Guia de implementação do SGSI

Plano de Projeto para os Requisitos da ISO-27001

[TEMPLATE ANPPD]

Nota de uso

Nota: O objetivo deste documento é ajudá-lo a reconhecer as atividades relacionadas ao estabelecimento de um SGSI. Este documento não deve ser considerado como consultoria profissional para estabelecer ou implementar um SGSI. O uso deste guia não garante uma implementação bem sucedida nem uma implementação pronta para certificação. Se você deseja implementar um SGSI, considere contratar um consultor profissional especializado na Implementação do SGSI.

Associação Nacional dos Profissionais de Privacidade de Dados

Índice

Visão geral de um SGSI

Segurança da informação é a proteção da informação para garantir:

- Confidencialidade: garantir que as informações sejam acessíveis apenas àqueles autorizados a acessá-las;
- Integridade: garantir que as informações sejam precisas e completas e não sejam modificadas sem autorização;
- Disponibilidade: garantir que as informações sejam acessíveis aos usuários autorizados, quando necessário.

A segurança da informação é alcançada através da aplicação de um conjunto adequado de controles (políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware).

Um **Sistema de Gerenciamento de Segurança da Informação (SGSI)** é uma maneira de proteger e gerenciar informações com base em uma abordagem sistemática do risco comercial para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação. É uma abordagem organizacional para segurança da informação.

A ISO/IEC publica dois padrões que se concentram no SGSI de uma organização:

- **O padrão do código de prática: ISO/IEC 27002:2013 (ISO / IEC 17799)**. Esse padrão pode ser usado como um ponto de partida para o desenvolvimento de um SGSI. Fornece orientações para o planejamento e implementação de um programa para proteger ativos de informações. Ele também fornece uma lista de controles (salvaguardas) que você pode considerar implementando como parte do seu SGSI.
- **O padrão do sistema de gerenciamento: ISO/IEC 27001:2013**. Esse padrão é a especificação para um SGSI. Explica como aplicar a ISO/IEC 27002:2013 (ISO / IEC 17799); Ele fornece o padrão contra o qual é realizada a certificação, incluindo uma lista dos documentos necessários. Uma organização que busca a certificação do seu SGSI é examinada em relação a esse padrão.

Esses padrões são protegidos por direitos autorais e devem ser adquiridos. (Para obter informações sobre compras, consulte seção 1, "Adquira uma cópia dos padrões ISO / IEC").

Os padrões estabelecem as seguintes práticas:

- Todas as atividades devem seguir um método. O método é arbitrário, mas deve ser bem definido e documentado;
- Uma empresa ou organização deve documentar seus próprios objetivos de segurança. Um auditor verificará se esses requisitos são cumpridos;

- Todas as medidas de segurança usadas no SGSI devem ser implementadas como resultado de uma análise de risco para eliminar ou reduzir os riscos a um nível aceitável;
- O padrão oferece um conjunto de controles de segurança. Cabe à organização escolher quais controles devem ser implementados com base nas necessidades específicas de seus negócios.
- Um processo deve garantir a verificação contínua de todos os elementos do sistema de segurança através de auditorias e revisões;
- Um processo deve garantir a melhoria contínua de todos os elementos do sistema de gerenciamento de informações e segurança. (A norma ISO/IEC 27001:2013 adota o modelo PDCA como base e espera que o modelo seja seguido em uma implementação do SGSI);

Essas práticas formam a estrutura na qual você estabelecerá um SGSI. As seções a seguir descrevem as etapas envolvidas no estabelecimento de um SGSI.

Nota: É importante lembrar que, embora este guia forneça exemplos, a implementação de um SGSI é baseado em processos e específico para sua organização. Considere usar o guia e exemplos como um ponto de partida para discussão na sua organização, e não como um conjunto de modelos.

1. Adquira uma cópia dos padrões ISO / IEC

Antes de estabelecer um SGSI e redigir os vários documentos para o SGSI, você deve adquirir cópias das normas ISO / IEC pertinentes, a saber:

O padrão do código de prática: ISO/IEC 27002:2013 (ISO / IEC17799). Esse padrão pode ser usado como ponto de partida para o desenvolvimento de um SGSI. Ele fornece orientação para o planejamento e implementação de um programa para proteger ativos de informação. Ele também fornece uma lista de controles (salvaguardas) que você pode considerar implementar como parte do seu SGSI.

O padrão do sistema de gerenciamento: ISO/IEC 27001:2013. Esse padrão é a especificação para um SGSI. Ele explica como aplicar a ISO/IEC 27002:2013 (ISO / IEC17799). Ele fornece o padrão contra o qual a certificação é realizada, incluindo uma lista dos documentos necessários. Uma organização que busca a certificação de seu SGSI é examinada conforme esse padrão.

Você pode adquirir esses padrões na seguinte loja on-line:

- A loja online da ANBT: https://www.abntcatalogo.com.br

2. Obtenha suporte de gerenciamento

Conforme descrito na ISO/IEC 27001:2013, o gerenciamento desempenha um papel importante no sucesso de um SGSI.

Do que você precisa: Seção de responsabilidade de gerenciamento da ISO/IEC 27001:2013.

A gerência deve se comprometer com o estabelecimento, implementação, operação, monitoramento, revisão, manutenção e aprimoramento do SGSI. O compromisso deve incluir atividades como garantir que os recursos adequados estejam disponíveis para trabalhar no SGSI e que todos os funcionários afetados pelo SGSI tenham a treinamento, conscientização e competência adequados.

Resultados: O estabelecimento dos seguintes itens demonstra o compromisso da gerência:

- Uma política de segurança da informação. Essa política pode ser um documento independente ou parte de manual geral de segurança usado por uma organização. (Para obter orientações adicionais, veja o exemplo abaixo);
- Objetivos e planos de segurança da informação. Novamente, essas informações podem ser um documento independente ou parte de um manual geral de segurança usado por uma organização (para obter orientações adicionais, veja o exemplo abaixo);
- Funções e responsabilidades pela segurança da informação. Uma lista das funções relacionadas à segurança da informação deve ser documentada nos documentos de descrição do trabalho da organização ou como parte do manual de segurança ou documentos de descrição do SGSI.
- Anúncio ou comunicado à organização sobre a importância de aderir à política de segurança da informação;
- Recursos suficientes para gerenciar, desenvolver, manter e implementar o SGSI.

Além disso, a administração participará do processo PDCA do Planejar-Fazer-Verificar-Agir do SGSI, conforme descrito na ISO/IEC 27001:2013 para:

- Determinar o nível aceitável de risco: A evidência dessa atividade pode ser incorporada aos documentos de avaliação de riscos, descritos mais adiante neste guia. (Veja as etapas 6 a 8).
- Realizar análises gerenciais do SGSI em intervalos planejados: A evidência dessa atividade pode ser parte do processo de aprovação dos documentos no SGSI;
- Garantir que o pessoal afetado pelo SGSI receba treinamento e seja competente para as funções e responsabilidades que eles são designados para cumprir e estejam cientes desses papéis e responsabilidades: A evidência dessa atividade pode ser obtida por meio de registros de treinamento e documentos de revisão.

Exemplo:

Este exemplo mostra uma possível declaração de política com metas e objetivos.

Política de segurança

A proteção dos ativos da empresa é vital para o sucesso de nossos negócios. Para esse fim, estabelecemos um sistema de gerenciamento de segurança da informação que opera todos os processos necessários para identificar as informações que precisamos proteger e como devemos protegê-las.

Como as necessidades de nossos negócios mudam, reconhecemos que nosso sistema de gerenciamento deve ser continuamente alterado e aprimorado para atender às nossas necessidades. Para esse efeito, estamos continuamente estabelecendo novos objetivos e revisando regularmente nossos processos.

Objetivos

É política da nossa empresa garantir que:

- As informações são acessíveis apenas a pessoas autorizadas dentro ou fora da empresa.
- A confidencialidade das informações é mantida.
- A integridade das informações é mantida durante todo o processo.
- Planos de continuidade de negócios são estabelecidos, mantidos e testados.
- Todo o pessoal é treinado em segurança da informação e é informado de que a conformidade com a política é obrigatória.
- Todas as violações de segurança da informação e suspeitas de vulnerabilidades são relatadas e investigadas.
- Existem procedimentos para apoiar a política, incluindo medidas de controle de vírus, senhas e planos de continuidade.
- Os requisitos comerciais para disponibilidade de informações e sistemas serão atendidos.
- O gerente de segurança da informação é responsável por manter a política, fornecer suporte e conselhos durante a sua implementação.
- Todos os gerentes são diretamente responsáveis por implementar a política e garantir a conformidade da equipe em seus respectivos departamentos.

Essa política foi aprovada pela administração da empresa e deve ser revisada pela equipe de revisão anualmente:

Assinatura: _____ Data: _____

Cargo: _____

Figura 1: Exemplo de Política de Segurança

3. Determine o escopo do SGSI

Quando a gerência tiver assumido os compromissos apropriados, você poderá começar a estabelecer seu SGSI. Nesta etapa, você deve determinar em que medida deseja que o SGSI se aplique à sua organização.

Do que você precisa:

Você pode usar vários documentos de "resultado" criados como parte da etapa 2, como:

- A política de segurança da informação;
- Os objetivos e planos de segurança da informação;
- As funções e responsabilidades relacionadas à segurança e segurança da informação que foram definidos pela gerência.

Além disso, você precisará de:

- Listas das áreas, locais, ativos e tecnologias da organização que serão controladas pelo SGSI.

Ao revisar essas listas, você pode responder a perguntas semelhantes às seguintes:

- Quais áreas da sua organização serão cobertas pelo SGSI?
- Quais são as características dessas áreas: suas localizações, ativos e tecnologias a serem incluídas no SGSI?
- Você exigirá que seus fornecedores obedeçam ao seu SGSI?
- Existem dependências em outras organizações? Elas devem ser consideradas?

Seu objetivo será cobrir o seguinte:

- Os processos usados para estabelecer o escopo e o contexto do SGSI;
- O contexto estratégico e organizacional.

Importante: Mantenha seu escopo gerenciável. Considere incluir apenas partes da organização, como um agrupamento lógico ou físico dentro da organização. As grandes organizações podem precisar de vários Sistemas de Gerenciamento de Segurança da Informação para manter a capacidade de gerenciamento. Por exemplo, eles podem ter um SGSI para o departamento financeiro e as redes usadas por esse departamento e um SGSI separado para o departamento e sistemas de Desenvolvimento de Software.

Resultado: um escopo documentado para o seu SGSI.

Quando você tiver determinado o escopo, precisará documentá-lo, geralmente em algumas declarações ou parágrafos. O escopo documentado geralmente se torna uma das primeiras seções do Manual de segurança da sua organização. Ou pode permanecer um documento independente em um conjunto de documentos SGSI que você planeja manter.

Geralmente, o escopo, a política de segurança e os objetivos de segurança são combinados em um documento.

Para obter orientações adicionais, consulte o exemplo a seguir.

Escopo e finalidade

A empresa está comprometida em proteger suas informações e as de seus clientes. Para atingir esse objetivo, a empresa implementou um Sistema de Gerenciamento de Segurança da Informação de acordo com a ISO / IEC 27001: 2013.

O SGSI da empresa é aplicável às seguintes áreas de negócios:

- Departamento financeiro;
- Sistemas e redes internas de TI usados para negócios de back-end (como e-mail, planilhas de horas, desenvolvimento e armazenamento de contratos e elaboração de relatórios).

(**Observação:** Os sistemas de TI nos quais o software da empresa é desenvolvido e armazenado fazem parte do SGSI de Desenvolvimento de Software. Consulte o Manual de Segurança de Desenvolvimento de Software para obter mais informações).

Exemplo:

Figura 2: Exemplo de declaração de escopo

4. Identifique a legislação aplicável

Depois de determinar o escopo, identifique quaisquer padrões regulamentares ou legislativos que se apliquem às áreas que você planeja cobrir com o SGSI. Esses padrões podem vir do setor em que sua organização trabalha ou de governos estaduais, locais ou federais ou de órgãos reguladores internacionais.

Do que você precisa: Padrões regulamentares ou legislativos atualizados que possam ser aplicáveis à sua organização. Pode ser útil ter opiniões e críticas de advogados ou especialistas com conhecimento sobre os padrões.

Resultados: Declarações adicionais no escopo do SGSI. Se o seu SGSI incorporar mais de dois ou três padrões legislativos ou regulamentares, você também poderá criar um documento ou apêndice separado no Manual de Segurança que lista todos os padrões aplicáveis e detalhes sobre os padrões.

Exemplo: O texto adicionado à declaração do escopo como resultado da identificação da legislação aplicável é mostrado no exemplo a seguir.

Escopo e finalidade

A empresa está comprometida em proteger suas informações e as de seus clientes. Para atingir esse objetivo, implementamos um Sistema de Gerenciamento de Segurança da Informação de acordo com a ISO / IEC 27001: 2013 e as regras e regulamentos que fazem parte da Lei Pública da OSHA 91-596 84 STAT. 1950.

O SGSI da empresa é aplicável às seguintes áreas de negócios:

- Departamento financeiro;
- Sistemas e redes internas de TI usados para negócios de back-end (como e-mail, planilhas de horas, desenvolvimento e armazenamento de contratos e elaboração de relatórios) (**Observação:** Sistemas de TI e redes nas quais o software da empresa é desenvolvido e armazenado fazem parte do SGSI de Desenvolvimento de Software. Consulte o Manual de Segurança de Desenvolvimento de Software para obter mais informações.

Figura 3: Exemplo de texto de escopo adicional

5. Defina um método de avaliação de risco

A avaliação de riscos é o processo de identificação de riscos, analisando ameaças, impactos e vulnerabilidades de sistemas de informação e informação e instalações de processamento, e a probabilidade de ocorrência. A escolha de um método de avaliação de risco é uma das partes mais importantes do estabelecimento de um SGSI.

Para atender aos requisitos da ISO/IEC 27001:2013, você precisará definir e documentar um método de avaliação de riscos e usá-lo para avaliar o risco para os ativos de informações identificados, tomar decisões sobre quais riscos são intoleráveis e, portanto, precisam ser mitigados, e gerenciar os riscos residuais por meio de políticas, procedimentos e controles cuidadosamente considerados.

A ISO/IEC 27001:2013 não especifica o método de avaliação de risco que você deve usar, no entanto, afirma que você deve usar um método que permita concluir as seguintes tarefas:

- Avaliar riscos com base em níveis de confidencialidade, integridade e disponibilidade.

Alguns métodos de avaliação de risco fornecem uma matriz que define os níveis de confidencialidade, integridade e disponibilidade e fornece orientações sobre quando e como esses níveis devem ser aplicados, conforme mostrado na tabela a seguir:

Impacto da perda	Baixo	Médio	Alto
Confidencialidade Garantir que as informações sejam acessíveis apenas às pessoas autorizadas a ter acesso	Pode-se esperar que a divulgação não autorizada de informações tenha um efeito adverso limitado nas operações, ativos ou indivíduos da organização.	Pode-se esperar que a divulgação não autorizada de informações tenha um sério efeito adverso nas operações organizacionais, ativos organizacionais ou indivíduos.	Pode-se esperar que a divulgação não autorizada de informações tenha um efeito adverso grave ou catastrófico nas operações organizacionais, ativos organizacionais ou indivíduos.
Integridade Proteger a precisão e a integridade das informações e métodos de processamento	Pode-se esperar que a modificação ou destruição não autorizada de informações tenha um efeito adverso limitado nas operações organizacionais, ativos organizacionais ou indivíduos.	Pode-se esperar que a modificação ou destruição não autorizada de informações tenha um sério efeito adverso nas operações organizacionais, ativos organizacionais ou indivíduos.	Pode-se esperar que a modificação ou destruição não autorizada de informações tenha um efeito adverso grave ou catastrófico nas operações organizacionais, ativos organizacionais ou indivíduos.
Disponibilidade Garantir que usuários autorizados tenham acesso a informações e ativos associados quando necessário	Pode-se esperar que a interrupção do acesso ou uso de informações ou de um sistema de informações tenha um efeito adverso limitado nas operações organizacionais, ativos organizacionais ou indivíduos.	Pode-se esperar que a interrupção do acesso ou uso de informações ou de um sistema de informações tenha um sério efeito adverso nas operações organizacionais, ativos organizacionais ou indivíduos.	Pode-se esperar que a interrupção do acesso ou uso de informações ou de um sistema de informações tenha um efeito adverso grave ou catastrófico nas operações organizacionais, ativos organizacionais ou indivíduos.

Figura 4: Exemplo da tabela de valores da empresa

- Estabeleça objetivos para reduzir o risco a um nível aceitável;
- Determine os critérios para aceitar o risco;
- Avalie as opções de tratamento de risco.

Você pode escolher entre vários métodos de avaliação de riscos, como os predominantes em seu setor. Por exemplo, se sua empresa estiver no setor de petróleo, você poderá descobrir que existem métodos de avaliação de risco relacionados a esse setor.

Do que você precisará:

Se você não estiver familiarizado com os métodos de avaliação de riscos, poderá consultar os seguintes exemplos publicados:

- ISO / IEC 13335 (Gerenciamento de segurança da informação e das comunicações)
- NIST SP 800-30 (Guia de Gerenciamento de Riscos para Informações) Sistemas de tecnologia) http://csrc.nist.gov/publications/nistpubs/
- Métodos de avaliação de risco específicos do setor de sua organização.

Resultados:

Quando você concluir esta etapa, deverá ter um documento que explique como sua organização avaliará os riscos, incluindo:

- A abordagem da organização para o gerenciamento de riscos à segurança da informação;
- Critérios para avaliação dos riscos à segurança da informação e o grau de garantia exigido.

Nota: Nas etapas subsequentes, descritas neste guia, você adicionará mais informações a este documento, que definirá os ativos que precisam ser protegidos, os riscos associados a cada um desses ativos e uma lista dos controles que serão usados para reduzir ou eliminar os riscos.

Para obter orientações adicionais, consulte o exemplo a seguir.

Exemplo: Este exemplo fornece um esboço possível para um documento de avaliação de risco que define a metodologia de avaliação de risco.

Índice

Figura 5: Exemplo do conteúdo de um documento de metodologia de avaliação de risco

6. Crie um inventário de ativos de informações para proteger

Para identificar riscos e os níveis de riscos associados às informações que você deseja proteger, primeiro você precisa fazer uma lista de todos os seus ativos de informações que são cobertos no escopo do SGSI.

Do que você precisará:

Você precisará do escopo definido na etapa 3 e da entrada da organização definida em seu escopo em relação aos ativos de informações.

Resultado:

Ao concluir esta etapa, você deve ter uma lista dos ativos de informações a serem protegidos e um proprietário para cada um desses ativos. Você também pode identificar onde as informações estão localizadas e quão crítico ou difícil seria substituir.

Essa lista deve fazer parte do documento da metodologia de avaliação de risco que você criou na etapa anterior.

Como você precisará dessa lista para documentar sua avaliação de risco, convém agrupar os ativos em categorias e, em seguida, criar uma tabela de todos os ativos com colunas para informações da avaliação e os controles que você optar por aplicar. (Você executará essas atividades nas etapas subsequentes deste guia). O exemplo a seguir mostra uma tabela de ativos.

Exemplo:

Avaliação de Riscos

Ativos	Detalhes	Proprietário	Localização	Perfil da Companhia	Valor de Substituição	Resumo do Risco	Valor do Risco	Controle	Controle Suficiente?
Informação Estratégica	Planos e médio e longo prazo	CEO	CEO PC		Alto				
Planos do Projeto	Planos de curto prazo	CEO	CEO PC		Médio				

Figura 6: Exemplo de tabela de ativos com colunas de espaço reservado para informações de avaliação

7. Identifique os riscos

Em seguida, para cada ativo que você definiu na etapa anterior, será necessário identificar os riscos e classificá-los de acordo com a gravidade e a vulnerabilidade deles.

Além disso, você precisará identificar o impacto que a perda de confidencialidade, integridade e disponibilidade pode ter sobre os ativos. Para começar a identificar riscos, você deve começar identificando ameaças e vulnerabilidades reais ou potenciais para cada ativo.

Uma ameaça é algo que pode causar danos. Por exemplo, uma ameaça pode ser uma das seguintes:

- Uma declaração da intenção de causar danos ou desastre;
- Potencial para causar um incidente indesejado, que pode resultar em danos a um sistema ou organização e seus ativos;
- Intencional, acidental ou ato criado pelo homem que poderia causar danos ou um ato de Deus (como um furacão ou tsunami).

Uma vulnerabilidade é uma fonte ou situação com potencial de dano (por exemplo, uma janela quebrada é uma vulnerabilidade; pode incentivar danos, como como uma quebra).

Um risco é uma combinação da probabilidade e gravidade ou frequência em que uma ameaça específica ocorrerá.

Do que você precisará:

- A lista de ativos que você definiu na etapa anterior.
- A metodologia de avaliação de risco definida na etapa 5.

Para cada ativo, você deve identificar vulnerabilidades que possam existir para esse ativo e ameaças que possam resultar dessas vulnerabilidades. Muitas vezes, é útil pensar em ameaças e vulnerabilidades em pares - com pelo menos um par para cada ativo e possivelmente vários pares para cada ativo.

Resultados:

Para cada ativo, você terá uma descrição de ameaças e vulnerabilidades e, usando sua metodologia de Avaliação de riscos, atribuirá níveis de confidencialidade, integridade e disponibilidade a esse ativo.

Se você usou uma tabela para a etapa 6, poderá adicionar essas informações a essa tabela, conforme mostrado no exemplo a seguir.

Exemplo:

Nota: No exemplo a seguir, a coluna Resumo do Risco descreve a ameaça e a vulnerabilidade. O

Avaliação de Riscos

Ativos	Detalhes	Proprietário	Localização	Perfil da Companhia	Valor de Substituição	Resumo do Risco	Valor do Risco	Controle	Controle Suficiente?
Informação Estratégica	Planos e médio e longo prazo	CEO	CEO PC	Alto I: Alto A: Médio	Alto	Divulgação (dá vantagem a terceiros)			
Planos do Projeto	Planos de curto prazo	CEO	CEO PC	Alto I: Alto A: Baixo	Médio	Divulgação (dá vantagem ao concorrente); empresa pode perder negócios			

perfil da CIA classifica a confidencialidade, integridade e disponibilidade do ativo.

Figura 7: Exemplo de identificação de risco

8. Avalie os riscos

Depois de identificar os riscos e os níveis de confidencialidade, integridade e disponibilidade, você precisará atribuir valores aos riscos.

Os valores ajudarão você a determinar se o risco é tolerável ou não e se você precisa implementar um controle para eliminar ou reduzir o risco.

Para atribuir valores a riscos, é necessário considerar:

- O valor do ativo que está sendo protegido;
- A frequência com que a ameaça ou vulnerabilidade pode ocorrer;
- O dano que o risco pode causar à empresa ou a seus clientes ou parceiros.

Por exemplo, você pode atribuir valores de Baixo, Médio e Alto aos seus riscos. Para determinar qual valor atribuir, você pode decidir que, se o valor de um ativo for alto e o dano de um risco especificado for alto, o valor do risco também deverá ser alto, mesmo que a frequência potencial seja baixa. O documento da Metodologia de Avaliação de Riscos deve informar quais valores usar e também pode especificar as circunstâncias em que valores específicos devem ser atribuídos.

Além disso, não deixe de consultar o documento da Metodologia de Avaliação de Riscos para determinar a implicação de um determinado valor de risco. Por exemplo, para manter seu SGSI gerenciável, sua Metodologia de Avaliação de Risco pode especificar que apenas riscos com um valor Médio ou Alto exigirão um controle no seu SGSI. Com base nas necessidades de seus negócios e nos padrões do setor, os riscos receberão valores apropriados.

Do que você precisará:

- Lista de ativos e seus riscos associados e níveis da companhia, criados na etapa anterior.
- Possibilidade de contribuição da administração quanto ao nível de risco que eles estão dispostos a aceitar para ativos específicos.

Resultados:

Ao concluir sua avaliação, você identificará quais ativos de informações têm risco intolerável e, portanto, requerem controles. Você deve ter um documento (às vezes chamado de Relatório de Avaliação de Riscos) que indica o valor do risco para cada ativo.

Na próxima etapa, você identificará quais controles podem ser aplicáveis aos ativos que requerem controle para reduzir o risco a níveis toleráveis.

Este documento pode ser autônomo ou fazer parte de um documento geral de Avaliação de Riscos que contém sua metodologia de avaliação de risco e essa avaliação de risco.

Exemplos:

Se você usou uma tabela semelhante à dos exemplos anteriores, o resultado após a conclusão desta etapa pode ser semelhante ao exemplo a seguir:

Avaliação de Riscos

Ativos	Detalhes	Proprietário	Localização	Perfil da Companhia	Valor de Substituição	Resumo do Risco	Valor do Risco	Controle	Controle Suficiente?
Informação Estratégica	Planos de médio e longo prazo	CEO	CEO PC	Alto I: Alto A: Médio	Alto	Divulgação (dá vantagem a terceiros)	Alto		
Planos do Projeto	Planos de curto prazo	CEO	CEO PC	Alto I: Alto A: Baixo	Médio	Divulgação (dá vantagem ao concorrente); empresa pode perder negócios	Médio		
Documentos do RH	Registros de funcionários	Conselho da empresa	Empresa de gestão de RH	Alto I: Alto A: Baixo	Médio	Divulgação de informações pessoais	Médio		

Figura 8: Exemplo de avaliação de riscos

9. Identifique objetivos e controles aplicáveis

Em seguida, para os riscos que você considerou intoleráveis, execute uma das seguintes ações:

- Decida aceitar o risco; por exemplo, ações não são possíveis porque estão fora de seu controle (como desastres naturais ou crise política) ou são muito caros.
- Transferir o risco, por exemplo, adquirir seguro contra o risco, subcontratar a atividade para que o risco seja repassado ao subcontratado, etc.
- Reduzir o risco para um nível aceitável através do uso de controles.

Para reduzir o risco, você deve avaliar e identificar os controles apropriados. Esses controles podem ser controles que sua organização já possui ou controles definidos na norma ISO/IEC 27002:2013 (ISO / IEC 17799).

(**Nota:** Um exame dos controles que você já possui em relação ao padrão e, em seguida, usar os resultados para identificar quais controles estão faltando é comumente chamado de "análise de gap").

Do que você precisará:

- Anexo A da ISO/IEC 27001:2013. Este apêndice resume os controles que você pode escolher.
- A ISO/IEC 27002:2013 (ISO / IEC 17799), que fornece mais detalhes sobre os controles resumidos na ISO/IEC 27001:2013.
- Procedimentos para os controles corporativos existentes.

Resultados:

Você deve terminar com dois documentos concluindo esta etapa:

- Um Plano de Tratamento de Riscos;
- Uma Declaração de Aplicabilidade.

O Plano de Tratamento de Riscos documenta o seguinte:

- O método selecionado para tratar cada risco (aceitar, transferir, reduzir);
- Quais controles já estão em vigor;
- Quais controles adicionais são propostos,
- O prazo durante o qual os controles propostos devem ser implementados.

A Declaração de Aplicabilidade (SOA) documenta os objetivos e controles de controle selecionados no Anexo A. A Declaração de Aplicabilidade geralmente é uma tabela grande em que cada controle do Anexo A da ISO/IEC 27001:2013 é listado com sua descrição e colunas correspondentes que indicam se esse controle foi adotado pela organização, a justificativa para adotar ou não o controle e uma referência ao local onde o procedimento da organização para usar esse controle está documentado.

A SOA pode fazer parte do documento de Avaliação de Risco; mas geralmente é um documento independente, pois é longo e é listado como um documento obrigatório no padrão.

Para obter ajuda adicional na criação de um Plano de Tratamento de Riscos e uma Declaração de Aplicabilidade, consulte os dois conjuntos de exemplos a seguir.

Exemplos de plano de tratamento de riscos:

Se você usou uma tabela conforme descrito nas etapas anteriores, a parte da análise de controle do seu Plano de Tratamento de Riscos pode ser coberta pela coluna Controle e pela coluna Controle suficiente, conforme mostrado a seguir.

Nota: Quaisquer riscos que você transferir para outras pessoas ou que optar por aceitar também

Avaliação de Riscos

Ativos	Detalhes	Proprietário	Localização	Perfil da Companhia	Valor de Substituição	Resumo do Risco	Valor do Risco	Controle	Controle Suficiente?
Informação Estratégica	Planos de médio e longo prazo	CEO	CEO PC	Alto I: Alto A: Médio	Alto	Divulgação (dá vantagem a terceiros)	Alto	15.1.1	Sim
Planos do Projeto	Planos de curto prazo	CEO	CEO PC	Alto I: Alto A: Baixo	Médio	Divulgação (dá vantagem ao concorrente); empresa pode perder negócios	Médio	15.1.1	Sim
Documentos do RH	Registros de funcionários	Conselho da empresa	Empresa de gestão de RH	Alto I: Alto A: Baixo	Médio	Divulgação de informações pessoais	Médio	Nenhum; Atividades de RH e gerenciamento de documentação terceirizados	Sim

devem ser registrados em seu plano de tratamento.

Figura 9: Exemplo de avaliação de risco com análise de controle incluída

Os requisitos remanescentes do Plano de Tratamento de Riscos podem ser atendidos adicionando esta tabela e explicando os métodos usados para tratar o risco e o período em que os controles serão implementados em um documento da Metodologia de Avaliação de Riscos, como o que você criou na etapa 5.

O conteúdo do documento revisado pode parecer com o seguinte exemplo:

Índice

Introdução

Preparação

- Escopo e limites;
- Objetivos e requisitos de segurança;
- Riscos aceitáveis
    - Descrição das principais vulnerabilidades;
    - Descrição das principais ameaças;
    - Riscos residuais.

Análise de Incerteza

- Premissas;
- Dependências Externas.

Melhorias planejadas

- Eficácia dos controles;
- Controles planejados;
- Avaliação do risco residual.

Palavras-chave e definições

- Escala de cores de valor de risco;
- Definições de confidencialidade, integridade, disponibilidade, responsabilidade e as consequências de sua ausência;
- Definições de termos-chave (como ativo, risco, vulnerabilidade a ameaças, informações, dados, controle).

Avaliação de ativos, Identificação de riscos, Análise de controle (a tabela Avaliação de risco)

Declaração de aplicabilidade (pode ser um resumo com ponteiro para a tabela detalhada em um documento separado)

- Seleção de controles;
- Exclusão de controles.

Figura 10: Exemplo de documento de avaliação de risco com informações de avaliação e SOA incluídos

Exemplo de Declaração de Aplicabilidade:

A seguir, um trecho de um documento de Declaração de Aplicabilidade. A coluna Referência identifica o local em que a declaração de política ou procedimento detalhado relacionado à implementação do controle está documentado.

Dois itens na coluna Referência estão incompletos neste exemplo, porque nesta etapa você pode não ter um conjunto completo de políticas e procedimentos para todos os controles. A próxima etapa

Controle	Título	App.	Declaração de Compliance	Referência
5	Política de segurança			
5.1	Política de segurança da informação		Fornecer orientação de gerenciamento e suporte para segurança da informação	
5.1.1	Documento da política de segurança da informação	Sim	A Política de Segurança da Informação é fornecida aos Novos Funcionários no primeiro dia de trabalho.	Manual de segurança da empresa
5.1.2	Revisão da política de segurança da informação	Sim	A Política de Segurança da Informação é revisada continuamente pela gerência, além de análises de gerenciamento	Documento de papéis e responsabilidades
6	Organizar a segurança da informação			
6.1	Organização interna			
6.1.1	Compromisso da gerência com a segurança da informação	Sim	Documentado na Política de segurança da informação	Política de segurança da Organização
6.1.2	Coordenação da segurança da informação	Sim	Por meio de um fórum de segurança, sessões de treinamento e trabalho diário	Procedimentos de segurança
6.1.3	Alocação de responsabilidades da segurança da informação	Sim	A alocação de responsabilidades de segurança da informação está documentada	Procedimentos de segurança Manual de segurança da Organização

aborda a criação de procedimentos adicionais para que você possa concluir a Declaração de Aplicabilidade.

Figura 11: Exemplo de declaração de aplicabilidade

10. Estabelecer políticas e procedimentos para controlar riscos

Para cada controle que você define, você deve ter instruções de política correspondentes ou, em alguns casos, um procedimento detalhado. O procedimento e as políticas são usados pelo pessoal afetado para que eles entendam suas funções e para que o controle possa ser implementado de forma consistente. A documentação da política e procedimentos é um requisito da ISO/IEC 27001:2013.

Do que você precisará:

Para ajudá-lo a identificar quais procedimentos você pode precisar documentar, consulte sua Declaração de Aplicabilidade.

Para ajudá-lo a escrever seus procedimentos para que sejam consistentes no conteúdo e na aparência, convém criar algum tipo de modelo para os documentadores de procedimentos usarem.

Resultados:

Documentos adicionais sobre políticas e procedimentos. (O número de documentos que você produz depende dos requisitos da sua organização).

Alguns desses procedimentos também podem gerar registros. Por exemplo, se você tiver um procedimento em que todos os visitantes de suas instalações devem assinar um log de visitantes, o próprio log se tornará um registro, fornecendo evidências de que o procedimento foi seguido.

As seções 4.3.2 e 4.3.3 da ISO/IEC 27001:2013 exigem que todos os documentos e registros que fazem parte do seu SGSI sejam adequadamente controlados. Portanto, documentos de política e procedimento também devem ser criados para tratar desses controles.

Exemplo:

O número de políticas, procedimentos e registros necessários como parte do seu SGSI dependerá de vários fatores, incluindo o número de ativos que você precisa proteger e a complexidade dos controles

Manual de segurança
Política de segurança
Metodologia de avaliação de riscos
Relatório de avaliação de riscos, lista de ativos e plano de tratamento
Declaração de aplicabilidade
Documento de Papéis e Responsabilidades
Procedimento 1: Segurança no local de trabalho
Procedimento 2: Controle de documentos e registros
Procedimento 3: Treinamento
Procedimento 4: Backups do servidor
Procedimento 5: Procedimento de auditoria
Registros:
- Cronograma de auditoria
- Registros de treinamento de funcionários
- Registros de revisão / avaliação de funcionários
- Problemas / não conformidades
- Registros de manutenção de servidores
- Registros de Revisão de Gestão

Figura 12: Exemplo de alguns documentos em um SGSI

11. Aloque recursos e treine a equipe

Recursos adequados (pessoas, tempo, dinheiro) devem ser alocados para a operação do SGSI e todos os controles de segurança. Além disso, a equipe que deve trabalhar no SGSI (mantendo-a e sua documentação e implementando seus controles) deve receber treinamento apropriado.

O sucesso do programa de treinamento deve ser monitorado para garantir sua eficácia. Portanto, além do programa de treinamento, você também deve estabelecer um plano para determinar a eficácia do treinamento.

Do que você precisará:

- Uma lista dos funcionários que trabalharão dentro do SGSI;
- Todos os procedimentos do SGSI a serem usados para identificar que tipo de treinamento é necessário e quais membros da equipe ou das partes interessadas precisarão de treinamento;
- Consentimento da gestão para alocação de recursos e planos de treinamento.

Resultados:

Não é necessária documentação específica nas normas ISO / IEC. No entanto, para fornecer evidências de que o planejamento e o treinamento de recursos foram realizados, você deve ter alguma documentação que mostre quem recebeu o treinamento e o treinamento recebido.

Você pode incluir uma seção para cada funcionário que lista o treinamento que eles devem receber. Além disso, você provavelmente terá algum tipo de procedimento para determinar quantas pessoas, qual valor e quanto tempo precisa ser alocado para a implementação e manutenção do seu SGSI. É possível que esse procedimento já exista como parte dos procedimentos operacionais da sua empresa ou que você queira adicionar uma seção SGSI à documentação existente.

Exemplo:

O exemplo a seguir mostra um modelo para um registro de treinamento de funcionários:

Conclusão de treinamento

Data de conclusão	Escopo	Supervisor / Trainer	Resultado	Tipo de treinamento / comentários

Plano de treinamento

Meta de conclusão	Escopo	Tipo de treinamento / comentários

Figura 13: Exemplo de registro de treinamento de funcionários

12. Monitore a implementação do SGSI

Para garantir que o SGSI seja eficaz e permaneça atual, adequado e eficaz a ISO/IEC 27001:2013 exige:

- A gerência deve revisar o SGSI em intervalos planejados. A revisão deve incluir a avaliação de oportunidades de melhoria e a necessidade de alterações no SGSI, incluindo a política de segurança e os objetivos de segurança, com atenção específica às ações corretivas ou preventivas anteriores e sua eficácia;
- Auditorias internas periódicas.

Os resultados das revisões e auditorias devem ser documentados e os registros relacionados às revisões e auditorias devem ser mantidos.

Do que você precisará:

Para executar análises gerenciais, a ISO/IEC 27001:2013 requer as seguintes informações:

- Resultados das auditorias e análises internas e externas do SGSI;
- Feedback das partes interessadas;
- Técnicas, produtos ou procedimentos que podem ser usados na organização para melhorar a eficácia do SGSI;
- Ações preventivas e corretivas (incluindo aquelas que podem ter sido identificadas em análises ou auditorias anteriores);
- Relatórios de incidentes, por exemplo, se houve uma falha de segurança, um relatório que identifica qual foi a falha, quando ocorreu e como foi tratado e possivelmente corrigido;
- Vulnerabilidades ou ameaças não abordadas adequadamente na avaliação de risco anterior;
- Ações de acompanhamento de análises anteriores;
- Quaisquer mudanças organizacionais que possam afetar o SGSI;
- Recomendações para melhoria.

Para executar auditorias internas periodicamente, é necessário definir o escopo, critérios, frequência e métodos. Você também precisa do procedimento (que deveria ter sido escrito como parte da etapa 10) que identifica as responsabilidades e os requisitos para o planejamento e a realização das auditorias, além de relatar resultados e manter registros.

Resultados:

Os resultados de uma revisão gerencial devem incluir decisões e ações relacionadas a:

- Melhorias no SGSI;
- Modificação de procedimentos que afetam a segurança da informação em todos os níveis da organização;
- Necessidades de recursos.

Os resultados de uma auditoria interna devem resultar na identificação de não conformidades e suas ações corretivas ou preventivas relacionadas. A ISO/IEC 27001:2013 lista os requisitos de atividades e registros relacionados à ações corretivas e preventivas.

Exemplo:

O exemplo a seguir mostra o esboço de um plano de ação preventivo. Esse plano pode ser o resultado de uma auditoria interna ou uma análise de gerenciamento do SGSI. Você pode usar um esquema semelhante para preparar um plano de ação corretiva.

Plano de Ação Preventiva:

Descrição

Esta seção deve identificar as ocorrências semelhantes ou relacionadas de não conformidades em questão. Deverá identificar, também, as ações corretivas que foram tomadas para cada não conformidade.

Esta seção também deve fornecer um motivo para a necessidade de uma ação preventiva a ser tomada.

1. **Plano de ação**

Esta seção descreverá o plano de ação selecionado para implementar a ação preventiva, de modo que esclareça como a ação preventiva deve ser implementada e o que é esperado como resultado.

2. **Objetivo**

Esta seção identificará o objetivo do plano de ação. O objetivo, na maioria dos casos, é evitar futuras ocorrências de não conformidades identificadas a partir de reincidências.

3. **Método**

Esta seção descreverá a abordagem adotada para evitar ocorrências futuras de não conformidades identificadas a partir de recorrência.

4. **Resultados esperados**

Esta seção identificará o que é esperado como resultado da implementação da ação preventiva. O resultado esperado de algum modo, deve ser consistente com o objetivo descrito acima.

5. **Resultados**

Esta seção identificará os resultados da ação preventiva. Pode ser necessário listar mais de um conjunto resultados, nos casos em que você pode auditar a área da não conformidade mais de uma vez após a implementação da ação preventiva. Isso permite que o auditor examine a consistência entre os resultados.

6. **Efetividade**

Esta seção identificará a eficácia na ação preventiva selecionada. A eficácia pode ser medida com base na consistência ou comparação dos resultados esperados e dos resultados reais. Se os resultados forem muito semelhantes, a ação preventiva foi muito eficaz

Figura 14: Exemplo de plano de ação preventivo

13. Prepare-se para a auditoria de certificação

Se você planeja ter seu SGSI certificado, precisará realizar um ciclo completo de auditorias internas, gerenciamento revisão e atividades no processo PDCA.

O auditor externo examinará primeiro os documentos do SGSI para determinar o escopo e o conteúdo de seu SGSI. Em seguida, o auditor examinará os registros e evidências necessários para verificar que você implementa e pratica o que está declarado no seu SGSI.

Do que você vai precisar:

- Todos os documentos que você criou nas etapas anteriores;
- Registros de pelo menos um ciclo completo de análises críticas da gerência, auditorias internas e atividades do PDCA, e evidência das respostas obtidas como resultado dessas revisões e auditorias.

Resultados:

Os resultados desta preparação devem ser um conjunto de documentos que você pode enviar a um auditor para revisão e conjunto de registros e evidências que demonstrarão com que eficiência você implementou completamente SGSI.

14. Peça ajuda

Como você pode ver neste guia, estabelecer, implementar e manter um SGSI pode exigir muito trabalho, especialmente em seus estágios iniciais. Se você é novo em sistemas de gerenciamento ou especificamente em informações sistemas de gerenciamento de segurança, considere contratar um consultor profissional de SGSI para orientá-lo no processo. A familiaridade de um consultor com os requisitos de um SGSI e os controles sugeridos nos padrões IEO / IEC podem economizar tempo e dinheiro e garantirão práticas de segurança eficazes e possivelmente uma certificação do SGSI bem-sucedida.

15. Apêndices

Apêndice A - Documentos e Registros

Conforme descrito neste guia, o seu SGSI dependerá de muitos documentos e registros.

Certos documentos são exigidos pela ISO/IEC 27001:2013 e registros são necessários para fornecer evidência da implementação do SGSI.

As listas a seguir fornecem um resumo dos documentos e registros discutidos nas seções anteriores deste guia.

Documentos

- Declarações documentadas da política e dos objetivos do SGSI;
- O escopo do SGSI;
- Procedimentos e controles de suporte ao SGSI;
- Descrição da metodologia de avaliação de risco;
- Relatório de avaliação de risco;
- Plano de tratamento de riscos;
- Procedimentos documentados necessários pela organização para garantir o planejamento, operação e controle de seus processos de segurança da informação e descrever como medir a eficácia de controles;
- Registros exigidos pela ISO/IEC 27001:2013;
- Declaração de aplicabilidade.

Os documentos listados aqui podem ser documentos separados ou apresentados juntos em um ou mais conjuntos de documentos.

Registros

Os registros necessários para o seu SGSI dependerão dos requisitos da sua empresa. A ISO/IEC 27001:2013: 2013 declara que os registros devem ser estabelecidos e mantidos para fornecer evidência de conformidade com requisitos e a operação efetiva do SGSI. Afirma ainda que o SGSI deve levar em consideração quaisquer requisitos legais ou regulamentares relevantes e obrigações contratuais. Eles devem ser controlados e mantidos de acordo com as políticas e procedimentos de controle e retenção de documentos da organização.

Alguns exemplos de registros são:

- Registros de auditoria interna;
- Registros de treinamento de funcionários;
- Atas de revisão da gerência;
- Registros de ações preventivas e corretivas;
- Relatórios de incidentes.

CLASSIFICAÇÃO DESSE DOCUMENTO - INFORMAÇÃO INTERNA

APROVAÇÕES

CISO Responsável pelo Projeto: _____

E-Mail:_____

Certificação:_____

CEO Autorizador do Projeto: _____

E-Mail:_____

Certificação:_____

Auditor Leader ISO-27001: _____

E-Mail:_____

Certificação:_____

São Paulo, 01 de janeiro de 2020

Luciene Rosa, DPO
Membro ANPPD – Comitê de Conteúdo

Anielle Martinelli, DPO
Diretora de Conteúdo da ANPPD

Dr. Davis Alves, DPO
Presidente da ANPPD