[logotipo da organização]

[nome da organização]

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

PROCEDIMENTOS DE SEGURANÇA PARA O DEPARTAMENTO DE TI

Commented [AES2]: Partes deste documento que precisam ser especificadas com mais detalhes podem ser elaboradas em documentos separados (políticas/procedimentos).

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

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 garantir o funcionamento correto e seguro tecnologia de informação e comunicação.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação (SGSI), isto é, a toda a tecnologia de informação e comunicação do escopo e a toda a documentação que faz parte do escopo.

Os usuários deste documentos são funcionários da [unidade organizacional da tecnologia de informação e comunicação].

2. Documentos de referência

- Norma ISO/IEC 27001, cláusulas A.5.7, A.5.14, A.5.37, A.7.10, A.7.14, A.8.4, A.8.6, A.8.7, A.8.8, A.8.9, A.8.10, A.8.12, A.8.13, A.8.15, A.8.16, A.8.17, A.8.18, A.8.20, A.8.21, A.8.22, A.8.23, A.8.31 e A.8.32
- Política de segurança da informação
- [Plano de recuperação de desastre]
- [Política de dispositivo móvel, teletrabalho e trabalho em home office]
- [Política de classificação da informação]
- [Inventário de ativos]
- [Política de segurança do fornecedor]
- [Política de desenvolvimento seguro]
- [Política de controle de acesso]

Commented [AES4]: Você pode encontrar um modelo para este documento na pasta "05_Politicas_gerais" do Kit de documentação ISO 27001.

3. Procedimentos operacionais para tecnologia da informação e comunicação

3.1. Gestão de mudanças

Todas as mudanças feitas nos sistemas operacionais ou de produção devem ser feitas da seguinte forma:

1. as mudanças podem ser propostas por [especifique os cargos]
2. as mudanças devem ser autorizadas pelo [cargo], que deve avaliar a sua justificativa de negócio e potenciais impactos negativos de segurança
3. as mudanças podem ser implementadas pelo [cargo]
4. o [cargo] é responsável por verificar se todas as mudanças foram implementadas de acordo com a solicitação
5. o [cargo] é responsável por testar e verificar a estabilidade do sistema – o sistema não deve ser colocado em produção antes que todos os testes estejam concluídos
6. a implementação das mudanças deve ser informada para [relacione os cargos que devem ser informados]

Commented [AES5]: Exclua este seção se o controle A.8.32

Commented [AES6]: Para mais informações sobre este tema, leia este artigo:

Commented [AES7]: Exclua este seção se a Política de gestão

Commented [AES8]: É possível especificar quais mudanças são

Commented [AES9]: Outra forma de elaborar as etapas pode

7. o [cargo] é responsável por atualizar todos os documentos (políticas, procedimentos, planos, etc.) que foram afetados pela mudança

Os registros de mudanças são mantidos [forneça o nome do formato ou descreva outro método para registro das mudanças].

3.2. Gestão de configuração

O [cargo] é responsável por documentar as definições de configuração de hardware, software, serviços e redes que devem ser aplicadas para garantir a operação correta e segura e para fornecer uma linha de base contra alterações incorretas.

3.3. Gestão de capacidade

O [cargo] é responsável por monitorar o uso de ativos de TIC e por planejar a capacidade necessária.

3.4. Proteção de antivírus/antimalware

[Nome do software de antivírus] deve ser instalado em cada plataforma (por exemplo, servidores físicos, virtuais ou em nuvem) fornecendo sistemas de TI administrados pelo departamento de TI, com atualizações automáticas ativadas.

3.5. Cópias de segurança

3.5.1. Procedimento para cópias de segurança

As cópias de segurança devem ser criadas por todos os sistemas identificados na [Estratégia de continuidade de negócios] e com a frequência especificada no mesmo documento.

O [cargo] é responsável pelo processo de criação de cópias de segurança de informações, software e imagens do sistema, e para garantir que os fatores nos cópias de segurança agendados sejam tratados adequadamente. [se necessário, descreva a tecnologia usada para a criação de cópias de segurança, especifique as responsabilidades das atividades, os locais de armazenamento dessas cópias de segurança, a sua proteção física, criptografia, senhas, etc.]

Os registros do processo de criação de cópias de segurança são criados automaticamente nos sistemas em que as cópias de segurança são feitas.

3.5.2. Teste das cópias de segurança

As cópias de segurança e o processo de restauração dessas cópias devem ser testados pelo menos [uma vez a cada três meses] com a implementação do processo de restauração de dados no [identifique o servidor em que a restauração dos dados é realizada] e a verificação de que todos os dados tenham sido recuperados.

O [cargo] é responsável pelo teste das cópias de segurança. Os registros dos testes das cópias de segurança são mantidos [descreva o formulário de registro – em papel ou formato eletrônico, se há um formato indicado, etc.].

Commented [AES10]: Exclua este seção se o controle A.8.20 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES11]: Exclua este seção se o controle A.8.6 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES12]: Exclua este seção se o controle A.8.7 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES13]: Exclua este seção se o controle A.8.13 estiver marcado como "Não aplicável" na Declaração de aplicabilidade.

Commented [AES14]: Exclua este seção se a Política de cópias de segurança [link] for um documento separado.

Commented [AES15]: Para mais informações sobre este tema, leia este artigo:

[link]

Commented [AES16]: Caso este documento não exista, todos os detalhes que requerem cópia de segurança devem ser listados aqui, por exemplo na tabela de cópias de segurança.

Commented [AES17]: As cópias de segurança devem ser armazenadas em local diverso (algo diferente do localização principal) para que de caso afetado ou um desastre.

Commented [AES18]: Ajuste a frequência de acordo com os seus padrões.

3.6. Gestão da segurança em redes

O [cargo] é responsável pela gestão e pelo controle de redes de computadores, por garantir a segurança das informações nas redes, prevenir vazamento de dados, e por proteger os serviços conectados à rede contra o acesso não autorizado. Portanto, é necessário:

- separar a responsabilidade operacional das redes da responsabilidades por aplicativos confidenciais e outros sistemas
- para proteger os dados confidenciais contra transmissão para uma rede pública por parte de [descreva a tecnologia usada para proteção e especifique as responsabilidades e os responsáveis]
- [redacted]
- segregar a rede por [descrever quais segmentos da rede são segregados; descreva se a segregação é física ou lógica]
- separar os ambientes de desenvolvimento, teste e sistemas operacionais
- [redacted]
- para filtrar o acesso a sites com conteúdo potencialmente malicioso ou ilegal, ou que podem ser usados para vazamento de dados
- [redacted]

O [cargo] deve monitore e testar periodicamente os controles implementados.

3.7. Serviços de rede

O [cargo] deve definir os recursos de segurança e o nível dos serviços esperados para todos os serviços de rede, sejam eles fornecidos internamente ou por meio de terceirização. Esses requisitos devem ser documentados com os fornecedores de serviços.

[redacted]

3.8. Exclusão de dados

Todos os dados armazenados em aplicativos, bancos de dados, servidores e redes devem ser excluídos pelo proprietário do ativo quando não forem mais necessários.

[redacted]

Commented [AES19]: Exclua este seção se o controle A.8.20 [redacted]

Commented [AES20]: Para obter mais informações sobre este tópico, leia estes artigos:

• Como gerenciar a segurança de rede de acordo com a ISO 27001 https://advisera.com/27001academy/pt-br/blog/2016/06/29/como-gerenciar-a-seguranca-de-rede-de-acordo-com-como-controle-a-13-1-da-iso-27001/

[redacted]

• Usando Sistemas de Detecção de Intrusão e Honeypots para atender controles de rede https://advisera.com/27001academy/pt-br/blog/2016/07/11/usando-sistemas-de-deteccao-de-intrusao-e-honeypots-para-atender-controles-de-rede-da-clausula-a-13-1-1-da-iso-27001/

[redacted]

Commented [AES21]: Ou refira-se à Política de dispositivo [redacted]

Commented [AES22]: A frequência pode ser especificada; por [redacted]

Commented [AES23]: Os controles podem ser especificados; por [redacted]

Commented [AES24]: Exclua este seção se o controle A.8.10 [redacted]

Commented [AES25]: Por exemplo, listar ferramentas [redacted]

3.9. Descarte e destruição de equipamentos e mídias

Todos os dados e os softwares licenciados armazenados em mídias de armazenamento móvel (por exemplo, em CD, DVD, pen drive USB, cartão de memória, etc., e também em papel) e em todos os equipamentos que contenham mídias de armazenamento (por exemplo, computadores, celulares, etc.) devem ser apagados ou a mídia deve ser destruída antes de ser descartada ou reutilizada.

3.9.1. Equipamentos

O [cargo] é responsável por verificar e apagar os dados dos equipamentos, a menos que outro procedimento seja indicado na Política de classificação da informação. [descreva a tecnologia usada para apagar dados de mídias nos equipan

3.9.2. Mídia de armazenamento móvel

O [cargo] é responsável por apagar os dados das mídias de armazenamento móvel, a menos que outro procedimento seja indicado na Política de classificação da informação.

3.9.3. Mídia em papel

Os funcionários da organização que gerem documentos são responsáveis por destruir mídias em papel, a menos que outro procedimento seja indicado na Política de classificação da informação.

3.9.4. Eliminação e destruição de registros; comissão de destruição de dados

Os registros de eliminação/destruição devem ser mantidos para todos os dados classificados como "Restritos" e "Confidenciais". Os registros devem incluir as seguintes informações: informações sobre a mídia, data de eliminação/destruição, método de eliminação/destruição, pessoa que realizou o processo.

3.10. Transferência de informações

3.10.1. Canais de comunicação eletrônica

As informações da organização devem ser trocadas por meio dos seguintes canais de comunicação eletrônica: e-mail, download de arquivos da Internet, transferência de dados via [forneça nomes de

Commented [AES26]: Exclua este seção se o controle A.7.10 e

Commented [AES27]: Exclua este seção se a Política de

Commented [AES28]: Para mais informações sobre este tema, leia este artigo:

Commented [AES29]: Pode-se explicar que isso significa

Commented [AES30]: Pode-se explicar que isso significa

Commented [AES31]: Exclua este texto se o controle A.5.9

Commented [AES32]: Exclua este texto se o controle A.7.14

Commented [AES33]: Trecho a ser excluído se essa Política

Commented [AES34]: Por exemplo, liste as ferramentas

Commented [AES35]: Pode ser, por exemplo, o disco rígido de

Commented [AES36]: Exclua este texto se o controle A.7.10

Commented [AES37]: Trecho a ser excluído se essa Política

Commented [AES38]: Exclua este texto se o controle A.8.10

Commented [AES39]: Trecho a ser excluído se essa Política

Commented [AES40]: Ou especifique outra tecnologia.

Commented [AES41]: Adapte os níveis de confidencialidade

Commented [AES42]: Exclua este seção se a Política de

Commented [AES43]: Exclua este seção se o controle A.5.14

sistemas de comunicação especializados], telefones, máquinas de fax, envio de mensagens de texto por SMS, mídias portáteis, fóruns e redes sociais.

[redacted]

Além dos controles descritos pela Política de classificação da informação, o [cargo] descreve outros controles para cada tipo de dados e canal de comunicação com base nos resultados da avaliação de riscos.

3.10.2. Relações com partes externas

Partes externas incluem os diversos fornecedores de serviços, empresas de manutenção de hardware e software, empresas que gerenciam transações ou processamentos de dados, clientes, etc.

O [cargo] deve preparar e assinar um acordo com a parte externa antes de trocar informações e/ou softwares, por meios eletrônicos, físicos ou verbais. O contrato pode estar em papel ou formato eletrônico (por exemplo, um contrato sobre termos e condições gerais) e deve conter cláusulas que estejam de acordo com a avaliação de riscos, incluindo, no mínimo:

- o método de identificação do terceiro
- as autorizações para acesso às informações
- a garantia de não repúdio
- [redacted]

Acordos com as partes externas precisam ser definidos de acordo com a [Política de segurança do fornecedor].

3.11. Tratamento de código fonte

O código fonte de programa é armazenado [redacted]

3.12. Uso de programa utilitários

O [cargo] é responsável por aprovar requisições para uso de [redacted]

3.13. Monitoramento do sistema

Com base nos resultados da avaliação de riscos, o [cargo] decide quais registros serão mantidos em quais sistemas e para quais sistemas e por quanto tempo eles serão armazenados. [redacted]

Commented [AES44]: A mídia em questão deve ser especificada.

Commented [AES45]: Adicione ou exclua canais de [redacted]

Commented [AES46]: Os fóruns e as redes sociais em questão [redacted]

Commented [AES47]: Este texto pode ser substituído com a [redacted]

Commented [AES48]: Trecho a ser excluído se essa Política [redacted]

Commented [AES49]: Exclua este seção se o controle A.5.14 [redacted]

Commented [AES50]: Exclua este seção se o controle A.8.4 [redacted]

Commented [AES51]: Por exemplo, usando GitHub, Bitbucket, [redacted]

Commented [AES52]: Exclua este seção se o controle A.8.18 [redacted]

Commented [AES53]: Um programa utilitário privilegiado é qualquer aplicativo capaz de alterar ou contornar configurações de segurança (por exemplo, permite que o usuário desligue um recurso de segurança ou acesse um arquivo ao qual ele normalmente não tem acesso).

[redacted]

Commented [AES54]: Os registros podem incluir atividades de [redacted]

Commented [AES55]: Exclua este texto se o controle A.8.15 [redacted]

O [cargo] é responsável por monitorar os registros das falhas informadas automaticamente todos os dias e por registrar as falhas informadas pelos usuários, analisar os erros ocorridos, para identificar novas ameaças potenciais, assim como um potencial para vazamento de dados, e tomar as ações corretivas adequadas. [autorizações específicas devem ser especificadas para as ações em caso de erro; a forma como o registro de erros é mantido também deve ser especificada]

O [cargo] é responsável por monitorar todas as vulnerabilidades de aplicativos e outros sistemas, e [cargo] deve selecionar ações a serem tomadas caso novas vulnerabilidades sejam identificadas.

O [cargo] é responsável por verificar os relatórios de testes de penetração realizados e avaliações de vulnerabilidade e tomar as ações corretivas apropriadas.

3.14. Monitoramento de ameaças externas

O [cargo] é responsável por monitorar fornecedores, fabricantes e grupos de referência de segurança

Commented [AES56]: Exclua este texto se o controle A.5.7

Commented [AES57]: Exclua este texto se o controle A.8.12

Commented [AES58]: Exclua este texto se o controle A.8.15

Commented [AES59]: É possível especificar se isso inclui, por

Commented [AES60]: Exclua este texto se o controle A.5.7

Commented [AES61]: Exclua este texto se o controle A.8.12

Commented [AES62]: Se necessário, deve-se fornecer mais

Commented [AES63]: Exclua este texto se o controle A.8.15

Commented [AES64]: Exclua este texto se o controle A.8.8

Commented [AES65]: Exclua este seção se o controle A.5.7

4. Gestão de registros mantidos de acordo com este documento

Nome do registro	*Local de armazenamento*			
[Nome do registro de mudança] – em formato eletrônico	[nome da pasta na intranet]			
[Decisões sobre os canais de comunicação usados para determinados tipos de informações, restrições e atividades	[nome da pasta na intranet]			

Commented [AES66]: Altere esses registros para combinar

proibidas] – formato eletrônico				
[Registros do processo de criação de cópias de segurança] – formato eletrônico	Sistema que executa o processo de criação de cópias de segurança	[cargo]	Os registros são somente leitura e não podem ser excluídos ou editados.	Os registros são armazenados por um ano.
[Registros de teste das cópias de segurança] – em papel ou formato eletrônico	[nome da pasta/do armário de armazenamento]	[cargo]	Somente o [cargo] tem o direito de acessar esses registros.	Os registros são armazenados por um ano.
[Recursos de segurança e nível esperado dos serviços para os serviços de rede] – em papel e formato eletrônico	Computador do [cargo], [nome da pasta / do armário de armazenamento]	[cargo]	Somente o [cargo] tem o direito de acessar esses registros.	Cinco anos após a expiração do contrato ou serviço fornecido.
[Registros de eliminação/destruição] – em formato de papel	[nome da pasta / do armário de armazenamento]	[cargo]	O armário é trancado e as chaves ficam em poder [cargos].	Os registros são armazenados por cinco anos.
[Registro da análise de registros] – em papel e formato eletrônico	Computador do [cargo], [nome da pasta / do armário de armazenamento]	[cargo]	Somente o [cargo] tem o direito de acessar esses registros.	Os registros são armazenados por cinco anos.

5. Validade e gestão de documentos

Este documento é válido a partir de [data].

O proprietário do documento é o [cargo], que deve verificar e, se necessário, atualizar o documento pelo menos [uma vez por ano].

Commented [AES67]: Isso é apenas uma recomendação; [texto ilegível]

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

- quantidade de incidentes relacionados ao funcionamento seguro dos sistemas de informação e comunicação
- [quantidade de incidentes em função de responsabilidades confusas para o funcionamento de sistemas de informações e comunicação]

[cargo]
[nome]

_____
[assinatura]

Commented [AES68]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.