PREFEITURA DE MAIRIPORÃ

SECRETARIA MUNICIPAL DE ADMINSTRAÇÃO RECURSOS HUMANOS E MODERNIZAÇÃO

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

PREFEITURA MUNICIPAL DE MAIRIPORÃ

DEPARTAMENTO DE TECNOLOGIA DA INFORMAÇÃO

Prefeitura de
MAIRIPORÃ

Sumário

1. Objetivo

O Departamento de Tecnologia da Informação que está inserido na Estrutura Organizacional da Secretaria Municipal de Administração, Recursos Humanos e Modernização da Prefeitura de Mairiporã tem por objetivo criar requisitos para estabelecer, implementar, manter e melhorar continuamente o Sistema de Segurança da Tecnologia da Informação – SGSI, incluindo os processos necessários e suas interações, de acordo com os requisitos deste documento.

Este documento apresenta uma visão geral do SGSI.

Na subseção 4.4 – Sistema de Segurança da Informação, a **Norma ABNT NBR ISSO/IEC 27001:2022** determina que:

"A organização deve estabelecer, implementar, manter continuamente um sistema de gestão da segurança da informação, incluindo os processos necessários e suas interações, de acordo com os requisitos deste documento".

O objetivo do Departamento de Tecnologia da Informação – DTI, é proteger os ativos da Prefeitura e de seus prestadores de serviços, contra as ameaças: internas ou externas, deliberadas ou acidentais.

2. Escopo do Sistema de Gestão de Segurança da Informação

O SGSI, aplicado pelo Departamento de Tecnologia da Informação, abrange toda Estrutura Organizacional da Prefeitura e deve ser cumprida e aplicada em todas as áreas da organização.

Inclusão

Localizaç	Endereç	
Mairiporã-SP center	Alameda Tibiriça,374 - 07600-084	Servidor Central –Paço Municipal Serviço em Tecnologia e Data Hosting.

Exclusão

Localizaç	Endereç	
Mairiporã-SP da	Alameda Tibiriça,535	DTI-Departamento da Tecnologia

3. Responsabilidade

Das responsabilidades específicas dos colaboradores da organização:

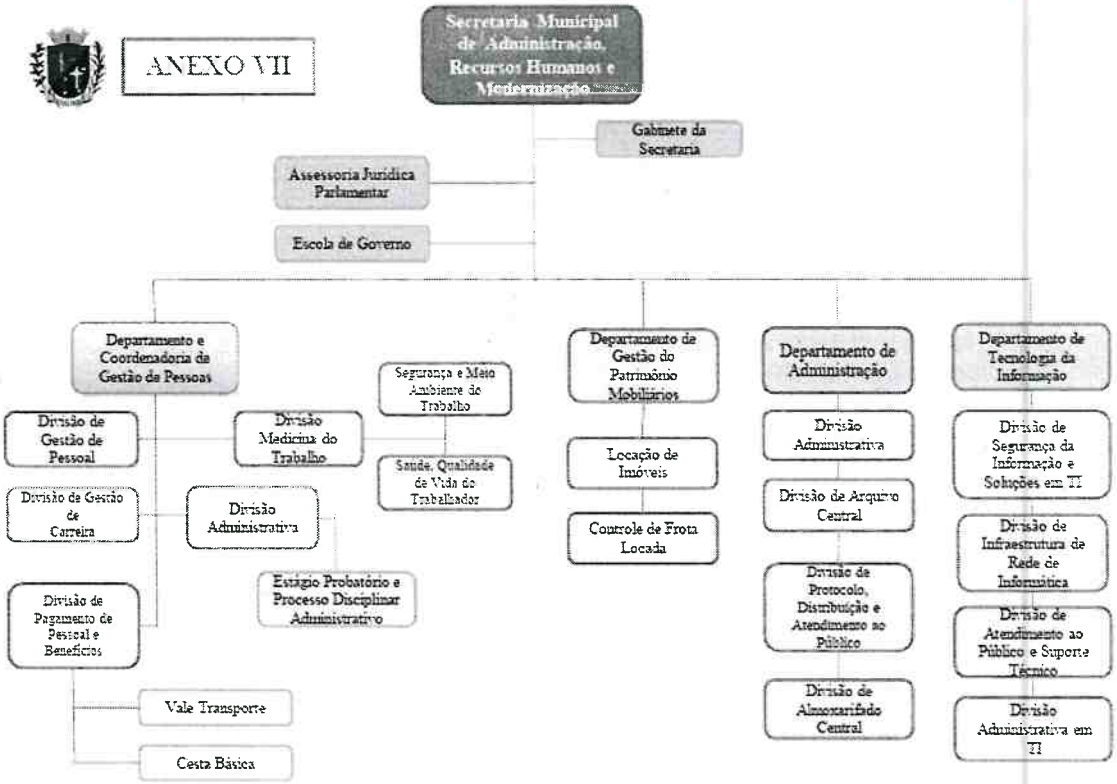
A direção e / ou gestor de segurança da informação serão os responsáveis por aprovar o escopo de certificação e sua aplicabilidade dentro do ambiente da organização.

Será de inteira responsabilidade de cada servidor, o prejuízo ou dano que vier a sofrer ou causar a organização e ou terceiros, em decorrência da não obediência às diretrizes e normas sobre a segurança da informação bem como nas regras internas, sendo submetido às medidas administrativas cabíveis.

4. Estrutura Organizacional

A TIC da Prefeitura esta integrada dentro da Secretaria da Administração com funções diversas, ora mais específicas, ora mais abrangentes e no que se refere ao destino dos esforços desses setores também varia, alguns atendem exclusivamente à Secretaria ao qual pertencem e outros a toda PMM.

ANEXO VII



Diretrizes e objetivos:

- **Missão**

Entregar ferramentas inovadoras que apoiem os servidores públicos na obtenção de resultados céleres e com qualidade no atendimento à população, garantindo assim que os investimentos em tecnologia sejam bem aplicados e otimizados para que possamos atingir a excelência na prestação dos serviços à população;

- **Visão**

Ofertar tecnologias que maximizem os resultados dos serviços prestados à população, gerando economia, sustentabilidade e melhorando sempre a visão da Administração Pública perante a população;

- **Valores Humanização**

Tratar os funcionários como seres humanos, alinhando seus desejos e expectativas às necessidades da Administração Pública;

- **Profissionalismo**

Gerar um ambiente agradável e organizado, visando maximizar os resultados;

- **Ética**

Priorizar a transparência, o comprometimento e o respeito, conduzindo nossos projetos com integridade e responsabilidade;

- **Inovação**

Apoiamos a criatividade, a capacitação e o ensino, além da produção de conhecimento e inovação de maneira sustentável e empreendedora;

- **Foco no resultado sustentável**

Nós agimos sempre para gerar valor para os clientes, gestores, colaboradores e a sociedade;

- **Qualidade**

Entregar produtos e serviços com a mais alta qualidade aos colaboradores solicitantes;

- **Respeito**

Oferecemos nossos serviços de tecnologia de maneira eficiente e sustentável para os colaboradores, gestores e comunidade.

5. Documentos de referência

Os documentos a seguir, no todo ou em parte, são referenciados e fornecem requisitos, diretrizes ou orientações que são indispensáveis à sua aplicação. Para referências datadas, aplicam-se somente as edições citadas. Para referências não datadas, aplicam-se as edições mais recentes do documento, incluindo emendas.

ISO/IEC 27000:2018	Information technology — Security techniques — Information security management systems — Overview and vocabulary
ABNT NBR ISO/IEC 27001:2022	Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos
ABNT NBR ISO/IEC 27002:2022	Segurança da informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação
ABNT NBR ISO/IEC27003:2017	Sistema de Gestão de Segurança da Informação (SGSI)
ABNT NBR ISO/IEC27004:2017	Sistema de Gestão de Segurança da Informação (SGSI)
ABNT NBR ISO/IEC27005:2019	Sistema de Gestão de Segurança da Informação (SGSI) Gestão de Risco
ABNT NBR ISO/IEC 3100:2018	Gestão de Riscos — Diretrizes

6. Documentos de complementares

Lei Federal Nº 12965 de 23 de abril de 2014	Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.
Lei Federal Nº 14129 de 29 de março de 2021	Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública
Lei Municipal Nº 4380 de 13 de	Estrutura Organizacional da Prefeitura Municipal de Mairiporã e dá outras providências.

fevereiro de 2025	
Lei Ordinária 4083 de 20 de dezembro de 2021	Agenda 2030 para o Desenvolvimento Sustentável da Organização das Nações Unidas (ONU) como diretriz de políticas públicas em âmbito municipal.
Decreto Nº 7327 de 05 de janeiro de 2015	Estabelece a Política de Segurança da Informação e utilização da rede de comunicação de dados, corrêio eletrônico, acesso a internet, equipamentos e ambientes de mensagens instanâneas, no âmbito da Prefeitura.
Decreto Nº 9484 de 06 de abril de 2022	Regulamenta a aplicação da Lei Federal nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD no âmbito da administração municipal direta e indireta.

7. Siglas

CMPD	Comissão Municipal de Proteção de dados.
DTI	Departamento de Tecnologia da Informação.
GRSIC	Gestão de Riscos de Segurança da Informação e Comunicação.
SGSI	Sistema de Gestão de Segurança da Informação.
PDCA	Plan-Do-Check-Act.
PMM	Prefeitura Municipal de Mairiporã.
LGPD	Lei Geral de Proteção de Dados Pessoais
TI	Tecnologia da Informação.

8. Termos e definições

Servidor Publico	Todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos da prefeitura municipal de Mairiporã, direta e indireta;
Funcionario tercerizado	No contexto deste documento, entende-se como colaborador quaisquer agente público, estagiário, menor aprendiz, terceirizados ou indivíduos que direta ou indiretamente utilizam ou suportam os sistemas, infraestrutura ou informações da instituição.

Para os efeitos deste documento, aplicam-se os termos e definições a seguir, baseados nas normas de referência, Glossário de Segurança da Informação da ISO/IEC 27000:2018, que devem ser interpretados somando-se as descrições. Em caso de divergência, prevalecem o termo e a definição estabelecidos no PDTI e no PSTI.

9. Contexto do Departamento de Tecnologia da Informação

O Departamento de Tecnologia da Informação assume um papel imprescindivel no contexto da Administração Pública, sob o foco da efetividade e inovação.

Para que se possa realizar um Sistema de Gestão de Segurança da Informação é necessário que a organização conte com um planejamento no qual estejam descritas as metas a serem alcançadas associadas ás ações que a área de DTI irá executar.

A Direção de TI deve buscar a melhor gestão dos recursos, primar pelas tendências tecnológicas modernas, que atendam pela qualidade na prestação dos serviços, viabilizando transparência e potencializando a eficiência, a economia e a eficácia.

10. Bens e serviços fornecidos a sociedade

O Departamento de Tecnologia da Informação contribui significativamente para o avanço da ciência e da tecnologia em benefício dos seus municipes, direta ou indiretamente, atraves da eficiencia e eficacia disponibilidade dos seus sistemas bem como adotando políticas de sustentabilidade a seus critérios de referencia **(Agenda 2030)**.

11. Liderança e compromisso

A Alta direção do Departamento de Tecnologia da Informação está comprometida com a melhoria contínua do seu sistema de gestão de segurança da informação, assim como com a sua eficácia, eficiência e efetividade.

Através da política de segurança da informação, a alta direção específica os objetivos gerais relacionados ao tema. Por sua vez, os objetivos específicos e seus indicadores são descritos no Decreto Nº 7327/2015.

Buscando a integração dos requisitos do SGSI aos processos organizacionais a alta direção estabeleceu como orgão consultivo, a Comissão Municipal de Proteção de Dados (CMPD), composta pelos representantes das unidades organizacionais da Prefeitura Municipal e determinou como sendo o foro para os alinhamentos estratégicos sobre os temas relacionados.

Visando prover os recursos necessários, ações de segurança da informação são contempladas no PDTI (Plano Diretor da Tecnologia da Informação), no PDTIC (Plano Diretor de Tecnologia da Informação e Comunicação) e nos PCAs (Planos de Contratação Anual). Os recursos financeiros são alocados com base na LOA (Lei Orçamentária Anual) que é uma ferramenta para garantir que o municipio execute suas políticas públicas e projetos de forma ordenada, controlada e dentro das limitações financeiras.

Para assegurar que os colaboradores compreendam a importância da eficácia da segurança da informação e de sua gestão, a alta direção, por meio do DTI, envia memorando aos departamentos atualizando o conhecimento no quesito segurança que anualmente atualiza e disponibiliza no site através de cartilhas.

Anualmente, durante a reunião de análise crítica do SGSI, a alta direção avalia se o mesmo está alcançando os resultados pretendidos. Quando necessário, são feitos apontamentos

para ajustes e ações corretivas, garantindo que os objetivos sejam atingidos.

12. Partes interessadas

O Departamento de Tecnologia da Informação está comprometido em criar, manter e melhorar um sistema de gestão de segurança da informação de acordo com a norma **ISO/IEC 27001:2022**. Isso significa que o Departamento se preocupa em ter uma boa governança, com treinamento adequado e papéis bem definidos para todos os envolvidos.

O DTI considera as necessidades e expectativas de todas as partes interessadas, assim como o ambiente em que opera. Essas informações ajudam a definir a estratégia e a implementação do Sistema de Gestão da Segurança da Informação, além de gerenciar a segurança das suas informações.

As informações sobre as necessidades e expectativas das partes interessadas estão detalhadas no PDTI, bem como toas as Secretarias envolvidas.

13. Declaração de aplicabilidade

Tendo como base uma análise periódica do seu contexto, das necessidades e expectativas das partes interessadas, do resultado do processo de avaliação e riscos e do processo de melhoria do sistema de gestão realizado com o apoio da análise crítica da alta direção, o DTI avalia a aplicabilidade dos controles que compõe o anexo A da norma **ABNT/NBR ISO/IEC 27001** e registra as informações no documento 06-SOA (Declaração de Aplicabilidade).

14. Política da segurança da informação

A Política de Segurança da Informação do DTI busca proteger os ativos de informação de sua propriedade e sua guarda, sendo elaborada com base na norma técnica **ABNT NBR ISSO/IEC 27001.**

"A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos."

15. Objetivos da segurança da informação

A gestão de segurança da informação e comunicação baseia-se no processo de melhoria contínua, denominado ciclo **PDCA - (Plan-Do-Check-Act)**, referenciado pela norma **ABNT NBR**

ISO/IEC 27001:2022. Estes processos estão diretamente ligados à política de segurança da informação de toda a Prefeitura.

Plan (planejar) – estabelecer o SGSI	Estabelecer a política, objetivos, processos e procedimentos do SGSI, relevantes para a gestão de riscos e a melhoria da segurança da informação para produzir resultados de acordo com as políticas e objetivos globais de uma organização.
Do (fazer) – implementar e operar o SGSI	Implementar e operar a política, controles, processos e procedimentos do SGSI.
Check (checar) - Monitorar e analisar criticamente o SGSI	Avaliar e, quando aplicável, medir o desempenho de um processo frente a política, objetivos e experiências práticas do SGSI e apresentar os resultados para a aanálise crítica pela direção.
Act (agir) – manter e melhorar o SGSI	Executar as ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e da análise crítica pela direção ou outra informação pertinente para alcançar a melhoria continua do SGSI.

No escopo deste sistema de gestão, os objetivos a serem alcançados, são definidos no documento. O nível de importância dos objetivos é definido baseado nos valores obtidos a partir da análise de risco.

16. ABNT NBR ISSO/IEC 27002

Este sistema de gestão e seus processos, para assegurar os aspectos de segurança da informação, são baseados na **Norma ISO/IEC 27001 ("Information security, cybersecurity and privacy protection - Information Security Management Systems - Requirements").**

Este sistema de gestão prevê diversas ações, subprocessos, políticas e procedimentos de segurança, praticando a missão de reduzir continuamente os riscos à segurança das informações aos ativos críticos de uma organização.

17. Papeis e responsabilidades

O modelo de Gestão da Segurança da Informação do DTI baseia-se **na Norma ISO/IEC 27001** e distribui-se na atuação dos seguintes grupos:

A comunicação das responsabilidades é realizada mediante publicação dos Memorandos do DTI da Prefeitura.

O DTI protegerá seus ativos, físicos e intelectuais (pessoas, informações, incluindo dados pessoais, sites, materiais, propriedade intelectual) de acordo com leis, contratos, regulamentos internos, regulamentos externos e sua avaliação de riscos.

18. Ações para endereçar riscos e oportunidades

O objetivo de gestão de riscos da segurança de informação do DTI é identificar os principais riscos aos seus macroprocessos. A análise de riscos é controlada e executada com o

apoio do Gestor de Risco da Segurança da Informação e está documentada através da planilha matriz de riscos, apresentada no documento como referencia a ISO 27005:2019 Gestão de Riscos.

Os riscos e oportunidades são avaliados regularmente. No processo de análise de riscos, o DTI realiza a avaliação baseada em metodologia própria referencia a ISO 27005:2019 Gestão de Riscos. Os impactos potenciais, são mapeados, definidos, endereçados e ações são planejadas para tratar e minimizar os riscos.

As auditorias são conduzidas anualmente para avaliar o status dos controles internos, conforme descrito no documento.

O gerenciamento de riscos é garantido pela matriz de riscos, descrevendo os riscos por categoria, frequência, vulnerabilidade etc.

Visando o acompanhamento, o planejamento e a melhoria contínua, anualmente a alta direção em conjunto com o gestor de segurança realiza a reunião de "Análise Crítica o Sistema de Gestão de Segurança da Informação".

No escopo deste sistema de gestão, os objetivos a serem alcançados, são definidos no documento. O nível de importância dos objetivos é definido baseado nos valores obtidos a partir da análise de risco.

19. Planejamento para o alcance dos objetivos

Todos os anos são definidos planos de ação para garantir uma melhoria contínua na gestão de segurança da informação.

20. Competências

As competências necessárias para trabalhar no Departamento de TI da Prefeitura, são publicadas nos editais de Concursos Públicos. As informações de pré-requisitos e competências são publicadas no Imprensa Oficial da Prefeitura Municipal.

No caso de recursos terceirizados, os pré-requisitos e competências são especificados no termo de referência dos editais de licitação pública. O gestor do contrato, que é um servidor com atribuições gerenciais, é designado para coordenar e comandar o processo de gestão e fiscalização da execução contratual.

21. Conscientização em segurança da informação

Todos os colaboradores devem participar dos treinamentos de conscientização da segurança da informação e procedimentos organizacionais relacionados à Segurança da Informação. Os treinamentos serão realizados de uma das seguintes formas:

(i) presencial ou

(ii) à distância utilizando um ambiente virtual de aprendizagem ou no formato de webinar.

Os colaboradores que não puderem estar presentes no dia dos treinamentos presenciais

deverão realizá-los utilizando uma das plataformas disponibilizadas.

É necessário conscientizar todos os colaboradores para que conheçam e entendam o que são:

I - Sistema de Gestão de Segurança;

II - Comissão Municipal de proteção de Dados;

III - Política de Segurança da Informação e Comunicação; e,

VI – Como todos os colaboradores podem contribuir.

Por intermédio das ações das campanhas de conscientização a instituição mantem os colaboradores cientes sobre a política de segurança da informação, das políticas e normas complementares. Assim como da importância da sua contribuição para o sistema de gestão e do impacto das não conformidades.

22. Comunicação

Os documentos controlados, relacionadas ao SGSI do DTI da Prefeitura, deverão ser anexados ao processo.

Os documentos controlados do SGSI devem especificar os papeis e as responsabilidades sobre o processo necessário para a sua divulgação, incluindo ao menos as seguintes informações: quando comunicar; com quem comunicar e como se comunicar.

Assunto	Frequência	Meio de Comunicação	Para quem será comunicado
Política de Segurança da Informação e Comunicação da Prefeitura em um todo – PMM	Quando necessário	E-mail (lista de distribuição); Site oficial da instituição	Todos os colaboradores
Normas e Políticas complementares de segurança da informação	Quando necessário	E-mail (lista de distribuição); site oficial da instituição; repositório de documentos controlados;	Partes interessadas
Procedimento técnicos e operacionais	Quando necessário	E-mail (lista de distribuição); repositório de documentos controlados; repositório de procedimentos;	Partes interessadas
Artefatos da campanha de conscientização em segurança da informação	Mensalmente	E-mail (lista de distribuição); Site oficial da instituição; redes sociais;	Todos os colaboradores e para o público em geral
Notificação de incidentes de segurança	Quando necessário	E-mail	Gestor de segurança da informação
Notificação de não conformidades do SGSI	Quando necessário	E-mail	Gestor de segurança dainformação
Circular interno	Mensal	Boletim de serviço	Todos os colaboradores
Comunicados em geral	Quando necessário	E-mail interno (lista de distribuição)	Todos os colaboradores

23. Informação documentada

Todos os documentos classificados como públicos devem ser disponibilizados no site da Prefeitura Municipal - Imprensa Oficial.

24. Auditoria interna

A auditoria interna poderá ser executada através de recursos internos da Prefeitura ou através de empresas terceirizada, a contratada deve garantir a aderência à estrutura de controle da **ISO/IEC 27001:2022**. As regras aplicáveis aos padrões ISO são descritas no documento que será elaborado pela empresa de auditoria contratada.

A auditoria interna deve ser realizada ao menos uma vez por ano.

25. Análise crítica da alta direção

Periodicamente, as equipes deverão encaminhar para o Gestor de segurança da informação, as informações sobre os seus indicadores. As informações sobre os indicadores e sobre os objetivos de segurança da informação serão analisadas de acordo com as metas locais definidas pelo Diretor do DTI.

Esta atividade ocorrerá com periodicidade anual, dentro dos quais serão incluídos os requisitos solicitados pelas **normas ISO/IEC 27001:2022**.

26. Melhorias

Esta seção descreve como serão tratadas as não conformidades e as oportunidades de melhoria do **SGSI**.

a. Não conformidades e ações corretivas

As não conformidades apontadas nas auditorias interna e externa, são endereçadas, planejadas para ação corretiva.

As ações corretivas poderão ser mapeadas em planos de ação ou em ações pontuais.

O acompanhamento da execução das ações de tratativas será realizado pelos líderes das equipes e reportado ao gestor de segurança.

b. Melhoria contínua

Oportunidades de melhoria devem ser identificadas e implementadas para aperfeiçoar a eficiência do sistema de gestão de segurança. Os planos de melhoria dizem respeito a todo o sistema.

Os planos de melhoria são implementados para aprimorar o sistema local, sua maturidade e sua eficiência.

O acompanhamento da execução das ações de tratativas será realizado pelos líderes das equipes e reportado ao gestor de segurança da informação.

27. Publicação e divulgação

Este documento deve ser de conhecimento do Diretor e/ou gestor de segurança da informação, dos auditores, dos servidores e dos colaboradores do DTI diretamente envolvidos na segurança da informação e no processo de certificação da **ISO/IEC 27001**.

O diretor e/ou gestor de segurança da informação são os responsáveis pela elaboração, pela avaliação do SGSI. O diretor é o responsável pela aprovação desta norma. Análise crítica do documento.

Este documento deverá ser analisado criticamente, quanto à sua eficácia e adequação ao SGSI do DTI, ao menos a cada 12 meses, ou quando ocorrem mudanças.

28. Histórico da revisão e quadro de aprovação

Revisão	Data	Itens Revisados
1.0	18/01/2025	Documento Inicial.
2.0	21/03/2025	Revisão e atualização da estrutura do documento com base na versão de 2022 da norma ABNT/NBR ISO/IEC 27001; Registro dos documentos do SGSI relacionados a cada seção do documento.
2.1	15/05/2025	Revisão e Atualização – inclusão da ISO 31000 Diretrizes – Gestão de Riscos

Quadro de Aprovação		
	Nome	**Atribuição**
Elaborado por:	Alexandre Chimura	Chefe de Divisão da Segurança da Informação
Verificado por:	Valdeir Almeida	Chefe de Divisão ADM –TI
Aprovado por:	Luiz Akimura	Diretor do Departamento de Tecnologia da Informação

29. Das disposições finais

A segurança da informação deve ser entendida como parte fundamental da cultura interna da organização, ou seja, qualquer incidente de segurança submete-se como alguém agindo contra os bons costumes regidos pela organização.

Para o cumprimento do previsto neste sistema o órgão deve definir seus próprios planos de ação, com atividades, prazos e responsáveis pela implementação dos processos de gestão de segurança da informação conforme descrito. Sendo necessário revisões regularmente deste documento, a fim de mantê-lo atualizado as necessidades da organização.