Política de Segurança da Informação

NIVEL CONFIDENCIALIDADE	Protected
DOCUMENTO REF	ISMS-DOC-05-4
VERSÃO	v1.1 Final
DATA	21 June 2024
DESENVOLVIDO POR	Project Manager
RESPONSAVEL PELO DOCUMENTO	Joaquim Francisco

Historial de Atualizações

VERSÃO	DATA	REVISTO POR	RESUMO DAS ATUALIZAÇÕES
V1.0 Final	12 Apr 24	Duarte Damas	Desenvolvimento versão base
V1.1 Final	21 Jun 24	Duarte Damas	Atualização dos pontos: 2.3; 2.4; 2.5; 2.6

Distribuição

NOME	DETALHES
Teams / SharePoint	

Aprovação

NOME	FUNÇÃO	MEIO DE APROVAÇÃO	DATA
Joaquim Francisco	Partner	e-mail	13 Set 2024

Índice

Tabelas

1 Introdução

Este documento define a política de segurança da informação da AMT Consulting.

Enquanto organização dinâmica e assente em tecnologia, a AMT Consulting reconhece a necessidade de garantir que seu negócio funcione sem problemas e sem interrupções para o benefício de seus clientes, acionistas e outras partes interessadas.

Para proporcionar esse nível de operação contínua, a AMT Consulting implementou um Sistema de Gestão de Segurança da Informação (SGSI) alinhado com a Norma Internacional de Segurança da Informação, ISO/IEC 27001. Esta norma define os requisitos para um SGSI com base nas melhores práticas internacionalmente reconhecidas.

O funcionamento do SGSI tem múltiplos benefícios para o negócio, incluindo:

- Proteção dos fluxos de receitas e rentabilidade da empresa
- Garantir a prestação de serviços aos clientes
- Manutenção e valorização do acionista
- Cumprimento de requisitos legais e regulamentares

A AMT Consulting decidiu manter a certificação completa de acordo com a norma ISO/IEC 27001 para que a adoção efetiva das melhores práticas de segurança da informação possa ser validada por um terceiro independente, um Organismo de Certificação Registado (RCB).

De acordo com a ISO/IEC 27001, os controlos de referência detalhados no anexo A da norma devem ser adotados quando apropriado pela AMT Consulting. Estes são revistos periodicamente à luz dos resultados das avaliações de risco e em conformidade com os planos de tratamento dos riscos em matéria de segurança da informação. Os pormenores dos controlos previstos no anexo A que foram implementados e dos que foram excluídos são definidos na Declaração de Aplicabilidade (SoA).

Além disso, foram adotados e aplicados, sempre que adequado, controlos reforçados e adicionais decorrentes das seguintes normas e/ou regulamentos:

- ISO/IEC 27001:2022 - Segurança da informação, cibersegurança e proteção da privacidade — Sistemas de gestão da segurança da informação — Requisitos
- ISO/IEC 27002:2022 - Segurança da informação, cibersegurança e proteção da privacidade - Controlos de segurança da informação
- ISO/IEC 27005:2022 - Segurança da informação, cibersegurança e proteção da privacidade - Orientações sobre a gestão dos riscos de segurança da informação
- Lei Portuguesa 58/2019 (assegura a aplicação nacional do Regulamento (UE) 2016/679)

A adoção destas referências fornece garantia adicional aos nossos clientes e reforça a nossa conformidade com a legislação internacional de proteção de dados.

2 Política de Segurança da Informação

2.1 Finalidade

Esta política estabelece a estrutura para gerir e proteger os ativos de informação da AMT Consulting, garantindo o cumprimento dos requisitos legais, regulatórios e contratuais e apoiando o Sistema de Gestão de Segurança da Informação (SGSI) da AMT Consulting.

2.2 Âmbito de Aplicação

A Política de Segurança da Informação aplica-se a todos os indivíduos da AMT Consulting, incluindo colaboradores, prestadores de serviço e terceiros associados. Regula a utilização e a proteção de todos os ativos de informação que abrangem sistemas digitais, redes, equipamentos, aplicações de software e documentos físicos, independentemente do formato ou meio.

A política abrange de forma abrangente todas as atividades e processos relacionados com o manuseamento dos ativos de informação, seja no local, remotamente ou por meio de dispositivos pessoais para fins profissionais, incluindo procedimentos operacionais, processamento de dados, atividades de comunicação e interações com os sistemas de informação da organização.

Sendo amplo, o âmbito garante que todas as atividades de segurança da informação, desde as operações diárias até as decisões estratégicas, são geridas de forma consistente e segura, refletindo o compromisso da organização em proteger os seus ativos de informação contra ameaças e vulnerabilidades.

2.3 Responsabilidade

A Política de Segurança da Informação deve ser implementada por todos os departamentos e unidades de negócio da AMT Consulting, em conjunto com a área de IT. As Políticas de Segurança da Informação definem os objetivos de controlo, uma vez que devem ser aplicados a todos os departamentos da AMT Consulting.

A Gestão de topo ('Management') está empenhada em satisfazer os requisitos de segurança da informação aplicáveis e em melhorar continuamente o Sistema de Gestão de Segurança da Informação.

Adicionalmente, o Management da AMT Consulting é o principal responsável pela implementação e controlo do Sistema de Gestão de Segurança da Informação (SGSI), incluindo a Supervisão, Alinhamento, Aprovação, Revisão e Melhoria Contínua das Políticas e Processos. O Management garante também que autoridades e responsabilidades sejam

atribuídas a funções especificas, por forma a assegurar a gestão de dados e informação, assegurar o cumprimento normativo e Legal aplicável, bem como representar o compromisso para com a Segurança da Informação.

Os **colaboradores,** incluindo a Gestão de topo e todos os membros da estrutura organizacional da Gestão de Segurança da Informação, são responsáveis por manter um comportamento consistente com a "Política de Segurança da Informação". Tal inclui seguir todas as orientações e procedimentos para o tratamento seguro da informação e Proteção de Dados.

Os colaboradores **da AMT Consulting são ainda responsáveis por comunicar** prontamente qualquer suspeita de violações de políticas, incidentes de segurança ou potenciais violações à autoridade apropriada dentro da organização; **manter a vigilância** e **adotar as melhores práticas de segurança** nas operações diárias. Isto inclui proteger credenciais e ativos da organização, usar senhas fortes e ter cuidado com anexos e links de e-mail.

O não cumprimento das regras de segurança da informação será tratado como uma violação das políticas internas e resultará em ações corretivas de acordo com o Processo Disciplinar interno e/ou leis e regulamentos aplicáveis.

2.4 Orientações para a Gestão da Segurança da Informação

Em linha com o nosso compromisso com a segurança da informação, a **AMT Consulting** implementou um Sistema de Gestão de Segurança da Informação (SGSI) alinhado com a norma ISO/IEC 27001:2022.

2.4.1 Definição de Segurança da Informação

A Segurança da Informação envolve a proteção da **confidencialidade, integridade** e **disponibilidade** de todas as formas ou formatos de informação, incluindo dados digitais, documentos em papel e conhecimento tácito. Esta garante que os dados sejam protegidos contra acesso, utilização, divulgação, alteração ou destruição não autorizados, garantindo assim a salvaguarda do seu valor, confiabilidade e acessibilidade. O âmbito inclui todos os processos e práticas que mantêm a segurança e a confidencialidade dos ativos de informação de uma organização.

2.4.2 Gestão de Riscos

A Gestão de Riscos é o processo de identificação, avaliação e controlo de ameaças aos ativos de informação de uma organização.

Desta forma, a AMT Consulting estabeleceu um modelo de *security governance* que inclui a definição de funções e responsabilidades de segurança, bem como metodologias para gerir e avaliar riscos de segurança. Tal envolve identificar, controlar e eliminar várias ameaças a dados e informação. Adicionalmente, a AMT Consulting definiu requisitos de segurança para a gestão de terceiros, alinhando-se com as necessidades do negócio e dos clientes e com os regulamentos relevantes.

2.4.3 Requisitos de segurança da informação

Uma definição clara dos requisitos de segurança da informação da AMT Consulting foi acordada e é mantida com as áreas de negócio *core* para garantir que todas as atividades do SGSI se concentrem no cumprimento desses requisitos. Os requisitos normativos, regulamentares e contratuais também foram documentados e incorporados no processo de planeamento.

Para a AMT Consulting, um princípio fundamental do Sistema de Gestão de Segurança da Informação (SGSI) é que as necessidades do negócio impulsionem os controlos implementados. A empresa comunica regularmente estes controlos a todos os colaboradores através de reuniões de equipa, sessões de sensibilização regulares e comunicações internas.

2.4.4 Gestão de Incidentes de Segurança

A Gestão de Incidentes de Segurança na AMT Consulting envolve a definição de responsabilidades e procedimentos para a gestão de incidentes de segurança. Incluindo, a prevenção, deteção, registo, comunicação, tratamento e investigação de incidentes e vulnerabilidades que possam comprometer a segurança da informação, a proteção de dados pessoais ou a continuidade do negócio. É identificado um único ponto de contacto para todos os relatórios de incidentes. O processo garante que os incidentes sejam registados e inclui melhoria contínua e revisões periódicas.

2.4.5 Gestão de Segurança de Recursos Humanos

A Segurança de Recursos Humanos na AMT Consulting implica que todos os colaboradores compreendam e cumpram com as suas responsabilidades de segurança da informação de acordo com as suas funções. As principais medidas incluem, Ampla Divulgação da Política de Segurança da Informação para todos os colaboradores, prestadores de serviço e outras partes interessadas; Sessões regulares de Formação e Sensibilização para reforçar a importância da segurança da informação e das responsabilidades individuais; Controlos de proteção durante as transições de emprego para proteger os interesses da AMT Consulting e de seus colaboradores durante os processos de início, alteração ou término de funções.

2.5 Princípios orientadores das atividades de segurança da informação

A informação gerida pela AMT Consulting, incluindo os seus processos de suporte, sistemas, aplicações e redes, são ativos valiosos. A perda de confidencialidade, integridade e disponibilidade pode levar a uma perda de credibilidade nos serviços prestados pela AMT Consulting. Por isso, a AMT Consulting está empenhada em defender um conjunto robusto de princípios que formam a base da nossa Política de Segurança da Informação. Estes princípios são parte integrante da nossa dedicação em salvaguardar a confidencialidade, integridade e disponibilidade dos nossos ativos de informação.

Ao aderir a esses princípios orientadores, garantimos uma abordagem consistente e eficaz à segurança da informação, alinhando as nossas práticas com os melhores padrões do setor e requisitos regulamentares. Cada princípio foi cuidadosamente selecionado para abordar os diversos aspetos da segurança da informação, desde a proteção de dados pessoais e sensíveis até o estabelecimento de uma infraestrutura de segurança resiliente e transparente. Abaixo estão os princípios-chave que a AMT Consulting segue fielmente para manter os mais altos padrões de segurança da informação:

- Confidencialidade: Garantir que dados e informação sejam acessíveis apenas às pessoas autorizadas a ter acesso.
- Integridade: Manter a precisão e integridade dos dados e impedir modificações não autorizadas.
- Disponibilidade: Garantir que os utilizadores autorizados tenham acesso a dados e informação e aos ativos associados quando necessário.
- Autenticação e Identificação: Identificar e autenticar utilizadores, equipamentos e entidades para garantir que apenas entidades, equipamentos e utilizadores autorizados possam aceder aos sistemas de informação.
- Princípio de Não Repúdio *(Non-Repudiation):* Estabelecer mecanismos para evitar a negação de envolvimento em transações ou atividades, fornecendo prova da integridade e origem dos dados.
- *Responsabilidade e Auditoria*: Responsabilizar indivíduos e sistemas pelas suas ações, com auditorias regulares de conformidade e segurança.
- Privacidade: Proteger dados pessoais e sensíveis em conformidade com as leis de privacidade e as melhores práticas.
- Princípio de Mínimo Privilégio e Separação de Funções: Conceder apenas os níveis mínimos de acesso necessários para que os utilizadores desempenhem as suas funções com base na sua identidade e função, distribuindo tarefas e privilégios entre múltiplas funções para evitar conflitos de interesses e fraudes.
- Princípio de *Open Security:* Evitar a dependência do sigilo de design ou implementação para segurança, e garantir medidas de segurança robustas e visíveis.
- Princípio de *Defense in Depth:* Implementação de múltiplas camadas de controlos de segurança para proteção contra diversas ameaças.
- Princípio de *Fail Safe:* Conceber sistemas para manter a postura de segurança em caso de falha ou comprometimento.

- Princípio de *Zero Trust*: *"Never trust, always verify"* implementar a verificação contínua de acessos, minimizando as zonas de confiança.

2.6 Objetivos de Segurança de Informação

Os objetivos de segurança da informação são essenciais para proteger dados confidenciais, garantir a conformidade com normas e regulamentos, gerir riscos e prevenir incidentes de segurança. Os objetivos de segurança da informação da AMT Consulting baseiam-se na compreensão clara dos requisitos de negócio, de acordo com o processo de revisão pela gestão, durante o qual são obtidas as opiniões das partes interessadas relevantes. Estes objetivos são documentados para um período definido, bem como com os detalhes sobre como serão alcançados. Os objetivos são avaliados e monitorizados como parte da revisões pela gestão para garantir que continuam válidos. Quaisquer alterações necessárias serão geridas através do processo de gestão de alterações. Os seguintes objetivos foram cuidadosamente definidos para abordar vários aspetos da nossa estrutura de segurança da informação:

- Objetivo 1 – Implementação efetiva da ISO27001 e obtenção da certificação
- Objetivo 2 – Manter a confiança das partes interessadas comunicando e reportando as atividades e resultados da segurança da informação e da ISO 27001
- Objetivo 3 – fornecer serviço ao cliente de alta qualidade e minimizar o tempo de inatividade do sistema (<0,5%)
- Objetivo 4 – Manter e reforçar o sistema de segurança da informação para minimizar a perda de receitas
- Objetivo 5 - Gerir equipamento e software informáticos para planear necessidades futuras e evitar a escassez de recursos
- Objetivo 6 - Aumento da Sensibilização dos Colaboradores para a Segurança da Informação
- Objetivo 7 - Cumprimento dos Requisitos Legais e Regulamentares
- Objetivo 8 - Melhoria da eficácia da gestão dos riscos
- Objetivo 9 - mitigar eficientemente quaisquer incidentes de segurança da informação e manter o total anual abaixo de 5.

2.7 Melhoria contínua do SGSI

Na AMT Consulting, entendemos que o panorama da segurança da informação está em constante evolução, surgindo constantemente novos desafios e ameaças. Por isso, estamos empenhados numa filosofia de melhoria contínua no nosso Sistema de Gestão de Segurança da Informação (SGSI).

A política da AMT Consulting em relação à melhoria contínua consiste em:

- Melhorar continuamente a eficácia do SGSI

- Melhorar os processos atuais para alinhá-los com as boas práticas, conforme definido na ISO/IEC 27001 e normas relacionadas
- Obter a certificação ISO/IEC 27001 e mantê-la continuamente
- Aumentar o nível de proatividade (e a perceção de proatividade das partes interessadas) no que diz respeito à segurança da informação
- Implementação de auditorias internas e externas. Auditorias internas, realizadas periodicamente para garantir que o nosso SGSI está a funcionar como pretendido e para identificar áreas de melhoria. As auditorias externas, conduzidas por partes independentes, fornecem uma avaliação objetiva da nossa conformidade com normas como a ISO/IEC 27001 e os requisitos legais relevantes.
- Rever anualmente as métricas relevantes para avaliar se é adequado alterá-las, com base nos dados históricos recolhidos
- Obter ideias de melhoria através de reuniões regulares e outras formas de comunicação com as partes interessadas
- Rever ideias de melhoria em reuniões regulares de gestão, a fim de estabelecer prioridades e avaliar prazos e benefícios
- Atualizar regularmente os nossos processos de avaliação e gestão de riscos para garantir que refletem com precisão o panorama atual das ameaças e o apetite de risco da organização
- Atualizar continuamente os nossos programas de formação e iniciativas de sensibilização para garantir que todos os colaboradores estão equipados com os conhecimentos e competências mais recentes para contribuir eficazmente para o nosso SGSI.

Ao incorporar a melhoria contínua no núcleo de nosso SGSI, garantimos que as nossas medidas de segurança da informação permaneçam eficazes, relevantes e alinhadas com nossos objetivos organizacionais e com a natureza evolutiva das ciberameaças.

2.8 Áreas de intervenção da segurança da informação

A AMT Consulting define políticas numa ampla variedade de áreas relacionadas com a segurança da informação, que são descritas em detalhe num conjunto abrangente de documentação (políticas, processos e procedimentos) que acompanham esta política abrangente de segurança da informação. Estas políticas foram concebidas para funcionar em harmonia com esta política abrangente e contribuir para o Sistema de Gestão de Segurança da Informação da AMT Consulting. Estas incluem, mas não se limitam ao conjunto de políticas apresentadas no quadro abaixo.

Cada uma destas políticas é definida e acordada por uma ou mais pessoas com competência na área relevante e, uma vez formalmente aprovadas, é comunicada a um público apropriado, tanto dentro como fora da organização.

A tabela abaixo mostra as políticas individuais dentro do conjunto de documentação e resume o conteúdo de cada política e o público-alvo das partes interessadas.

TÍTULO DA POLÍTICA	ÁREAS ABORDADAS	PÚBLICO-ALVO
Política de Acesso à Internet	Utilização comercial da Internet, utilização pessoal da Internet, gestão de contas de Internet, segurança e monitorização e utilizações proibidas do serviço de Internet.	Utilizadores do serviço de Internet
Política de Computação em Nuvem	*Due diligence*, inscrição, configuração, gestão e remoção de serviços de computação em nuvem.	Colaboradores envolvidos na aquisição e gestão de serviços na nuvem
Política de Dispositivos Móveis	Cuidado e segurança de dispositivos móveis como laptops, tablets e smartphones, que sejam fornecidos pela organização para utilização profissional.	Utilizadores de dispositivos móveis fornecidos pela empresa
Política de BYOD	*Bring Your Own Device* (BYOD) quando os colaboradores pretendam utilizar os seus próprios dispositivos móveis para aceder a informações empresariais.	Utilizadores de dispositivos pessoais para utilização comercial restrita
Política de Teletrabalho	Considerações de segurança da informação no estabelecimento e gestão de um local e acordo de teletrabalho, por exemplo, segurança física, seguros e equipamentos	Gestão e colaboradores envolvidos na criação e manutenção de um local de teletrabalho
Política de Controlo de Acesso	Registo e cancelamento de registo de utilizadores, fornecimento de direitos de acesso, acesso externo, revisões de acesso, política de palavras-passe, responsabilidades dos utilizadores e controlo de acesso a sistemas e aplicações.	Colaboradores envolvidos na configuração e gestão de controlo de acesso
Política de Controlo de Acesso Dinâmico	Aplicabilidade e utilização de controlos de acesso dinâmicos disponíveis em ambientes específicos.	Proprietários de ativos e equipa de TIC
Política Criptográfica	Avaliação de riscos, seleção de técnicas, implementação, testes e revisão de encriptação e gestão de chaves.	Colaboradores envolvidos na criação e gestão da utilização de tecnologia e técnicas criptográficas
Política de Segurança Física	Áreas seguras, segurança do papel e dos equipamentos e gestão do ciclo de vida dos equipamentos.	Todos os colaboradores
Política Anti-Malware	Firewalls, antivírus, filtragem de spam, instalação e verificação de software, gestão de vulnerabilidades, formação de sensibilização de utilizadores, monitorização e alertas de ameaças, análises técnicas e gestão de incidentes de malware.	Colaboradores responsáveis por proteger a infraestrutura da organização contra malware
Política de Backup	Ciclos de cópia de segurança, cópias de segurança na nuvem, armazenamento externo, documentação, testes de recuperação e proteção de suportes de armazenamento.	Colaboradores responsáveis pela conceção e implementação de sistemas de backup
Política de Registo e Monitorização	Configurações para recolha de eventos. Proteção e revisão.	Colaboradores responsáveis por proteger a infraestrutura da organização contra ataques

TÍTULO DA POLÍTICA	ÁREAS ABORDADAS	PÚBLICO-ALVO
Política de Software	Aquisição de software, registo, instalação e remoção de software, desenvolvimento interno de software e utilização de software na cloud.	Todos os Colaboradores
Política de Gestão Técnica de Vulnerabilidades	Definição de vulnerabilidade, fontes de informação, patches e atualizações, avaliação de vulnerabilidade, reforço, formação de sensibilização e divulgação de vulnerabilidade.	Colaboradores responsáveis por proteger a infraestrutura da organização contra malware
Política de Segurança de Rede	Projeto de segurança de rede, incluindo segregação de rede, segurança perimetral, redes sem fios e acesso remoto; gestão da segurança da rede, incluindo funções e responsabilidades, registo, monitorização e alterações.	Colaboradores responsáveis pela conceção, implementação e gestão de redes
Política de Mensagens Eletrónicas	Envio e receção de mensagens eletrónicas, monitorização de recursos de mensagens eletrónicas e utilização de e-mail.	Utilizadores de serviços de mensagens eletrónicas
Política de Colaboração Online	Utilização de ferramentas de colaboração para comunicação, partilha e videoconferência.	Utilizadores de ferramentas de colaboração online
Política de Desenvolvimento Seguro	Especificação de requisitos de negócio, design de sistemas, desenvolvimento e testes e desenvolvimento de software em outsourcing.	Colaboradores responsáveis por conceber, gerir e escrever código para desenvolvimentos de software à medida
Política de Segurança da Informação para Relações com Fornecedores	*Due diligence,* acordos com fornecedores, monitorização e revisão de serviços, alterações, litígios e cessação de contrato.	Colaboradores envolvidos na criação e gestão de relações com fornecedores
Política de Gestão de Disponibilidade	Requisitos e design de disponibilidade, monitorização e relatórios, não disponibilidade, testes de planos de disponibilidade e gestão de alterações.	Colaboradores responsáveis por projetar sistemas e gerir a prestação de serviços
Política de Conformidade de IP e Direitos de Autor	Proteção da propriedade intelectual, da lei, das penalizações e do cumprimento das licenças de software.	Todos os Colaboradores
Política de Retenção e Proteção de Registos	Período de retenção para tipos específicos de registos, utilização de encriptação, seleção de suportes, recuperação, destruição e revisão de registos.	Colaboradores responsáveis pela criação e gestão de registos
Política de Privacidade e Proteção de Dados Pessoais	Legislação, definições e requisitos de proteção de dados aplicáveis.	Colaboradores responsáveis pela conceção e gestão de sistemas que utilizam dados pessoais
Política de Clear Desk e Clear Screen	Segurança da informação exibida em ecrãs, impressa e armazenada em suporte removível.	Todos os Colaboradores
Política de Redes Sociais	Orientações sobre como as redes sociais devem ser utilizadas ao representar a organização e ao discutir questões relevantes para a organização.	Todos os Colaboradores
Política de Segurança de RH	Recrutamento, contratos de trabalho, cumprimento de políticas, processo disciplinar, rescisão.	Todos os Colaboradores

TÍTULO DA POLÍTICA	ÁREAS ABORDADAS	PÚBLICO-ALVO
Política de Utilização Aceitável	Compromisso dos colaboradores com as políticas organizacionais de segurança da informação.	Todos os Colaboradores
Política de Gestão de Ativos	Este documento estabelece as regras sobre a forma como os ativos devem ser geridos do ponto de vista da segurança da informação.	Todos os Colaboradores
Política de Gestão de Configuração	A configuração segura de hardware, software, serviços e redes.	Colaboradores responsáveis por conceber sistemas e gerir a prestação de serviços
Política de Eliminação de Informação	A eliminação da informação armazenada nos sistemas de informação, dispositivos ou em qualquer outro suporte de armazenamento, quando já não é necessária.	Colaboradores responsáveis pela conceção e gestão de sistemas que utilizam dados pessoais
Política de Data Masking	A utilização de técnicas de mascaramento de dados, como o anonimato e a pseudonimização, para proteger a informação de identificação pessoal (PII).	Colaboradores responsáveis pela conceção e gestão de sistemas que utilizam dados pessoais
Política de Prevenção de Fugas de Dados	A configuração de ferramentas de software relevantes para detetar e prevenir a fuga de dados.	Colaboradores responsáveis por projetar sistemas e gerir a prestação de serviços
Política de Monitorização	A monitorização do ambiente TIC para detetar atividades anómalas.	Colaboradores responsáveis por projetar sistemas e gerir a prestação de serviços
Política de Web Filtering	Restringir o acesso a sites da Internet considerados inadequados.	Colaboradores responsáveis por projetar sistemas e gerir a prestação de serviços
Política de Coding Seguro	Os princípios que serão utilizados ao desenvolver código seguro.	Colaboradores responsáveis por projetar, gerir e escrever código para desenvolvimentos de software sob medida
Política de Threat Intelligence	A recolha e utilização de informações sobre ameaças nos níveis estratégico, tático e operacional.	Colaboradores responsáveis por proteger a infraestrutura da organização contra ataques
Política de Denúncias (Whistleblowing)	A comunicação de questões sobre a segurança da informação e/ou violações do código de conduta e ética da organização.	Todos os Colaboradores e outras partes interessadas

Tabela 1: Conjunto de políticas incluídas no SGSI

2.9 Aplicação da política de segurança da informação

As declarações políticas feitas neste documento e no conjunto de políticas de apoio listadas na Tabela 1 foram revistas e aprovadas pela Gestão de topo da AMT Consulting e devem ser

cumpridas. O não cumprimento por parte de um colaborador destas políticas pode resultar na tomada de medidas disciplinares de acordo com o *Processo Disciplinar* em vigor.

As dúvidas relacionadas com qualquer política da AMT Consulting devem ser encaminhadas em primeira instância para o gestor direto do colaborador.

3 Áreas da norma abordadas

As seguintes áreas da norma ISO/IEC 27001 são abordadas por este documento:

- 5 Liderança
  - 5.1 Liderança e compromisso
  - 5.2 Política
- A.5 Controlos organizacionais
  - A.5.1 Políticas de segurança da informação

4 Frequência de revisão

Este documento é revisto no âmbito de um exercício anual que abrange também documentos importantes, como a avaliação de riscos e o plano de formação e/ou após mudanças significativas na organização.