[logotipo da organização]

[nome da organização]

POLÍTICA DE SEGURANÇA DE TI

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Commented [AES1]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

Commented [AES2]: Para aprender mais sobre a estrutura deste documento, leia este artigo:

Como estruturar os documentos para os controles do Anexo A da ISO 27001
https://advisera.com/27001academy/pt-br/blog/2014/11/04/como-estruturar-os-documentos-para-os-controles-anexo-da-iso-27001/

Commented [AES3]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. Finalidade, escopo e usuários

A finalidade deste documento é definir regras claras para o uso aceitável do sistema de informações e outros ativos de informações na [nome da organização].

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a todos os ativos de informações e sistemas de informações usados no escopo do SGSI.

Os usuários deste documento são todos os funcionários da [nome da organização].

Commented [AES4]: Inclua o nome da sua organização.

Commented [AES5]: Inclua o nome da sua organização.

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.9, A.5.10, A.5.11, A.5.14, A.5.17, A.5.32, A.6.7, A.7.7, A.7.9, A.7.10, A.8.1, A.8.7, A.8.10, A.8.12, A.8.13, A.8.19 e A.8.23
- Política da segurança da informação
- [Política de classificação da informação]
- [Procedimento de gestão de incidentes]
- [Inventário de ativos]
- [Procedimentos de segurança para o departamento de TI]
- [Política de transferência de informações]

Commented [AES6]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

Commented [AES7]: Você pode encontrar modelos para estes documentos na pasta "09_Anexo_A_Controles_de_seguranca" do Kit de documentação ISO 27001.

3. Uso aceitável dos ativos de informações

Commented [AES8]: A medida em que cada um dos itens listados é necessário deve ser com base nos resultados da avaliação de riscos.

3.1. Definições

Sistema de informações – inclui todos os servidores e clientes, a infraestrutura da rede, o suporte ao programa de aplicativos e ao sistema, os dados e outros subsistemas e componentes de computador de propriedade de ou usados pela organização ou que estão sob responsabilidade da organização. O uso de um sistema de informações também inclui o uso de serviços internos ou externos, como o acesso à Internet, o e-mail, etc.

[illegible]

3.2. Uso aceitável

Os ativos de informações só podem ser usadas para as necessidades comerciais com a finalidade de [illegible]

3.3. Responsabilidade pelos ativos

Commented [AES9]: Exclua este seção se o controle A.5.9 [illegible]

Todos os ativos de informações possuem um proprietário designado no Inventário de ativos. [illegible]

3.4. Exclusão de informações

Quando não for mais necessário, o proprietário do ativo deve excluir as informações confidenciais [illegible]

3.5. Atividades proibidas

É proibido usar os ativos de informações de forma que consuma capacidade de forma desnecessário, enfraqueça o desempenho do sistema de informações ou represente uma ameaça à segurança. Também é proibido:

- fazer download de arquivos de imagem ou vídeo sem finalidade comercial, enviar correntes por e-mail, jogar, etc.
- instalar softwares em um computador local sem a permissão explícita de [cargo]
- usar aplicativos Java, controle Active X e outros códigos móveis, exceto quando autorizado por [cargo]
- [illegible]
- [illegible]
- [illegible]

3.6. Retirada de ativos do local

Os equipamentos, as informações ou os softwares, independente de suas formas ou meio de armazenamento, não podem ser retirados do local sem permissão prévia por escrito de [cargo].

[illegible]

3.7. Devolução de ativos no encerramento do contrato

Mediante o encerramento de um contrato de atividade ou outro tipo de contrato em relação ao uso de diversos equipamentos, [illegible]

3.8. Procedimento para cópias de segurança

O usuário deve [especifique o método de procedimento para cópia de segurança] todas as [illegible]

3.9. Proteção por antivírus/antimalware

O [nome do antivírus/antimalware] deve estar instalado em todos os computadores com [illegible]

3.10. Autorizações para uso do sistema de informações

Commented [AES10]: Exclua este seção se o controle A.8.10 [illegible]

Commented [AES11]: Trecho a ser excluído se o controle [illegible]

Commented [AES12]: Trecho a ser excluído se essa Política [illegible]

Commented [AES13]: Exclua este seção se o controle A.7.10 [illegible]

Commented [AES14]: Pode ser especificado se essa permissão [illegible]

Commented [AES15]: Exclua este seção se o controle A.5.11 [illegible]

Commented [AES16]: Exclua este seção se o controle A.8.13 [illegible]

Commented [AES17]: Ajuste a frequência com base nos [illegible]

Commented [AES18]: Para saber mais sobre o assunto, leia este artigo: [illegible]

Commented [AES19]: Certifique-se de que isso não interfira [illegible]

Commented [AES20]: Exclua este seção se o controle A.8.7 [illegible]

Os usuários do sistema de informações só podem acessar esses ativos do sistema de informações para o qual obtiveram autorização explícita do proprietário do ativo.

[illegible]

[illegible]

3.11. Responsabilidades da conta dos usuários

O usuário não deve, direta ou indiretamente, permitir que outras pessoas usem seus direitos de acesso, isto é, nome de usuário, e não deve usar o nome de usuário e/ou a senha de outra pessoa. O uso de nomes de grupos é proibido.

[illegible]

3.12. Responsabilidades de senhas

Os usuários devem aplicar as seguintes boas práticas de segurança ao selecionar e usar senhas:

- as senhas não devem ser divulgadas a outras pessoas, incluindo a gestão e os administradores do sistema
- as senhas não devem ser escritas a menos quê um método de segurança tenha sido aplicado por [cargo]
- [illegible]
- [illegible]
- senhas fortes devem ser selecionadas da seguinte forma:
  - use pelo menos 16 caracteres
  - use pelo menos um caractere numérico
  - [illegible]
  - [illegible]
  - uma senha não deve ser uma palavra registrada em dicionário ou que faça parte de um dialeto ou jargão de qualquer idioma, nem qualquer uma dessas palavras escrita ao contrário
  - as senhas não devem ser baseadas em dados pessoais (por exemplo, data de nascimento, endereço, nome de um membro da família, etc.)
  - [illegible]
- as senhas devem ser alteradas a cada três meses
- a senha deve ser alterada no ato da primeira entrada no sistema
- [illegible]
- [illegible]

3.13. Política de mesa limpa e tela limpa

Commented [AES21]: Trecho a ser excluído se o controle [illegible]

Commented [AES22]: Exclua este seção se a Política de senhas [illegible]

Commented [AES23]: Exclua este seção se o controle A.5.17 [illegible]

Commented [AES24]: Exclua este item se a Política de mesa [illegible]

Commented [AES25]: Para saber mais sobre o assunto, leia este artigo:

[illegible]

Todas as informações classificadas como "Uso interno", "Restrito" ou "Confidencial", [illegible]

3.13.1. *Política de mesa limpa*

Commented [AES26]: Exclua este seção se o controle A.7.7 [illegible]

Se a pessoa autorizada não estiver no local de trabalho, todos os documentos em papel, bem como dispositivos móveis (endpoints), e todas as mídias de armazenamento de dados classificadas como confidenciais devem ser removidas da mesa ou de outros locais (impressoras, máquinas de fax, copiadoras, etc.) para evitar o acesso não autorizado.

[illegible]

Commented [AES27]: Altere esta referência para [illegible]

3.13.2. *Política de tela limpa*

Commented [AES28]: Exclua todo este item se os controles [illegible]

Commented [AES29]: Exclua este seção se o controle A.7.7 [illegible]

Se a pessoa autorizada não estiver no local de trabalho, todas as informações confidenciais devem ser removidas da tela e o acesso deve ser negado a todos os sistemas aos quais essa pessoa possui autorização de acesso.

[illegible]

Commented [AES30]: Adapte ao sistema usado na [illegible]

As informações nos quadros brancos (por exemplo, aquelas disponíveis nas salas de reunião) devem ser apagadas quando não forem mais necessárias.

3.13.3. *Proteção de instalações e equipamentos compartilhados*

Commented [AES31]: Exclua este seção se o controle A.8.1 [illegible]

Os documentos que contêm informações confidenciais devem ser removidos imediatamente de impressoras, máquinas de fax e copiadoras.

[illegible]

Commented [AES32]: Por exemplo, pelo trancamento da instalação, etc.

[illegible]

Commented [AES33]: Por exemplo, pelo trancamento da instalação, etc.

O uso não autorizado de impressoras, copiadoras, escâneres e outros equipamentos compartilhados para cópias [especifique as máquinas e seus locais] é evitado [especifique como].

Commented [AES34]: Por exemplo, pelo trancamento da [illegible]

[illegible]

Commented [AES35]: Por exemplo, mais de duas semanas.

Commented [AES36]: Inclua o nome da sua organização.

3.14. Uso da Internet

A Internet pode ser acessada somente por meio da rede local da organização com a infraestrutura adequada e proteção do firewall. O acesso direto à Internet por meio de modem, acesso móvel à Internet, redes sem fio ou outros dispositivos de acesso direto à Internet é proibido.

[redacted]

O usuário deve considerar todas as informações recebidas através de sites não confiáveis. Essas informações só podem ser usadas com finalidades comerciais depois que a sua autenticidade e precisão tiverem sido verificadas.

[redacted]

3.15. E-mail e outros métodos de troca de mensagens

Os métodos de troca de mensagens além da correspondência eletrônica incluem download de arquivos da Internet, transferência de dados via [forneça nomes de sistemas de comunicação especializados], telefones, máquinas de fax, envio de mensagens de texto por SMS, mídias portáteis, fóruns e redes sociais.

[redacted]

Os usuários só podem enviar mensagens que contenham informações verdadeiras. É proibido enviar materiais com conteúdo importuno, desagradável, sexualmente explícito, rude, difamador ou de qualquer outra forma inaceitável ou ilegal. Os usuários não devem enviar spam para pessoas com as quais não tenham relações comerciais ou que não solicitaram a informação em questão.

Caso um usuário receba um e-mail de spam, ele/ela devem informar o [cargo].

[redacted]

O usuário deve salvar todas as mensagens que contenham dados importantes para os negócios da organização com o uso do método especificado pelo [cargo].

[redacted]

Commented [AES37]: Exclua este seção se o controle A.5.12 [redacted]

Commented [AES38]: A mídia em questão deve ser [redacted]

Commented [AES39]: Os fóruns e as redes sociais em questão [redacted]

Commented [AES40]: Trecho a ser excluído se essa Política [redacted]

3.16. Direitos autorais

Os usuários não devem copiar o software de propriedade da organização sem autorização, exceto em casos permitidos pela lei, pelo proprietário ou pelo [cargo].

Os usuários não devem copiar o software ou outros materiais originais de outras fontes e são responsáveis por todas as consequências que possam surgir de acordo com a lei de propriedade intelectual.

3.17. Computação móvel

3.17.1. Introdução

Os equipamentos de computação móvel incluem todos os tipos de computadores portáteis, celulares, smartphones, cartões de memória e outros equipamentos móveis usados para armazenar, processar e transferir dados, independentemente de onde tal equipamento é utilizado.

Os equipamentos acima mencionados podem ser retirados do local somente após a obtenção de autorização de acordo com a seção 3.6 desta política – Retirada de ativos das instalações.

3.17.2. Regras básicas

Deve tomar-se cuidados especiais quando o equipamento de computação móvel estiver em veículos (incluindo carros), espaços públicos, quartos de hotel, locais de reuniões, centros de conferência e outras áreas não protegidas fora das instalações da organização.

A pessoa que levar equipamentos de computação móvel para fora das instalações deve seguir essas regras:

- os equipamentos de computação móvel que contiverem informações importantes, confidenciais ou críticas não devem ser deixados sem supervisão e, se possível, devem ser trancados fisicamente. Também é possível usar travas espaciais para garantir a segurança do equipamento
- ao usar equipamentos de computação móvel em locais públicos, o usuário deve tomar cuidado para que os dados nãoo sejam lidos pelas pessoas não autorizadas
- as atualizações de patches e outras configurações do sistema são realizadas [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- a proteção contra código malicioso é instalada e atualizada [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- a pessoa que usa equipamentos de computação móvel fora das instalações é responsável por criar cópias de segurança dos dados periodicamente [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- a conexão com as redes de comunicação deve ser realizada [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- as informações em computadores portáteis devem ser criptografadas [especifique como isso é implementado tecnicamente ou faça referência a um documento que define o processo]
- a proteção de dados confidenciais deve ser implementada de acordo com a [Política de classificação de informações]

Commented [AES41]: Exclua este seção se o controle A.5.32 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES42]: Exclua este seção se o controle A.8.1 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES43]: Exclua este seção se a Política de Segurança Móvel, Teletrabalho e Trabalho em Home Office estiver descrita em um documento separado.

Commented [AES44]: Exclua este parágrafo se o controle A.7.10 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES45]: Trecho a ser excluído se o controle A.7.9 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES46]: Ex.: acesso semanal ao servidor da

Commented [AES47]: Ex.: obrigando a instalação da

Commented [AES48]: Ex.: acessando a rede da organização e

Commented [AES49]: Por exemplo, estabelecendo um canal

Commented [AES50]: Especifique o tipo de informação armazenada em computadores portáteis que deve ser criptografada de acordo com as práticas da sua organização.

Por exemplo, discos rígidos internos, arquivos confidenciais, arquivos específicos como confidenciais, etc.

Commented [AES51]: Por exemplo, por meio de criptografia de disco inteiro, criptografia de arquivo ou criptografia de compartimento.

Commented [AES52]: Caso sua organização não possua uma

- a pessoa que usa equipamento de computação móvel fora do local deve observar as instruções do fabricante em relação à proteção do equipamento (por exemplo, contra condições climáticas, exposição a interferência eletromagnética, vibração física, etc.)
- [illegible]

O [cargo] é responsável pelo treinamento e pela conscientização de pessoas que usam equipamentos de computação móveis fora das instalações da organização.

3.18. Teletrabalho e trabalho em home office

3.18.1. Introdução

Teletrabalho significa que equipamentos de informação e comunicação são usados para permitir que os usuários trabalhem fora da organização, incluindo a trabalho em home office. O teletrabalho não inclui o uso de celulares fora das instalações da organização.

[illegible]

3.18.2. Regras adicionais para teletrabalho

Todas as pessoas que realizam teletrabalho devem seguir as regras para computação móvel definidas na seção 3.17 deste documento e as regras definidas abaixo:

- o local físico onde é realizado o teletrabalho deve ser protegido por [especifique como é feita a implementação técnica ou faça referência a um documento que define o processo]
- no mínimo, as pessoas que realizam teletrabalho devem ter [liste aqui as configurações mínimas necessárias para o teletrabalho]
- [illegible]
- a devolução de dados e equipamentos em caso de rescisão do contrato de trabalho deve ser implementada de acordo com a seção 3.7 desta Política
- as atividades especificamente proibidas para funcionários que realizam teletrabalho são: [enumerar aqui as atividades expressamente proibidas aos colaboradores no exercício do teletrabalho]
- [illegible]

3.19. Monitoramento do uso dos sistemas de informação e comunicação

Todos os dados que são criados, armazenados, enviados ou recebidos por meio de sistemas de informações ou outros sistemas de comunicação da organização,incluindo diversos aplicativos,e-mails, fax, etc., sejam informações pessoais ou não, são consideradas de propriedade da [nome da organização].

Commented [AES53]: A ser excluído caso o uso de dispositivos [illegible]

Commented [AES54]: Se sua organização não possui uma [illegible]

Commented [AES55]: Você pode usar o seguinte treinamento de conscientização de segurança para treinar seus funcionários: [illegible]

Commented [AES56]: Para saber mais sobre o assunto, leia este artigo: [illegible]

Commented [AES57]: Exclua este seção se a Política de [illegible]

Commented [AES58]: Exclua este seção se o controle A.6.7 [illegible]

Commented [AES59]: A autorização pode ser concedida [illegible]

Commented [AES60]: Exemplos de elementos a serem usados são:
- prevenção do acesso não autorizado de residentes, transeuntes, etc., pela utilização de salas e gabinetes com fechaduras, não funcionamento em espaços partilhados, layouts que impeçam a visualização ou audição de informação por terceiros, etc.
[illegible]

Commented [AES61]: Por exemplo, fonte de alimentação [illegible]

Commented [AES62]: Caso a Política de mesa limpa e tela [illegible]

Commented [AES63]: Caso sua organização não possua uma [illegible]

Commented [AES64]: Por exemplo, participar de reuniões com [illegible]

Commented [AES65]: Você pode excluir este texto se não [illegible]

Commented [AES66]: Por exemplo, alterar configurações em [illegible]

Commented [AES67]: Você pode excluir este texto se não [illegible]

Commented [AES68]: Inclua o nome da sua organização.

Os usuários concordam que as pessoas autorizadas da organização podem acessar todos esses dados e que o acesso feito por essas pessoas não será considerado uma violação à privacidade dos usuários.

A organização pode usar ferramentas especializadas com a finalidade de identificar e bloquear métodos proibidos de comunicação e filtrar conteúdo proibido.

3.20. Incidentes

Todo funcionário, fornecedor ou terceiro que esteja em contato com os dados e/ou sistemas da [nome da organização] deve informar quaisquer fragilidades, incidentes ou eventos que indiquem um possível incidente conforme o Procedimento de gestão de incidentes.

Commented [AES69]: Inclua o nome da sua organização.

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*	*Responsável pelo armazenamento*	*Controles para proteção do registro*	*Tempo de retenção*
[Autorizações para instalação de software, uso de aplicativos Java e controles Active X, uso de ferramentas criptográficas, download de código de programa de mídias externas, instalação de dispositivos periféricos] – formato eletrônico	[pasta na intranet]	[cargo]	Os registros não podem ser editados; somente o [cargo] tem o direito de armazenar esses registro.	Os registros são armazenados por três anos.
[Autorização para retirar os ativos de rede] – formato eletrônico	[pasta na intranet]	[cargo]	Os registros não podem ser editados; somente o [cargo] tem o direito de armazenar esses registro.	Os registros são armazenados por três anos.
[Autorização de acesso a determinadas páginas de internet] – formato eletrônico	[pasta na intranet]	[cargo]	Os registros não podem ser editados; somente o [cargo] tem o direito de	Os registros são armazenados por três anos.

Commented [AES70]: Ajuste conforme adequado.

			[redacted]	
[Decisão sobre como os tipos de dados podem ser trocados] – formato eletrônico	[pasta na intranet]	[cargo]	Os registros não podem ser editados; somente o [cargo] tem o direito de armazenar esses registro.	Os registros são armazenados por três anos.
[Decisão sobre como as mensagens que contêm dados importantes para os negócios devem ser armazenadas] – formato eletrônico	[pasta na intranet]	[cargo]	Os registros não podem ser editados; somente o [cargo] tem o direito de armazenar esses registro.	Os registros são armazenados por três anos.
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Somente o [cargo] pode conceder aos demais funcionários o acesso a qualquer um dos documentos mencionados acima.

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

[redacted]

Commented [AES71]: Isso é apenas uma recomendação; [redacted]

Ao avaliar a eficácia e a adequação deste documento, os seguintes critérios devem ser considerados:

- quantidade de incidentes relacionados ao uso não aceitável ou não autorizado de ativos de informações
- [redacted]

[cargo]

[nome]

_____

[assinatura]

Commented [AES72]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.