOS SISTEMAS DE INFORMAÇÃO

Os sistemas de informação da Secretaria Municipal de Educação de Araruama devem suportar pelo menos 2 itens da relação abaixo:

- As senhas devem ser configuradas para expirar após um período máximo de 90 dias;
- Devem possuir pelo menos 8 caracteres;
- Devem conter 3 dos 5 critérios abaixo:
 - Caractere do alfabeto em letra maiúscula;
 - Caractere do alfabeto em letra minúscula;
 - Caractere especial (como @, \$, %);
 - Um dígito de 0 –9;
 - Caractere unicode (saída de teclado não padronizada, como ASCII, árabe, hebraico ou chinês).

Contas de usuários deverão ser bloqueadas após 10 (dez) tentativas inválidas de acesso a um sistema de informação. A conta deverá permanecer bloqueada até que seja habilitada pelo setor de TI.

A captura de senhas deverá ser em campos que não exibam os dígitos;

4.2.11. AUDITORIA DAS CONTAS

Os responsáveis funcionais pelos sistemas serão responsáveis por examinar periodicamente os

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 15/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

direitos de acesso concedidos a usuários e fazer quaisquer alterações necessárias.

A TI deverá garantir que seja possível detectar e identificar violações de segurança das informações. Entre as violações estão, por exemplo, tentativas de usuários de obter acesso a sistemas de informações não autorizados e mal uso de direitos de acesso com privilégios.

Todas as violações de segurança identificadas deverão ser investigadas.

Trilhas de auditoria de acesso a sistemas de informação críticos deverão ser feitas e mantidas por um período de tempo definido.

Não há necessidade de trilhas de auditoria de atividades de usuários sem privilégios, e poderão ser instituídas a critério da Gerência de TI.

A quantidade de processos estabelecidos para monitorar o uso de sistemas de informações deverá ser determinada pela Gerência de TI com base no risco relativo de cada sistema de informações.

As atividades empreendidas por contas com privilégios deverão ser monitoradas. Esse monitoramento incluirá:

- Trilhas de auditoria de todo acesso a sistemas de informação deverão ser feitas e mantidas por um período de tempo definido.
- Um processo para identificar exceções nessas trilhas de auditoria deverá ser estabelecido.

4.2.12. ACESSO REMOTO

Os dispositivos de autenticação usados para acesso remoto a sistemas de informação da Secretaria Municipal de Educação de Araruama deverão ser fornecidos pela TI.

4.2.13. E-MAIL

A Secretaria Municipal de Educação de Araruama se reserva ao direito de bloquear ou pôr em quarentena e-mails com anexo suspeitos de conter códigos maliciosos, que possam afetar os sistemas da empresa.

E-mails comerciais legítimos que forem bloqueados serão liberados mediante solicitação do usuário.

O envio de mensagens de e-mail simulando ser de outra pessoa (e-mails fictícios) é expressamente proibido.

O envio de e-mails não comerciais não solicitados (como correntes que incentivem os destinatários a encaminhar o e-mail a outros usuários) a contas de e-mail da Secretaria Municipal de Educação de Araruama ou externas é proibido.

Não é permitido que nenhum usuário configure os equipamentos eletrônicos da empresa (Desktop, Laptop e VMs) com os dados de suas contas de e-mail pessoal.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 16/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.2.14. INTERNET

Não serão permitidas conexões à internet que burlam os mecanismos de proteção dos sistemas da Secretaria Municipal de Educação de Araruama, a partir de desktop ou notebook já conectado a uma rede da Secretaria Municipal de Educação de Araruama.

Os usuários serão responsáveis por cumprir as leis de direito autoral com relação a qualquer upload ou download de material da internet.

4.2.15. MENSAGENS INSTANTÂNEAS

Os usuários somente poderão usar sistemas de mensagens instantâneas autorizados pela Gerência de TI enquanto estiverem conectados a redes da Secretaria Municipal de Educação de Araruama.

A Secretaria Municipal de Educação de Araruama se reserva o direito de bloquear o uso de sistemas de mensagens instantâneas caso seja necessário para proteger o ambiente de TI.

4.2.16. SERVIÇOS DE E-MAIL DA INTERNET

A Secretaria Municipal de Educação de Araruama não possui nenhum controle sobre os serviços de webmail e seu uso poderá burlar sistemas de proteção de antivírus, aumentando os riscos associados ao uso desses serviços.

A TI poderá bloquear sites de webmail pessoais caso considere importante para garantir a disponibilidade e segurança dos sistemas de informação.

4.2.17. MÍDIAS DE ARMAZENAMENTO PORTÁTEIS

Mídias de armazenamento portáteis somente poderão ser conectadas aos sistemas da Secretaria Municipal de Educação de Araruama se o usuário tiver se certificado de que elas estejam livres de códigos maliciosos.

4.3. GESTÃO PARA ACESSO REMOTO

Garantir que os riscos associados a colaboradores e terceiros que acessem remotamente os sistemas de informação da Secretaria Municipal de Educação de Araruama sejam geridos adequadamente. Esses riscos incluem:

- Acesso remoto aos sistemas de informação das redes Secretaria Municipal de Educação de Araruama por pessoas não autorizadas;
- Uso de equipamentos que não sejam corretamente protegidos contra códigos nocivos; e
- Usuários que tenham acesso aos sistemas de informação sem estarem autorizados.

4.3.1. PADRÕES DE ACESSO REMOTO

Serviços de Infraestrutura Global definirão os padrões seguros de acesso remoto e arquitetônicos

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 17/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

exigidos para acessar os sistemas de informações remotamente.

4.3.2. APROVAÇÃO

Solicitações de acesso remoto a sistemas da Secretaria Municipal de Educação de Araruama deverão ser aprovadas pela Gerência direta da unidade de negócios e pela Gerência de TI.

Todos os terceiros cujo acesso remoto seja aprovado, deverão assinar um acordo de sigilo e confidencialidade com a Secretaria Municipal de Educação de Araruama antes de receberem as credenciais de acesso. Caberá à Área de TI em parceria com Recursos Humanos, estabelecer um cronograma para a entrega dos respectivos acordos de confidencialidade a todos os usuários com acesso remoto anterior à publicação desta Política.

4.3.3. AUTENTICAÇÃO

Usuários de acesso remoto deverão usar um dispositivo de autenticação de dois fatores além de suas credenciais de rede de acesso remoto aos sistemas de informação da Secretaria Municipal de Educação de Araruama.

Os dispositivos de autenticação de dois fatores serão fornecidos pela Secretaria Municipal de Educação de Araruama.

Os usuários de acesso remoto são responsáveis pela custódia de seus dispositivos de autenticação de dois fatores.

A área de TI poderá permitir acesso a portais considerados seguros sem a necessidade de autenticação de dois fatores, desde que este portal ou interface esteja baseado em protocolo criptografado (HTTPS) e esteja em ambiente protegido ou zona desmilitarizada (DMZ), além de permitir acesso a aplicativos baseados em exigências comerciais.

4.3.4. CONTROLES DE ACESSO

Os usuários de dispositivos geridos pelas redes Secretaria Municipal de Educação de Araruama poderão ter acesso total aos sistemas de informação das redes da Secretaria Municipal de Educação de Araruama, em conformidade com seus níveis atuais de autorização.

Os dispositivos geridos pela Secretaria Municipal de Educação de Araruama deverão possuir software padrão de acesso remoto instalado, e incluir, no mínimo, um software adequado de proteção contra código nocivo.

Os usuários de dispositivos não geridos pela Secretaria Municipal de Educação de Araruama serão guarnecidos com acesso a uma interface gerida pela Secretaria Municipal de Educação de Araruama. Isso irá permitir:

- Acesso seguro de aplicação, específico para cada usuário, com base em exigências comerciais; e
- Acesso ao ambiente protegido da Secretaria Municipal de Educação de Araruama.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 18/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.3.5. AMBIENTE DE TRABALHO REMOTO

Quando operar em um ambiente de trabalho fora do escritório, as condições ambientais e de segurança deverão ser de padrão apropriado.

4.4. GESTÃO DE VULNERABILIDADE

A análise de vulnerabilidades deve ser realizada sistematicamente nas interações com sistemas de informação e demais dispositivos. Ao identificar uma vulnerabilidade, o colaborador da gerencia de TI de abrir um Ticket no sistema de Service Center classificado como incidente.

Deverá ser avaliado o grau da vulnerabilidade, levando em consideração:

- O impacto potencial de tal vulnerabilidade no ambiente;
- O grau de importância dos componentes do sistema de informação que possam ser afetados pela vulnerabilidade.

Baseado no grau de cada vulnerabilidade, as ações corretivas (tais como a implementação de um patch de software ou trabalho manual) e tempo de resposta deverão ser estabelecidos.

4.4.1. AUDITORIA DE AVALIAÇÃO DE VULNERABILIDADE

A área de TI deve garantir a realização de auditorias de avaliação de vulnerabilidade em dispositivos essenciais e sistemas críticos com regularidade, pelo menos uma vez por ano.

Todos os novos componentes de sistemas de informação devem ser examinados quanto a vulnerabilidades antes de utilizados na produção.

Em caso de surgimento de ameaça crítica, todos os componentes de rede e dispositivos de cliente devem ser examinados imediatamente para se definir seus status de vulnerabilidade.

Avaliações de vulnerabilidade independentes em dispositivos essenciais devem ser feitas por terceiros pelo menos uma vez por ano.

4.4.2. AVALIAÇÕES DE VULNERABILIDADE NÃO-AUTORIZADAS

Qualquer atividade de avaliação de vulnerabilidade ou uso de ferramentas para realizar avaliações de vulnerabilidade devem ser autorizadas pela área de TI.

4.5. GESTÃO DE MUDANÇAS

Para suportar seus processos de negócio, a Secretaria Municipal de Educação de Araruama conta com uma robusta infraestrutura de TI e diversos sistemas de informação que sofrem mudanças provocadas por alterações do negócio, evolução tecnológica ou atualizações legais. A política de gestão de mudanças estabelece definições que devem ser aplicadas nas mudanças de itens de

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 19/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

configuração de forma a garantir que não sejam afetadas a disponibilidade, confidencialidade e integridade das informações.

A Gerência de TI deve implementar e manter um processo formal de gerenciamento de mudanças de forma que todas as mudanças em infraestrutura e/ou sistemas de informação sejam registradas e possam ser rastreadas.

O processo de gerenciamento de mudanças deve compreender minimamente as seguintes atividades:

4.5.1. PLANEJAMENTO DA MUDANÇA

As mudanças em infraestrutura e/ou sistemas de informação devem ser endereçadas a colaboradores da Gerencia de TI para análise previa em relação a sua viabilidade técnica e financeira.

Havendo entendimento que a mudança deve ser registrada, o especialista deve elaborar documento de Requisição de Mudanças – RFC com informações relevantes, tais como a descrição da mudança, justificativa, análise de risco, cadernos de teste e plano de rollback. Pode, opcionalmente, incluir outras informações na Requisição de serviços que venham a trazer entendimento das tarefas que serão realizadas.

4.5.2. REGISTRO E CLASSIFICAÇÃO DAS MUDANÇAS EM SISTEMA DE SERVICE CENTER

A Secretaria Municipal de Educação de Araruama deverá disponibilizar um sistema de Service Center para que sejam registradas as demandas de mudanças na infraestrutura e/ou sistemas de informação. Por padrão tickets de mudanças devem ser abertos por integrantes da área de TI. Deve ser identificado minimamente o solicitante, IC e justificativa da mudança, e deve ser feita uma classificação de prioridade, considerando minimamente se a mudança é planejada ou não planejada (emergenciais).

Devem ser anexadas ao ticket da mudança todas as informações eletrônicas disponíveis.

4.5.3. AUTORIZAÇÃO DA MUDANÇA PELO USUÁRIOS

Todas as mudanças deverão ser aprovadas formalmente (por e-mail, formulário ou aceite em sistema) por usuários chaves dos sistemas afetados e seus respectivos coordenadores.

4.5.4. ANÁLISE DE VIABILIDADE DA MUDANÇA

As mudanças planejadas deverão ser analisadas em comitê de mudanças com base nas informações registradas na Requisição de Mudanças no sistema de Service Center. Uma vez aprovada a mudança deverá ser agendada para uma data no calendário anual de mudanças. As deliberações do comitê deverão ser registradas em ata que deverá ser assinada pelos integrantes do comitê e digitalizada para arquivo. A ata do comitê de mudanças deve ser enviada antes da janela de mudanças aos usuários afetados e a Gerencia de TI;

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 20/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.5.5. HOMOLOGAÇÃO EM AMBIENTE DE TESTE

Visando evitar afetar os sistemas de informações da Secretaria Municipal de Educação de Araruama, as mudanças deverão ser testadas e verificadas em um ambiente de teste separado antes de serem aplicadas no ambiente de produção.

Cada mudança deverá ser submetida a uma bateria de testes previamente acordada com o fornecedor e com o usuário chave do sistema.

Os ambientes de teste deverão corresponder à configuração em vigor dos ambientes de produção, incluindo hardware, sistemas operacionais, softwares de sistemas e softwares aplicativos nesses ambientes.

4.5.6. GESTÃO DE PATCH

A gestão de patches tem que considerar as seguintes atividades:

- Avaliação do impacto comercial da implementação ou não de patches;
- A obtenção de patches de software e firmware à medida que forem disponibilizados pelos vendedores;
- Decisão da direção de Tecnologia da Informação quanto à aplicação ou não dos patches;
- Ambiente de teste dentro do qual todos os patches possam ser testados antes de implementados no ambiente de produção;
- Implementação dos patches de acordo com os requisitos da Política de Controle de Mudanças do Grupo;
- Capacidade de monitorar a eficácia do processo de gestão de patch, por exemplo, a capacidade de rastrear o histórico do patch, o tempo decorrido entre a detecção da vulnerabilidade até a apresentação do patch como medida de eficácia e vulnerabilidades reincidentes em sistemas previamente remediados com patch.
- Apenas as pessoas autorizadas pelo Gerente de TI podem instalar os patches.
- Quando não houver patches disponíveis pelos fabricantes, qualquer implementação de outras soluções ou paliativos para as vulnerabilidades deverá estar de acordo com a Política de Controle de Mudanças.

4.5.7. APROVAÇÃO DA GERÊNCIA DE TI

Todas as mudanças (planejadas e não planejadas) deverão ser aprovadas formalmente pelo Gerente de TI (por e-mail, formulário ou aceite em sistema).

4.5.8. EXECUÇÃO DAS MUDANÇAS

As mudanças deverão ser executadas por colaboradores da área de TI ou fornecedores (desde que devidamente identificado) seguindo as instruções contidas na Requisição de Serviço cadastrada no sistema de Service Center e seus anexos. As mudanças poderão ser empreendidas de forma local ou remota. Em caso de mudanças executadas por fornecedores, deverá haver um integrante da Gerência de TI acompanhando.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 21/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.5.9. REVERSÃO DA MUDANÇA

Em caso de mudanças mal sucedidas deverá ser executado o plano de rollback de forma a resgatar o funcionamento do serviço de TI nas condições anteriores a mudança.

4.5.10. ACEITE DO USUÁRIO

As mudanças realizadas com sucesso deverão ser testadas em ambiente de produção pelos respectivos usuários-chave dos sistemas. Os usuários deverão dar aceite formal (por e-mail, formulário ou aceite em sistema) sobre a efetividade da mudança e conformidade do funcionamento do sistema ou serviço de TI.

4.5.11. DOCUMENTAÇÃO

A documentação dos sistemas de informação deverá ser atualizada de acordo com cada mudança, e a documentação antiga arquivada ou descartada, conforme a necessidade. Nessa documentação deverão estar inclusos procedimentos de sistema, de usuário e a documentação de continuidade dos negócios.

As mudanças deverão ser documentadas adequadamente, de forma a manter o controle apropriado de versão dos sistemas de informação.

4.5.12. PLANOS DE CONTINUIDADE DOS NEGÓCIOS E DE RECUPERAÇÃO DE DESASTRES

Planos de continuidade dos negócios e de recuperação de desastres deverão ser atualizados com as mudanças relevantes.

4.6. MONITORAMENTO DE SISTEMAS ELETRÔNICOS

Estabelecer as circunstâncias e condições sob as quais o monitoramento das atividades dos sistemas de informação da Secretaria Municipal de Educação de Araruama podem ser realizadas.

4.6.1. CRITÉRIOS DE MONITORIA

Os sistemas de informação da Secretaria Municipal de Educação de Araruama viabilizam os negócios de forma essencial, e todos os esforços deverão ser empregados para garantir seu uso eficaz e efetivo nos negócios.

A Secretaria Municipal de Educação de Araruama irá monitorar o uso do sistema de informações:

- Se houver suspeita de violação de alguma norma contida nessa política ou outras políticas do grupo;
- Se houver suspeita de uso não autorizado;
- Se houver suspeita de violação de dispositivo contratual;
- Visando evitar ou detectar qualquer suspeita de crime ou crime ocorrido, ou qualquer violação à legislação aplicável;

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 22/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

- Visando cooperar com as autoridades competentes em detectar e evitar qualquer atividade ilegal ou que possa constituir falta profissional;
- Para evitar ataques de códigos mal-intencionados; ou
- Para monitorar o desempenho do sistema.

Embora o monitoramento seja feito para proteger os interesses comerciais da SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA, algumas proteções específicas a usuários encontram-se definidas nessa política.

4.6.2. PROCEDIMENTOS

Toda a atividade de monitoramento deverá ser de acordo com a legislação pertinente.

A área de TI da Secretaria Municipal de Educação de Araruama se reserva o direito de acessar, monitorar, ler, filtrar, bloquear, utilizar e/ou atuar em relação a dados ou informações detidas ou transmitidas pelos sistemas de informação da Secretaria Municipal de Educação de Araruama, sujeito às exigências da legislação aplicável.

O monitoramento não-intrusivo será realizado rotineiramente pela área de Tecnologia da Informação, utilizando mecanismos automatizados, a fim de garantir o uso eficaz dos sistemas de informação da Secretaria Municipal de Educação de Araruama e monitorar o atendimento, pelos usuários, às políticas e normas do Grupo.

O monitoramento não-intrusivo será realizado por programa de software que monitora e registra as atividades dos sistemas de informação da Secretaria Municipal de Educação de Araruama. Esse monitoramento inclui, sem limitação:

- Internet;
- E-mail;
- Criação, edição e exclusão de arquivos nas pastas pessoais e compartilhadas na rede;
- Utilização dos sistemas de informação da Secretaria Municipal de Educação de Araruama. As diversas áreas da Secretaria Municipal de Educação de Araruama poderão designar gerentes responsáveis pela revisão de pedidos de interceptação intrusiva e monitoramento. Essa responsabilidade incluirá:
 - Determinar se há fundamentos suficientes para sustentar a interceptação ou monitoramento proposto;
 - Autorizar, autorizar com restrições ou proibir tal interceptação ou monitoramento proposto;
 - Autorizar interceptação ou monitoramento apenas por um determinado período;
 - Definir quem poderá realizar tal interceptação ou monitoramento;
 - Definir quem poderá realizar tal interceptação ou monitoramento; A interceptação ou monitoramento deve ser conduzido com respeito ao princípio da dignidade, privacidade e igualdade em relação às pessoas sujeitas à interceptação ou monitoramento. Os dados obtidos durante a interceptação ou monitoramento:
 - Deverão ser coletados e guardados de forma segura a fim de evitar seu uso, cópia ou divulgação não autorizada;
 - Somente poderão ser utilizados para fins jurídicos e legítimos, inclusive como meio de prova em processos disciplinares ou judiciais;

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 23/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

- Deverão ser destruídos assim que possível, caso não sejam relevantes ou aplicáveis aos motivos pelos quais a interceptação ou monitoramento tenha sido autorizado;
- Deverão ser destruídos após um período definido de tempo;
- Caso sejam futuramente necessários como prova, deverão ser guardados de forma segura para garantir que a integridade das informações não seja comprometida. Em caso de ausência do usuário, havendo necessidade de acesso a informações eletrônicas de um usuário por outro;
- Caso o empregado não esteja disponível, a aprovação deverá ser obtida de acordo com o processo de obtenção de permissão para interceptação ou monitoramento intrusivo;
- O empregado deverá ser informado sobre tal acesso.

Os usuários não deverão desenvolver, baixar, instalar ou utilizar qualquer ferramenta, dispositivo ou programa que frustre a interceptação ou monitoramento dos sistemas de informação da Secretaria Municipal de Educação de Araruama. As exigências dessa política deverão ser comunicadas a todos os usuários.

4.7. GESTÃO DE RECUPERAÇÃO DE DESASTRES

Visa assegurar a disponibilidade contínua das informações e dos sistemas de informação da Secretaria Municipal de Educação de Araruama.

Um plano para recuperação de serviços de tecnologia da informação, documentado e testado, proporciona uma resposta imediata e organizada para situações de desastre e reduz o risco de impactos significativos de natureza financeira e jurídica ou na reputação da empresa.

4.7.1. ANÁLISE DO IMPACTO NOS NEGÓCIOS

Uma análise do impacto nos negócios deverá ser conduzida para determinar o impacto resultante da indisponibilidade do sistema/serviço, o tempo que os negócios poderão se manter sem o sistema/serviço e períodos críticos ao longo do ano.

4.7.2. IDENTIFICAÇÃO DE SERVIÇOS CRÍTICOS

Os serviços críticos prestados pela TI ou terceiros deverão ser identificados bem como o seu impacto nos negócios e os prazos para recuperação calculados.

Outras dependências como hardware ou outros sistemas específicos, deverão ser identificadas para cada serviço crítico.

Estratégias para recuperação de dados e para recuperação de desastres deverão ser estabelecidas para esses serviços.

4.7.3. INSTALAÇÕES DE PROCESSAMENTO ALTERNATIVAS

Quando as estratégias para recuperação de desastres exigirem a provisão de instalações de processamento alternativas:

- Assegurar que a instalação alternativa seja convenientemente distante, de forma que um incidente

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 24/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

no local primário não afete o local alternativo;

- Assegurar que a instalação alternativa use serviços de infraestrutura diferentes, como de água e energia e que haja infraestrutura de telecomunicação adequada;
- Deverá ser providenciado que os usuários finais sejam acomodados, de acordo com as necessidades para a continuidade dos negócios;
- A capacidade de se recuperar adequadamente de um desastre no local alternativo deverá ser testada pelo menos uma vez por ano;
- As políticas da TI da Secretaria Municipal de Educação de Araruama deverão ser cumpridas nas instalações alternativas;
- Quando o uso ou teste da instalação alternativa estiver concluído, todas as informações da Secretaria Municipal de Educação de Araruama deverão ser totalmente removidas da instalação, com o uso de uma ferramenta aprovada pela TI.

4.7.4. BACKUP DE INFORMAÇÕES

Diariamente deve ser feita uma cópia integral de cada banco de dados, utilizando, se possível, recursos de backup online disponíveis nas ferramentas de SGBD, independentemente se o servidor de arquivos encontra-se instalado em datacenter próprio ou de terceiros.

4.7.5. PROCEDIMENTOS DE RECUPERAÇÃO TÉCNICA

Os procedimentos técnicos de recuperação deverão incluir informações suficientes para permitir que pessoal devidamente qualificado, não familiarizado com o local, os servidores ou sistemas, sejam capazes de efetuar a recuperação.

Os procedimentos devem incluir:

- Informações de configuração de servidor, como endereços de rede, partições e nomes de servidor;
- Sistema operacional e outras versões de software e níveis de patch necessários;
- Localização de bancos de dados, arquivos de log e compartilhamentos de rede;
- Procedimentos de instalação para todos os softwares;
- Plano geral de gerenciamento de recuperação para rastrear o progresso da recuperação;
- Um exame após o desastre para analisar a causa raiz do desastre, a causa raiz de qualquer falha no processo de recuperação e no desempenho geral de recuperação.

4.7.6. EQUIPE DE RECUPERAÇÃO TÉCNICA

Equipes de recuperação técnica deverão ser identificadas e documentadas, com as seguintes informações para cada equipe:

- As funções e responsabilidades da equipe;
- O líder da equipe;
- Os nomes e informações de contato completas para cada membro da equipe;
- Um substituto para membro da equipe.

4.7.7. DISPONIBILIDADE DE MATERIAL PARA RECUPERAÇÃO

Os seguintes itens deverão ser armazenados com segurança fora do local, onde possam ser acessados sem que seja necessário acessar o centro de dados afetado:

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 25/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

- Plano de recuperação.
- Acesso às mídias rotuladas como backup.
- Mídias de instalação de softwares.
- Códigos de licença e seriais para as mídias de instalação de softwares. Esses itens devem ser mantidos sempre atualizados.

4.7.8. TESTE DO PLANO DE RECUPERAÇÃO

O plano de recuperação deverá ser testado anualmente, ou após cada alteração de grande proporção ao ambiente, como atualização de hardware, consolidação de servidor ou alterações de aplicativos de grandes proporções.

O teste deverá ser desempenhado por pessoal devidamente qualificado, não familiarizado com a infraestrutura e os sistemas.

Os resultados de cada teste deverão ser analisados a fim de se corrigir quaisquer problemas identificados e avaliar se há necessidade de alterações aos processos de recuperação.

4.7.9. MANUTENÇÃO DO PLANO DE RECUPERAÇÃO

Os procedimentos de controle de alterações deverão incluir a avaliação de cada solicitação de alteração para determinar o impacto no plano de recuperação e incluir uma fase de acompanhamento para assegurar que o plano seja atualizado antes da alteração ser considerada como concluída.

O plano deverá ser revisto a cada 06 (seis) meses para assegurar que equipes de recuperação, arranjos para transporte e acomodação estejam em dia.

4.7.10. ALTERAÇÕES NAS NECESSIDADES DOS NEGÓCIOS

O plano de recuperação de TI deverá ser reavaliado, pelo menos, uma vez ao ano para determinar se ele continua atendendo às necessidades dos negócios.

Alterações nos negócios que possam afetar a adequabilidade do plano de recuperação deverão ser incorporadas nesta avaliação.

4.7.11. CONTINUIDADE DOS NEGÓCIOS

Os planos de recuperação de desastres de TI deverão ser integrados aos planos gerais de continuidade dos negócios.

Deverá haver um plano de comunicação para coordenar os planos de recuperação de desastres de TI com os estabelecimentos comerciais na eventualidade de um desastre.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 26/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

4.8. PROTEÇÃO AMBIENTAL E FÍSICA

Garantir que riscos físicos e do ambiente enfrentados pelos sistemas de informações da Secretaria Municipal de Educação de Araruama sejam administrados de forma apropriada.

Entre esses riscos estão:

- Acesso não autorizado a sistemas de informações;
- Risco de perda financeira;
- Riscos ambientais, como danos causados por fogo e água; e
- Roubo de equipamentos.

4.8.1. ÁREAS PROTEGIDAS

Instalações que alojem vários servidores críticos, dispositivos de comunicação, dispositivos de rede e cabos são classificadas como áreas protegidas.

A Gerência de TI deverá avaliar as instalações em que os sistemas de informações da Secretaria Municipal de Educação de Araruama ficam alojados e determinar:

- Se as instalações se qualificam como áreas protegidas ou não; e
- O quanto de proteção deve ser aplicado na área protegida.

4.8.2. PROTEÇÃO FÍSICA E AMBIENTAL DE ÁREAS PROTEGIDAS

As seguintes medidas de proteção física e ambiental deverão ser aplicadas às áreas protegidas:

- Proteção adequada por meio de sistemas de controle de acesso físico.
- Pontos de entrada e saída (por exemplo, portas e janelas) devidamente protegidos.
- Demarcação como áreas de "acesso restrito".
- Perímetros a serem construídos de forma a evitar fácil penetração ou acesso, como, por exemplo, não localizados em paredes externas de um prédio, sem janelas e proteção no piso e teto.
- Equipamentos de monitoramento visual para identificar pessoas que ingressem na área.
- Proteção para fornecimento de energia ininterrupto e gerador de backup, quando necessário para garantir a continuidade dos sistemas do negócio.
- Sistemas de detecção e prevenção contra incêndio que emitam alertas automaticamente para as pessoas apropriadas em caso de início de incêndio, que funcionem de acordo com processos definidos.
- Conformidade com a política de segurança da Secretaria Municipal de Educação de Araruama com regulamentos e legislações pertinentes de saúde e segurança, incluindo saídas de incêndio demarcadas e acessíveis.
- Sistemas de ar condicionado que operem continuamente, projetados para manter as instalações de acordo com as especificações recomendadas de temperatura e umidade dos fabricantes de equipamentos de TI.
- Monitoramento de temperatura, umidade, energia e limpeza para detectar problemas em potencial com equipamentos de ar condicionado e fontes de energia.
- Iluminação de emergência ativada em caso de queda de energia.
- Proibido comer, beber ou fumar.
- Manter limpo e livre de contaminação desnecessária.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 27/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

- Um programa periódico de limpeza especializada, cuja frequência deve ser adequada ao ambiente, que inclua limpeza embaixo do piso e em cima do teto quando houver piso elevado ou teto falso.
- Monitoramento das atividades de terceiros ou de prestadores de serviços (como faxineiros, por exemplo).
- Inspeção e testes periódicos em equipamentos de detecção e monitoramento de acordo com as especificações dos fabricantes.
- Procedimentos para autorizar revistas e revogar acesso físico.
- Controle apropriado de áreas de entrega e carregamento.
- Dispositivos devem ser claramente rotulados, sem fornecer detalhes do serviço prestado por eles.
- Proteção contra incêndio.

4.8.3. CABOS DE TELECOMUNICAÇÃO E DE ENERGIA

Os cabos de telecomunicação e de energia deverão ser protegidos contra interceptação e danos. Cabos de energia deverão ser separados dos cabos de comunicação para evitar interferência.

4.8.4. PERDA OU ROUBO DE EQUIPAMENTOS

A perda ou roubo de qualquer hardware ou software de computador e de telefonia deverá ser comunicado a área de TI.

4.8.5. MESA ORGANIZADA

Uma política de “mesa organizada” deverá ser adotada, o que inclui guardar em segurança informações comerciais confidenciais, documentos e mídias portáteis de armazenamento quando não estiverem sendo usados.

4.8.6. MATERIAIS PERIGOSOS

O armazenamento de materiais perigosos ou combustíveis perto ou dentro de áreas protegidas é proibido.

4.8.7. EQUIPAMENTOS DE GRAVAÇÃO

Nenhum gravador de vídeo ou áudio, máquina fotográfica ou outro tipo de gravador poderá ser levado para dentro de áreas protegidas sem a aprovação prévia da Gerência de TI.

4.8.8. MOVIMENTAÇÃO DE EQUIPAMENTOS

A Gerência de TI deverá assegurar que processos estejam implantados para o controle adequado da movimentação de equipamentos para dentro e fora das áreas protegidas.

Toda movimentação de equipamentos de TI para dentro e fora de áreas protegidas deverá ser feita exclusivamente pela equipe de TI.

4.8.9. DESCARTE

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 28/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2024				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Todas as informações de dispositivos a serem descartados deverão ser totalmente removidas rodando o software de limpeza de dados aprovado pela TI ou por meio da devida destruição dos componentes de armazenamento de informações.

4.8.10.REPARO E MANUTENÇÃO

O reparo e a manutenção de equipamentos deverão ser efetuados de acordo com as recomendações dos fornecedores.

Somente pessoas autorizadas pela área de TI poderão efetuar reparo e manutenção de equipamentos.

Acordos de confidencialidade deverão ser assinados com prestadores de serviço que efetuem reparo e manutenção nos equipamentos.

Atividades de reparo e manutenção realizadas por terceiros ou prestadores de serviços (como técnicos) em áreas protegidas serão monitoradas pela área de TI.

4.8.11.ACESSO FÍSICO

O acesso físico a áreas protegidas será limitado a pessoas autorizadas somente, por meio de mecanismos apropriados de controle de acesso.

Todo acesso físico a áreas protegidas deverá ser registrado e periodicamente revisado.

4.8.12.GERENCIAMENTO DE INCIDENTES

Em caso de incidentes em áreas protegidas, um exame deverá ser realizado para determinar a causa raiz do incidente e as ações a serem tomadas para evitar a reincidência.

Incidentes deverão ser periodicamente examinados a fim de garantir que os processos existentes sejam apropriados ao ambiente.

4.8.13.BACKUP E ARMAZENAMENTO

Fitas de backup ou suas cópias devem ser armazenadas com segurança fora das instalações para garantir sua disponibilidade em caso de desastres.

4.8.14.CERTIFICAÇÕES DE FORNECEDORES

Nos casos que a Secretaria Municipal de Educação de Araruama contratar serviços de Datacenters ou aplicações que são executadas na nuvem (Cloud Computing), o fornecedor deverá fornecer anualmente certificados que assegurem que a infraestrutura está conforme com as declarações e requerimentos desta política, sendo um dos certificados exigidos o ISAE3402.

4.8.15.AUDITORIAS

A Gerência de TI deverá garantir que auditorias sejam realizadas anualmente nas áreas protegidas

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 29/36	Data para Revalidação: 01/01/2025
Título: Normas e regras relacionadas a TI					
Descrição da Revisão: Revisão da Política Corporativa de TI Emissão Inicial: 01/01/2024				Palavra(s) Chave: Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

para assegurar a conformidade com esta política.

5. CONFORMIDADE

A conformidade com esta política é obrigatória. Os funcionários que violarem essa política poderão ser expressamente advertidos ou suspensos disciplinarmente e, dependendo da gravidade da violação, poderão ser demitidos e vir a responder processo judicial, sobretudo se o mau uso dos sistemas vier a causar prejuízos à empresa ou à sua imagem. Violações a esta política por terceiros poderão resultar no cancelamento do acesso às informações e aos sistemas de informação da Secretaria Municipal de Educação de Araruama, no término do vínculo e em processo judicial.

Quaisquer exceções às exigências desta política deverão ser autorizadas pelo CEO da SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA ou seu representante nomeado.

6. ÍNDICE DE ANEXOS

Anexo 1 - Definições utilizadas na Política Corporativa de TI

Anexo 2 - Termo de Responsabilidade e Cautela de Equipamentos de TI

Anexo 3 - Termo de Confidencialidade para Utilização de Sistemas de Informação

Anexo 4 - Termo de Responsabilidade para Utilização de Contas com Privilégios

CIRCULAÇÃO	
<input checked="" type="checkbox"/> Geral	<input type="checkbox"/> Restrita: Especificar:
Garantir a ciência por todos os colaboradores da empresa. Incluir esta ciência no processo de admissão.	

HISTÓRICO DE REVISÕES			
Data	Revisão	Elaboração	Descrição
01/10/2023	0	Clébio Silva	Criação do documento
01/03/2024	1	Clébio Silva	Revisão ordinária da norma

Elaboração	Revisão	Aprovação
Nome: Clébio José Reis da Silva	Nome: Daniel Almarante / Bruno Maciel	Nome: Luiza Cristina da Silva Vianna
Assinatura:	Assinatura:	Assinatura:

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 30/36	Data para Revalidação: 01/01/2025
Título: Anexo 1 – Definições utilizadas na Política Corporativa de TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2025				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Anexo 1 - Definições utilizadas na Política Corporativa de TI

Acesso Remoto - A capacidade de acessar informações ou sistemas de informação da Secretaria Municipal de Educação de Araruama a partir de locais remotos.

Acesso Seguro - Garante acesso a programas ou recursos específicos (tais como servidores) através de ambiente protegido da Secretaria Municipal de Educação de Araruama.

Acesso Total à Rede - Acesso a todos os recursos (tais como aplicativos, servidores e impressoras) na rede da SECRETARIA MUNICIPAL DE EDUCAÇÃO DE ARARUAMA, dentro das restrições impostas pelas permissões existentes de acesso aos usuários.

Ambiente de Produção - Local onde fica um sistema de informação que hospede dados comerciais reais ou verdadeiros, em oposição aos dados de teste.

Ambiente de Teste - Local onde fica um sistema de informação que hospede dados de teste, usados apenas para fins de desenvolvimento, teste ou garantia da qualidade.

Ambiente Protegido pela Secretaria Municipal de Educação de Araruama - O ambiente protegido pela Secretaria Municipal de Educação de Araruama é fornecido através de uma interface de web que permite acesso dos usuários a um conjunto específico de aplicações, tais como e-mail e pastas pessoais. Esse ambiente previne que usuários tenham total acesso à rede, a não ser que eles atendam as exigências da Política de Gestão para Acesso Remoto.

Área de Quarentena - Uma área de uma rede da Secretaria Municipal de Educação de Araruama na qual um dispositivo de cliente não-seguro fique isolado do resto da rede. Essa área tem a capacidade de filtrar e evitar qualquer tráfego entre o dispositivo não-seguro e o resto da rede da Secretaria Municipal de Educação de Araruama.

Área Protegida - Instalações que alojem vários servidores críticos, dispositivos de comunicação, dispositivos de rede e cabos são classificadas como áreas protegidas.

Autenticação de Dois Fatores - Um método de autenticação que exige um dispositivo físico e uma senha para acessar o dispositivo, usada para limitar o risco de acesso não autorizado aos sistemas de informação.

BI - Business Intelligence

Secretaria Municipal de Educação de Araruama - Todas as subsidiárias da Secretaria Municipal de Educação de Araruama, Inc.

Categorias - Grupo de Itens organizados por similaridade técnica e/ou de aplicação. Ex.: Alimentação, Consultoria e Auditoria, Beneficiamento etc.

Código Mal-Intencionado - Ampla categoria de códigos projetados para danificar ou excluir informação, tais como vírus, trojans, spam, key loggers e spyware.

Colaboradores - Todo o pessoal da Secretaria Municipal de Educação de Araruama, incluindo funcionários de meio período e de período integral, temporários e contratados.

Componentes de Rede - Qualquer dispositivo que resida fisicamente na rede da Secretaria Municipal de Educação de Araruama.

Conexão com Fio - Conexão Ethernet física entre um dispositivo de cliente e a rede Secretaria Municipal de Educação de Araruama.

Conexão sem Fio - Conexão feita entre um dispositivo de cliente e uma rede da Secretaria Municipal de Educação de Araruama, seja local ou remota, utilizando tecnologia sem fio, tais como 802.X, Bluetooth, HSDPA ou GPRS.

Conta com Privilégios - Contas com Privilégios são usuários com direitos privilegiados que lhes permitem acesso a serviços e funções administrativos, aos quais usuários sem privilégios restringidos.

Credenciais de Rede - O nome de usuário e senha exigidos para acessar uma rede.

Criptografia - Procedimento que torna o conteúdo de uma mensagem ou arquivo ilegível a qualquer pessoa que não tenha autorização para lê-lo.

Despesas Reembolsáveis - são todas as despesas realizadas por funcionários da Secretaria Municipal de Educação de Araruama, empresas controladas e administradas, necessárias para o exercício de suas funções.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 31/36	Data para Revalidação: 01/01/2025
Título: Anexo 1 – Definições utilizadas na Política Corporativa de TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2025				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Direitos de acesso com privilégios - Direitos de acesso que oferecem total controle em um sistema, ou com a capacidade de anular controles.

Dispositivo administrado pela Secretaria Municipal de Educação de Araruama - Dispositivo de cliente que tenha sido configurado de acordo com o Ambiente Operacional Padrão da Secretaria Municipal de Educação de Araruama e não permita a instalação, remoção ou alteração de software, ou modificação da configuração do dispositivo pelo usuário.

Dispositivo do Cliente - Qualquer dispositivo de computação utilizado para se conectar às informações ou sistemas de informação da Secretaria Municipal de Educação de Araruama.

Dispositivo Gerido pela Secretaria Municipal de Educação de Araruama - Um dispositivo do cliente que tenha sido configurado com o Ambiente de Operação Padrão da Secretaria Municipal de Educação de Araruama e não forneça aos usuários a habilidade de instalar, remover ou modificar o software, ou modificar o dispositivo de configuração.

Dispositivo Não Administrado pela Secretaria Municipal de Educação de Araruama - Dispositivo de cliente que não cumpra os requisitos de um dispositivo administrado pela Secretaria Municipal de Educação de Araruama.

Dispositivo Não Gerido pela Secretaria Municipal de Educação de Araruama - Um dispositivo de cliente que não atende às exigências de um Dispositivo Gerido pela Secretaria Municipal de Educação de Araruama.

Dispositivo Não Seguro - Qualquer dispositivo não-administrado pela Secretaria Municipal de Educação de Araruama.

Dispositivo Seguro - Qualquer dispositivo administrado pela Secretaria Municipal de Educação de Araruama.

Dispositivos Administrados pela Secretaria Municipal de Educação de Araruama – Dispositivo de cliente que tenha sido configurado de acordo com o Ambiente Operacional Padrão da Secretaria Municipal de Educação de Araruama e não permita a instalação, remoção ou alteração de software, ou modificação da configuração do dispositivo pelo usuário.

Dispositivos de Autenticação - Um dispositivo físico usado para acessar sistemas de informações, nas credenciais de rede de um usuário ou acima, para limitar o risco de acesso não autorizado aos sistemas de informações.

Dispositivos de Cliente – Qualquer dispositivo de computação utilizado para se conectar à informações ou sistemas de informação da Secretaria Municipal de Educação de Araruama.

Dispositivos Móveis – Dispositivos portáteis de clientes, como notebooks e smartphones.

Dispositivos Não Administrados pela Secretaria Municipal de Educação de Araruama – Dispositivos de clientes que não atendam às exigências de um Dispositivo Administrado pela Secretaria Municipal de Educação de Araruama.

LTI - Lista de Tecnologias Implementáveis

Entidades Terceiras - Parceiros comerciais, consultores, terceirizados, fornecedores e prestadores de serviço da Secretaria Municipal de Educação de Araruama.

Ferramentas Poderosas - Ferramentas que podem coletar e modificar remotamente informações de configuração e obter direitos de acesso com privilégios aos sistemas.

Firmware - Combinação de software e hardware que tenha sido escrita em memória ROM.

Funções Incompatíveis - Funções que, caso fossem desempenhadas por uma única pessoa, permitiria que ela anulasse os sistemas de controle.

Informações - Todas as informações de qualquer natureza e forma possuídas, guardadas, utilizadas ou sob controle da Secretaria Municipal de Educação de Araruama, que abrangem conhecimento (incluindo propriedade intelectual, comunicação verbal e conhecimentos sabidos por pessoas), dados eletrônicos e informações em papel impresso (incluindo impressão de computador e documentos contratuais).

Internet - Uma rede mundial de computadores que fornece uma variedade de informações e formas de comunicação a seus usuários, consistindo em uma forma de grupo de redes interconectadas que se utilizam de protocolos padronizados de comunicação. O termo internet também inclui as informações disponíveis nessa rede.

Item de configuração – Qualquer componente que precisa ser gerenciado, a fim de entregar um serviço de TI.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 32/36	Data para Revalidação: 01/01/2025
Título: Anexo 1 – Definições utilizadas na Política Corporativa de TI					
Descrição da Revisão: Revisão da Política Corporativa de TI				Palavra(s) Chave:	
Emissão Inicial: 01/01/2025				Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Monitoramento Não Intrusivo – Monitoramento automatizado para garantir o atendimento às políticas e normas da Secretaria Municipal de Educação de Araruama e uso efetivo dos sistemas de informação da Secretaria Municipal de Educação de Araruama.

Monitoramento ou interceptação intrusiva – Interceptação ou monitoramento de conteúdo de dados de usuário mantidos ou transmitidos para os sistemas de informação da Secretaria Municipal de Educação de Araruama, a fim de obter, por exemplo, prova de atendimento às normas e políticas.

Oracle: Sistema integrado de gestão; ERP.

Patch - Software projetado para atualizar ou resolver problemas em aplicativo de software ou prevenir exploração de vulnerabilidades.

Princípio de Menor Privilégio - Conceder a um usuário o mínimo de privilégios possível para permitir a legitimação das operações nos sistemas de informação da Secretaria Municipal de Educação de Araruama a fim de que possam cumprir suas atribuições.

Proprietário de Informação - Pessoa responsável pela criação, o armazenamento ou descarte de informações ou dados.

Proprietário de Sistema - A pessoa responsável por estabelecer as regras para o uso e a proteção apropriados dos dados / informações em um sistema.

Rede da Secretaria Municipal de Educação de Araruama - A infraestrutura de comunicação digital da Secretaria Municipal de Educação de Araruama, tais como servidores, firewalls e roteadores.

Rede Pública - Uma rede que não seja administrada pela Secretaria Municipal de Educação de Araruama.

Rede Segura - Rede administrada pela Secretaria Municipal de Educação de Araruama que esteja de acordo com as normas básicas de segurança mínima da Secretaria Municipal de Educação de Araruama para garantir a integridade comercial.

Registro - A criação de uma nova conta de usuário, após o que o acesso a outras informações e sistemas de informações poderá ser fornecido.

Segurança da Informação - A conservação das informações e sistemas de informações relacionados à Confidencialidade (garantindo que as informações e os sistemas de informações só possam ser acessados por usuários autorizados), Integridade (protegendo a precisão e integralidade das informações) e Disponibilidade (garantindo que as informações e os sistemas de informações possam ser acessados pelos usuários autorizados quando necessário).

Sistemas de Informação - Repositórios eletrônicos, inclusive, entre outros, computadores, dispositivos de computador, aplicativos de computador e redes de computador que processem, transmitam ou armazenem informações e que sejam de propriedade, alugados, emprestados ou que estejam sob o controle da Secretaria Municipal de Educação de Araruama.

Smartphone - Um smartphone é um telefone móvel com atributos de computador pessoal.

Sniffers - Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores. Pode ser usado por um invasor para capturar informações sensíveis (como senhas de usuários), em casos onde estejam sendo utilizadas conexões inseguras, ou seja, sem criptografia.

Software - Os programas exigidos para permitir que o computador execute tarefas específicas.

Software de Limpeza de dados - Software utilizado para remover dados de um dispositivo de armazenamento de informações no limite em que não possa haver qualquer recuperação dos dados.

Terceiros - Parceiros comerciais, consultores, terceirizados, fornecedores e prestadores de serviços que acessam, ou não, o sistema de informação da Secretaria Municipal de Educação de Araruama.

TI – Tecnologia da Informação.

Unidade de Negócio - Qualquer empresa ou divisão da Secretaria Municipal de Educação de Araruama.

Usuários – Colaboradores ou terceiros que façam uso dos sistemas de informação da Secretaria Municipal de Educação de Araruama.

Vulnerabilidade - Alguma fraqueza no sistema que permita a violação da integridade, confidencialidade, controle de acesso, disponibilidade, consistência ou mecanismo de auditoria do sistema ou dados e programas nele contidos por um inimigo.

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 33/36	Data para Revalidação: 01/01/2025
Título: Anexo 2 – Termo de Responsabilidade e Cautela de Equipamentos de TI					
Descrição da Revisão: Revisão da Política Corporativa de TI Emissão Inicial: 01/01/2024				Palavra(s) Chave: Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

ANEXO 2 - TERMO DE RESPONSABILIDADE E CAUTELA DE EQUIPAMENTOS DE TI

Pelo presente, responsabilizo-me pela guarda e posse do bem relacionado abaixo, respondendo perante a Secretaria Municipal de Educação de Araruama no que diz respeito à má utilização ou qualquer dano causado ao bem, assumindo os encargos de fiel depositário, nos termos do artigo 627 e seguintes do Código Civil Brasileiro, na ocorrência de qualquer dos eventos acima ou arcar com os custos de eventuais consertos, caso a Diretoria de Tecnologia e Operações julgue necessários.

Em caso de roubo, furto, extravio e perda do equipamento abaixo, deverei efetuar o registro do Boletim de Ocorrência numa delegacia policial e, de posse deste documento, contatar a área de TI para entregar cópia do mesmo.

Comprometo-me, ainda, a utilizá-lo de forma estritamente funcional, no período em que exercer cargo na Secretaria Municipal de Educação de Araruama, obrigando-me a devolvê-lo, assim como todos os seus pertences e acessórios, em perfeito estado de conservação em caso de demissão ou a pedido do RH ou superior responsável.

Nestes termos, e após conferir e achar de acordo, declaro que recebi o bem relacionado e que o mesmo encontra-se em perfeita condição de uso.

Local e data: _____, ____/____/____

Assinatura: _____

CPF: _____

Equipamento:

Tipo: Laptop/Notebook () Desktop () Monitor () Aparelho Celular ()
 Tablet () Placa GPRS () Outro () _____

Marca: _____

Modelo: _____

Número de série ou IMEI: _____

Acessórios: _____

DEVOLUÇÃO

Atesto que o aparelho foi devolvido em ____/____/____ nas seguintes condições:

Com a embalagem? ()Sim ()Não

Em: ()Perfeito estado ()Apresentando defeito ()Faltando peças ou acessórios

Local e data: _____, ____/____/____

Responsável pelo recebimento

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 34/36	Data para Revalidação: 01/01/2025
Título: Anexo 3 – Termo de Confidencialidade para Utilização de Sistemas de Informação					
Descrição da Revisão: Revisão da Política Corporativa de TI Emissão Inicial: 01/01/2024				Palavra(s) Chave: Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Anexo 3 - Termo de Confidencialidade para Utilização de Sistemas de Informação

Todos os usuários de contas com acesso aos sistemas de informação deverão previamente ler e assinar o termo de responsabilidade a seguir.

Termo de Confidencialidade para Utilização de Sistemas de Informação

Todos os colaboradores e prestadores de serviços que requeiram acesso aos sistemas de informação devem seguir o procedimento atual de solicitação de acesso Secretaria Municipal de Educação de Araruama, ler e assinar o presente termo. O acesso aos sistemas não será concedido aos que, por qualquer motivo venham a se recusar a assinar esse documento.

Esse termo define que:

1. O acesso a sistemas de informação é caracterizado por qualquer conta (identificador) e a senha que possa ser fornecida pela Secretaria Municipal de Educação de Araruama para acesso a qualquer sistema de informação fornecido pela Secretaria Municipal de Educação de Araruama, incluindo, acesso a internet, acesso a rede de dados, acesso a aplicativos etc. A partir da concessão deste acesso, o proprietário da conta passa-se a ser usuário de sistema de informação.
2. Os acessos aos sistemas de informação deverão ser utilizados apenas para a execução correta das funções designadas. O usuário que descobrir que possui um acesso indevido, deve informar imediatamente a Gerência de TI.
3. O usuário não deve se utilizar dos acessos a ele concedidos para conseguir ou fornecer acesso a outros e a recursos computacionais, ou ainda prover informações do ambiente computacional sem prévia autorização do Grupo TI e do responsável pelo recurso.
4. O usuário autoriza o monitoramento invasivo ou não invasivo das informações utilizadas ou geradas por ele durante o exercício normal das suas funções.
5. Durante a utilização dos acessos aos sistemas de informação, o usuário não deve alterar nenhuma configuração do ambiente, sistema ou aplicações que não estejam diretamente relacionados à atividade descrita nas suas funções.
6. O usuário se compromete a zelar pela confidencialidade, integridade e disponibilidade de todos os dados e informações, os quais serão tidos como sigilo profissional, inclusive após 05 (cinco) anos a partir do término do meu contrato de trabalho.

Eu li o termo acima e utilizarei o acesso aos sistemas de informação de acordo com os termos dispostos e com as demais políticas e normas de segurança atuais ou que venham a ser editadas e divulgadas nessa empresa e que venham a normatizar a utilização dos sistemas de informação. Também estou plenamente ciente de que o não cumprimento dos termos deste documento ou má utilização do meu acesso será considerado violação grave, podendo a empresa suspender o acesso e buscar os meios legais para defender seus interesses.

Local e Data: _____, ____/____/_____.

Nome: _____

Assinatura: _____

CPF: _____

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 35/36	Data para Revalidação: 01/01/2025
Título: Anexo 4 – Termo de Responsabilidade para Utilização de Contas com Privilégios					
Descrição da Revisão: Revisão da Política Corporativa de TI Emissão Inicial: 01/01/2024				Palavra(s) Chave: Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

Anexo 4 - Termo de Responsabilidade para Utilização de Contas com Privilégios

Todos os usuários de contas com privilégios devem previamente ler e assinar o termo de responsabilidade a seguir.

Termo de Responsabilidade para Utilização de Conta com Privilégios

Todos os colaboradores e prestadores de serviços que requeiram acesso com privilégios especiais devem seguir o procedimento atual de solicitação de acesso da Secretaria Municipal de Educação de Araruama, ler e assinar o presente termo. O acesso especial não será concedido aos que, por qualquer motivo venham a se recusar a assinar esse documento.

Esse termo define que:

1. O acesso especial é caracterizado pela custódia da conta (identificador) e a senha correspondente com acessos privilegiados ou total acesso ao ambiente, como por exemplo, o administrador ou root.
2. Os usuários com acesso especial devem ter o conhecimento apropriado para a utilização do login.
3. O acesso especial deve ser utilizado estritamente quando necessário.
4. Os usuários com acesso especial não devem se utilizar dos privilégios para conseguir ou fornecer acesso a recursos computacionais, ou ainda prover informações do ambiente computacional sem prévia autorização do Grupo TI e do responsável pelo recurso.
5. Ao utilizar a conta com privilégios, o usuário não deverá executar jogos, programas, scripts, comandos ou qualquer outro software não homologado pelo Grupo TI ou que causem impacto ao ambiente computacional da Secretaria Municipal de Educação de Araruama.
6. O usuário de conta com privilégios não pode se utilizar de seus privilégios sobre o sistema para ler arquivos ou e-mail de outros usuários Secretaria Municipal de Educação de Araruama, a não ser em casos específicos e previstos pelas políticas do Grupo TI e estritamente autorizado.
7. Durante a utilização do acesso especial, o usuário não deve alterar nenhuma configuração do ambiente, sistema ou aplicações que não estejam diretamente relacionados à atividade descrita no processo de autorização para uso desta conta.
8. Todas as alterações em configurações, executáveis, ou qualquer outra alteração no ambiente efetuadas com conta com privilégios deve passar por avaliação e aprovação prévia do responsável técnico do ambiente e todos os responsáveis pelo negócio da Secretaria Municipal de Educação de Araruama, através do processo de Gerenciamento de Mudanças publicado pelo Grupo TI e definido em política.

Eu li o termo acima e utilizarei conta com privilégios de acordo com os termos dispostos e com as demais políticas e normas de segurança atuais ou que venham a ser editadas e divulgadas nessa empresa que venham a normalizar a utilização da conta com privilégios. Também estou plenamente ciente de que o não cumprimento dos termos deste documento ou má utilização do meu acesso será considerado violação grave, podendo a empresa suspender o acesso e buscar os meios legais para defender seus interesses.

Local e Data: _____, ____/____/_____.

Nome: _____

Assinatura: _____

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.

	POLÍTICA CORPORATIVA DE TI				Data da Revisão: 01/01/2024
	Número: 1.0	Localizador: Normas e regras de TI	Revisão: 2	Folha: 36/36	Data para Revalidação: 01/01/2025
Título: Anexo 4 – Termo de Responsabilidade para Utilização de Contas com Privilégios					
Descrição da Revisão: Revisão da Política Corporativa de TI Emissão Inicial: 01/01/2024				Palavra(s) Chave: Política; Norma; Regra; TI	
Elaborador: DITEI – Divisão de Tecnologia e Informática					

CPF: _____

Aviso Legal

Este documento pode conter informações confidenciais e/ou privilegiadas. Se você não for o destinatário ou a pessoa autorizada a receber este documento, não deve usar, copiar ou divulgar as informações nele contidas ou tomar qualquer ação baseada nessas informações.

Disclaimer

The information contained in this document may be privileged and confidential and protected from disclosure. If the reader of this document is not the intended recipient, or an employee agent responsible for delivering this document to the intended recipient, you are hereby notified that any dissemination, distribution or copying of this communication is strictly prohibited.