ISO 27001, TUDO QUE VOCÊ PRECISA SABER

Este e-book foi desenvolvido para sanar as dúvidas a cerca do que se trata a norma ISO 27001, para que ela serve, como implementá-la e quais seus benefícios para a empresa. Continue a leitura para aprofundar seu conhecimento sobre essa ISO.

ostec
Segurança digital de resultados

ÍNDICE

INTRODUÇÃO

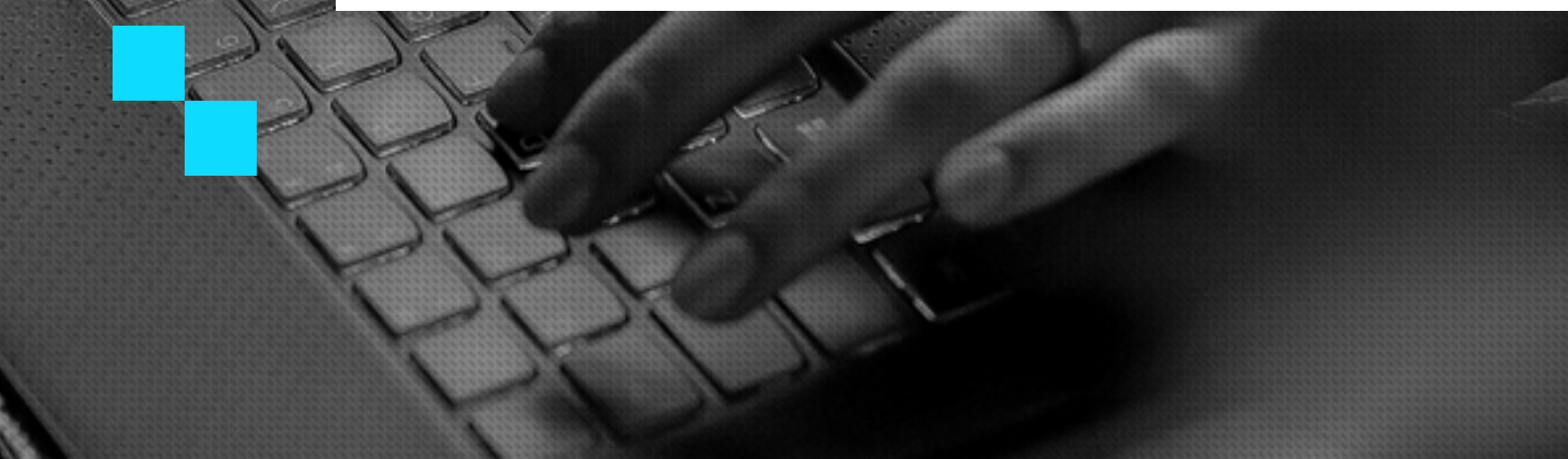
Certificações como a ISO 27001 são muito importantes para padronizar processos que previnam ataques e atuem de forma estratégica para garantir a privacidade de dados de uma empresa.

Uma organização que possui a ISO 27001 comprova que segue diretrizes que resultam em uma segurança eficaz. Essa comprovação é importante, pois fraquezas e falhas na segurança de dados impactam não somente na empresa em si, mas também os colaboradores, clientes, parceiros e quaisquer outras pessoas e empresas que tenham relacionamento com a organização.

A ISO 27001, além de ser uma das principais e mais importantes certificações de segurança da informação, contribui para o fortalecimento das ações da sua empresa.

Mas você sabe o que é a certificação ISO 27001?

Neste e-book, explicaremos do que se trata essa norma, para que ela serve, como implementá-la e quais seus benefícios para a empresa. Continue a leitura para aprofundar seu conhecimento sobre essa ISO.



O que é ISO 27001?

A ISO/IEC 27001 é a norma de referência internacional que fornece requisitos para proteger as informações de maneira sistemática, através da adoção de um Sistema de Gerenciamento de Segurança da Informação (SGSI). Ela foi publicada em outubro de 2005 pela International Organization for Standardization (ISO) e pela International Electrotechnical Commission, e foi desenvolvida com base na Norma Britânica BS 7799-2, efetivamente substituindo esse padrão que deixou de ser válido.

Geralmente é chamada de ISO/IEC 27001 ou apenas de ISO 27001, mas o nome completo dessa norma é ISO/IEC 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação – Requisitos.

A ISO 27001 pode ser implementada em qualquer tipo de organização, independente do segmento ou porte. O objetivo da norma é **elevar o nível da segurança da informação das organizações** permitindo mitigar e gerenciar os riscos por meio da implantação de um Sistema de Gestão de Segurança da Informação. Os reflexos da certificação poderão ser percebidos em todos os setores da empresa, além de ser considerado um diferencial competitivo perante o mercado.

É importante deixar claro que nenhuma organização é obrigada a ter a certificação ISO/IEC 27001. Porém, essa pode vir a ser uma exigência de clientes e parceiros antes de fecharem contrato com a empresa.

Por isso, adotar os padrões da norma é uma decisão estratégica, que deve ser tomada de acordo com as necessidades, tamanho e área de atuação do negócio.

Como é organizada a ISO 27001?

A ISO / IEC 27001 é dividia em 11 seções e Anexo A, onde as seções de 0 a 3 são introdutórias (e não são obrigatórias para a implementação), enquanto as seções de 4 a 10 são obrigatórias – significando que todos os seus requisitos devem ser implementados em uma organização se ela quer estar em conformidade com a norma. Os controles do Anexo A devem ser implementados apenas se declarados como aplicáveis na Declaração de Aplicabilidade.

De acordo com o Anexo SL das Diretivas ISO / IEC da International Organization for Standardization, os títulos das seções da ISO 27001 são os mesmos da ISO 22301:2012, na nova ISO 9001:2015, e outras normas de gestão, permitindo uma integração mais fácil destas normas.credenciais de acesso no gerenciador de senhas, sempre que necessitar acessar uma aplicação, basta você utilizar a senha mestra que os dados de acesso serão preenchidos automaticamente, liberando acesso ao aplicativo/site.

Seção 0_ Introdução – explica o propósito da ISO 27001 e sua compatibilidade com outras normas de gestão.

Seção 1_ Escopo – explica que esta norma é aplicável a qualquer tipo de organização.

Seção 2_ Referência normativa – refere-se a ISO / IEC 27000 como uma norma onde termos e definições são apresentados.

Seção 3_ Termos e definições – novamente, refere-se a ISO / IEC 27000.

Seção 4_ Contexto da organização – esta seção é parte da etapa de planejamento (Plan) do ciclo PDCA e define requisitos para o entendimento de assuntos externos e internos, partes interessadas e seus requisitos, e a definição do escopo do SGSI.

Seção 5_ Liderança – esta seção é parte da etapa de planejamento (Plan) do ciclo PDCA e define as responsabilidades da Alta Direção, estabelecendo papéis e responsabilidades, e o conteúdo da política de segurança da informação de alto nível.

Seção 6_ Planejamento – esta seção também faz parte da etapa de planejamento (Plan) do ciclo PDCA e define requisitos para a avaliação de risco, tratamento de risco, Declaração de Aplicabilidade, plano de tratamento de risco, e define os objetivos de segurança da informação.

Seção 7_ Apoio – mais uma seção da etapa de planejamento (Plan) do ciclo PDCA e define requisitos de disponibilidade de recursos, competências, conscientização, comunicação e controle de documentos e registros.

Seção 8_ Operação – esta seção é parte da etapa execução (Do) do ciclo PDCA e define a implementação da avaliação e tratamento de risco, assim como controles e outros processos necessários para atingir os objetivos de segurança da informação.

Seção 9_ Avaliação do desempenho – esta seção é parte da etapa verificação (Check) do ciclo PDCA e define requisitos para o monitoramento, medição, análise, avaliação, auditoria interna e análise crítica pela Direção.

Seção 10_ Melhoria – esta seção é parte da etapa de atuação (Act) do ciclo PDCA e define requisitos para não conformidades, ações corretivas e melhoria contínua.

Anexo A_ este anexo disponibiliza um catálogo de 114 controles (salvaguardas) distribuídos em 14 seções (seções de A.5 até A.18).

Para que serve a ISO 27001?

Por conta da preocupação no que se diz respeito à confiança no tratamento adequado de informações e dados sensíveis dentro de uma empresa, a ISO 27001, assim como as outras normas da família ISO, traz de uma abordagem sistemática para a proteção de informações confidenciais dentro de uma organização.

Essa preocupação com os dados pode partir da própria empresa, onde suas informações são extremamente relevantes e até confidenciais, de um possível fornecedor ou parceiro e até mesmo de clientes que forneçam seus dados pessoais para a organização.

Sendo assim, para garantir a segurança da informação, prevenir-se de ataques e agir estrategicamente, é necessário possuir processos fortes e estruturados. Para chegar a isso, uma série de pontos precisam ser observados. Com esse intuito existe a norma de padronização, para assegurar que uma organização atenda a todas as exigências para um SGSI adequado.

Assim, a adoção à norma ISO 27001 serve para garantir a adesão de um conjunto de requisitos, processos e controles que procuram gerir os riscos de forma apropriada.

Essa norma traz características que só beneficiam as organizações certificadas por ela.

Principais características da ISO 27001

A ISO 27001 tem como foco os princípios de confidencialidade, integridade e disponibilidade da informação. Ela visa identificação de riscos, definições de estratégias para sua mitigação e implementação de salvaguardas.

Abaixo, separamos as principais características dessa norma. Confira.

Análise de risco

A norma exige que a empresa faça uma análise de riscos de segurança periodicamente e sempre que mudanças significativas forem propostas ou estabelecidas. Para que essa análise seja feita da maneira correta, é preciso estabelecer critérios de aceitação de risco assim como a definição de como esses riscos serão medidos.
Também se devem avaliar as possíveis consequências dos riscos identificados, a probabilidade de que ocorram e seus níveis.

Comprometimento alta gestão

A norma também exige que a alta administração demonstre comprometimento com o SGSI, além de ser essa parte da empresa a responsável em si pela segurança da informação.

Os líderes também são responsáveis por assegurar que todos os recursos para a implantação do sistema estejam disponíveis e alocados corretamente e têm a obrigação de orientar colaboradores para que o sistema seja verdadeiramente eficiente.

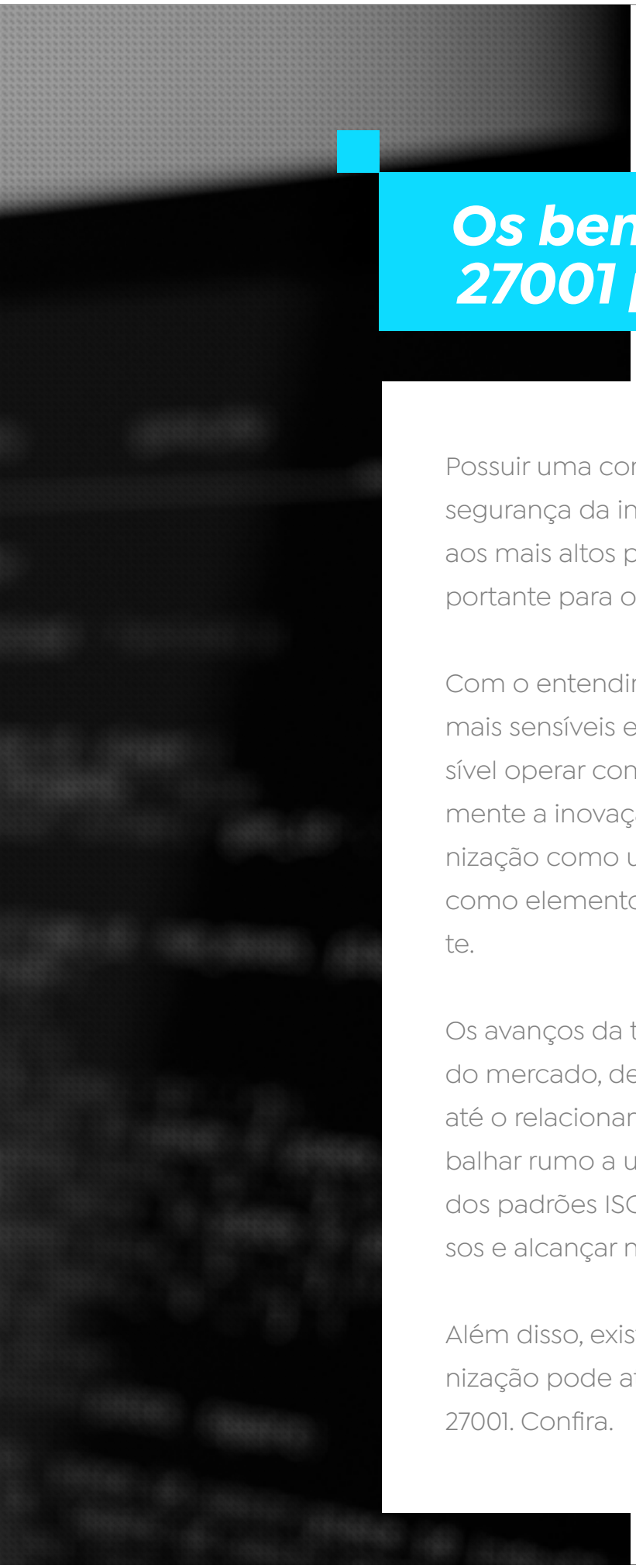
Definição de objetivos e estratégias

Durante o planejamento, a empresa precisa ter muito claro quais são seus objetivos de segurança e quais serão as estratégias estabelecidas para atingir esses objetivos. Os objetivos, entretanto, não podem ser genéricos, devem ser mensuráveis e considerar requisitos de segurança.

Recursos e competências

A organização também deve garantir que todos os recursos necessários não só para a implementação, mas também para a manutenção do sistema estejam disponíveis.

Além disso, é preciso estabelecer quais são as competências necessárias e certificar-se de que as pessoas responsáveis são qualificadas o suficiente é inclusive com documentação comprobatória.



Os benefícios da ISO 27001 para sua empresa

Possuir uma comprovação oficial de que a gestão de segurança da informação da sua empresa obedece aos mais altos padrões do setor é um diferencial importante para o negócio.

Com o entendimento de que as informações e dados mais sensíveis estão devidamente protegidos, é possível operar com mais confiança, buscando continuamente a inovação e o crescimento do setor e da organização como um todo. Ter a segurança da informação como elemento estratégico é cada vez mais importante.

Os avanços da tecnologia impactam todos os setores do mercado, desde o desenvolvimento de produtos até o relacionamento com o cliente. Sendo assim, trabalhar rumo a uma segurança da informação dentro dos padrões ISO 27001 é uma forma de alinhar processos e alcançar novos patamares.

Além disso, existem outros benefícios que uma organização pode atingir com a implementação da ISO 27001. Confira.

Melhores práticas

A ISO 27001 fornece as melhores práticas referentes a Gestão da Segurança da Informação, seus controles são reconhecidos internacionalmente, além de abrangerem a Segurança da Informação em todos os níveis.

Conformidade

A norma exige que você esteja em conformidade com todas as leis e requisitos contratuais, impactando positivamente na gestão de riscos, redução de impacto e governança corporativa. Ou seja, a metodologia implementada pela ISO 27001 consegue colocar o negócio em conformidade com a maioria das legislações de proteção de dados vigentes.

Redução de riscos

Com a análise de riscos e seu plano de tratamento, os controles são planejados e direcionados para evitar que qualquer ponto fraco do sistema seja explorado.

Vantagem competitiva

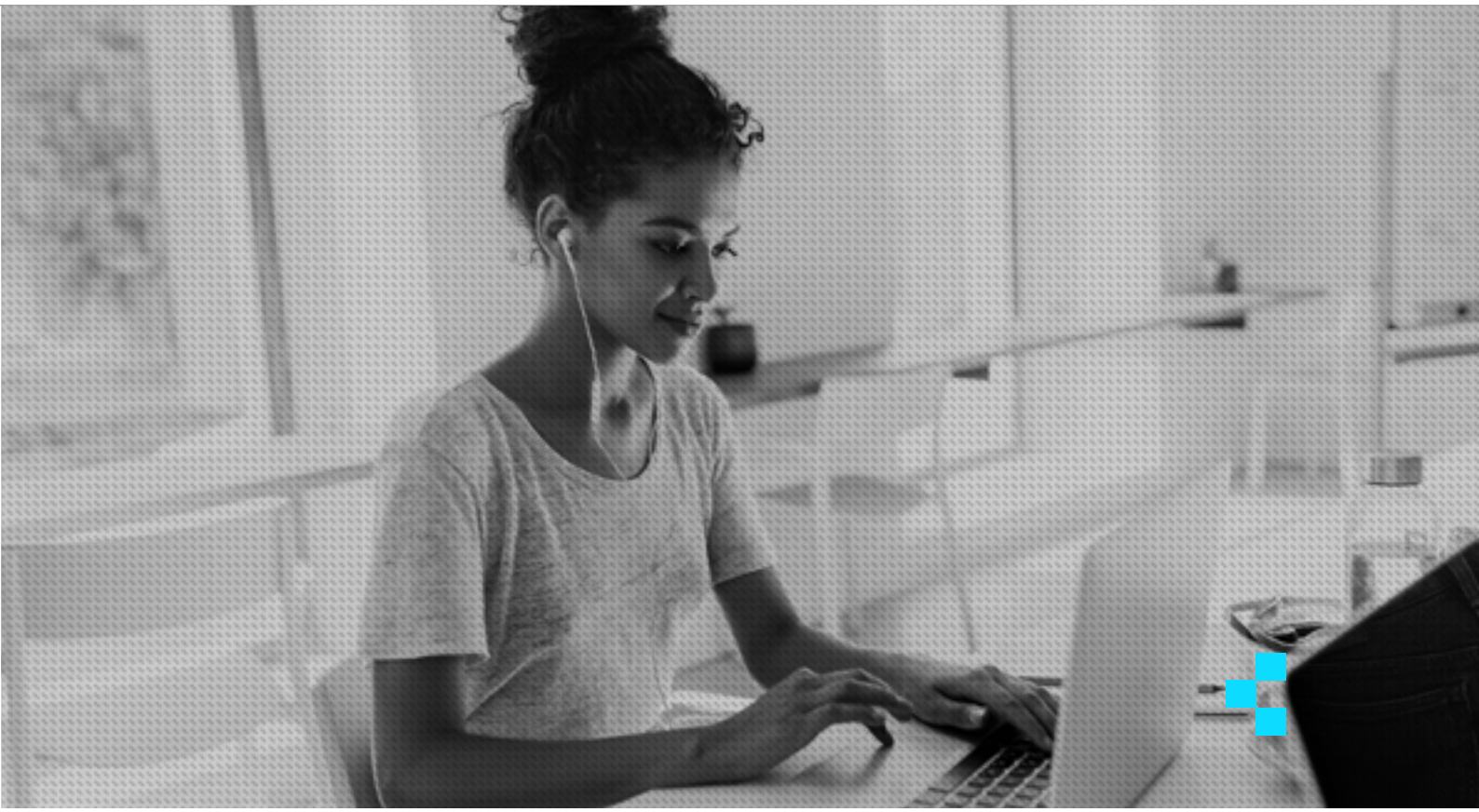
Seguir as práticas de ISO 27001 e até mesmo possuir a certificação ISO 27001 demonstra o compromisso da empresa com a segurança da informação. Assim, a confiabilidade dos clientes em relação a empresa aumenta consideravelmente.

Além disso, uma empresa certificada pode aumentar o número de oportunidades de negócios, tendo em vista que muitas empresas no momento da contratação exigem que seus fornecedores ou parceiros detenham a certificação como garantia de conformidade com as leis e um alto nível de preocupação referente a segurança da informação.

Organização interna da empresa

A ISO 27001 define que é necessário determinar as responsabilidades e seus responsáveis, acabando com aquela dúvida de quem decide ou cuida de determinado assunto. Ou seja, quando as ações são bem definidas e os objetivos esclarecidos, o desempenho operacional se torna mais efetivo.

Além disso, a norma aumenta os níveis de aderência da sensibilidade, participação e motivação dos colaboradores no que tange a segurança da informação.



Melhoria contínua

É uma das principais características e ações definidas pela norma. A ISO deixa evidente que a empresa deve assumir o compromisso de melhorar seus processos de gestão sempre que necessário. Por isso, auditorias devem ser realizadas para a empresa ter a chance de rever, analisar e alterar seus processos caso seja necessário devido ao surgimento de um gap ou oportunidade.

Integração de sistemas de gestão

Uma das bases da ISO 27001 é o ciclo PDCA (planejar, fazer, verificar, agir), que também faz parte de outras normas de sistemas de gestão.

Consequentemente, fica mais simples desenvolver um sistema de gestão único que atenda aos requisitos de outras normas, por exemplo, a ISO 9001 – sistema de gestão da qualidade.

Implementando a ISO 27001

Você analisou todos os benefícios da ISO 27001 e resolveu ter essa certificação em sua empresa. Mas como fazer isso?

Em uma organização, para implementar a ISO 27001, é necessário seguir 16 etapas:

Obter o apoio da gerência

Durante o planejamento, a empresa precisa ter muito claro quais são seus objetivos de segurança e quais serão as estratégias estabelecidas para atingir esses objetivos. Os objetivos, entretanto, não podem ser genéricos, devem ser mensuráveis e considerar requisitos de segurança.

Tratar como um projeto

A implementação da ISO 27001 envolve várias atividades, pessoas e tempo. É necessário definir o que deve ser feito, a pessoa designada para cada tarefa e quanto tempo ela terá para realiza-la.

Definir o escopo do projeto de certificação ISO 27001

Em casos de grandes organizações, é possível implementar a ISO 27001 em apenas uma parte dela – a que lida com dados. Portanto, antes de iniciar a implementação, deve ser definido o escopo.

Escrever o SGSI

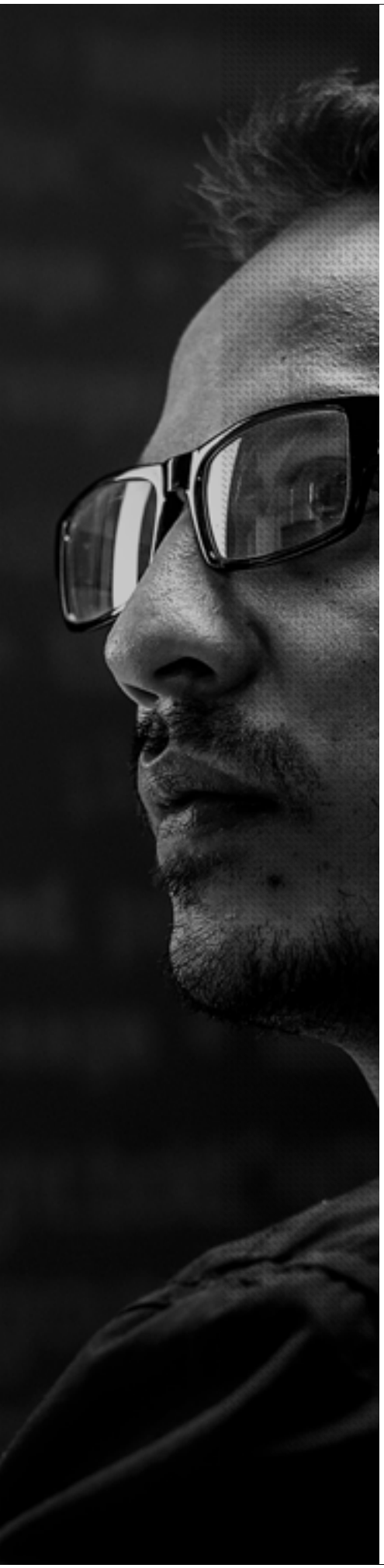
O SGSI é um documento de alto nível, que não deve ser muito detalhado, mas deve definir algumas questões básicas da segurança da informação em sua organização. O objetivo desse documento é definir o que se deseja alcançar e como manter o controle sobre isso.

Definir metodologia da avaliação de riscos

A avaliação de riscos é a tarefa mais complexa do projeto da ISO 27001. É importante definir as regras para a identificação de ativos, vulnerabilidades, ameaças, impactos e probabilidade, e definir o nível de risco aceitável.

Realizar avaliação de riscos e tratamento de riscos

Nesta etapa, é necessário implementar o que foi definido na etapa anterior. Para organizações de porte maior, isso pode demorar um pouco. O objetivo é ter uma visão abrangente sobre os perigos para a informação da organização.



O propósito do processo de tratamento de riscos é diminuir os riscos que não são aceitáveis. Isso geralmente é feito pelo uso dos controles do Anexo A.

É preciso escrever um relatório de avaliação de riscos, que documente todos os passos dados durante os processos de avaliação de riscos e tratamento de riscos. Além disso, deve-se obter a aprovação dos riscos residuais, seja como um documento separado ou como parte da Declaração de aplicabilidade.

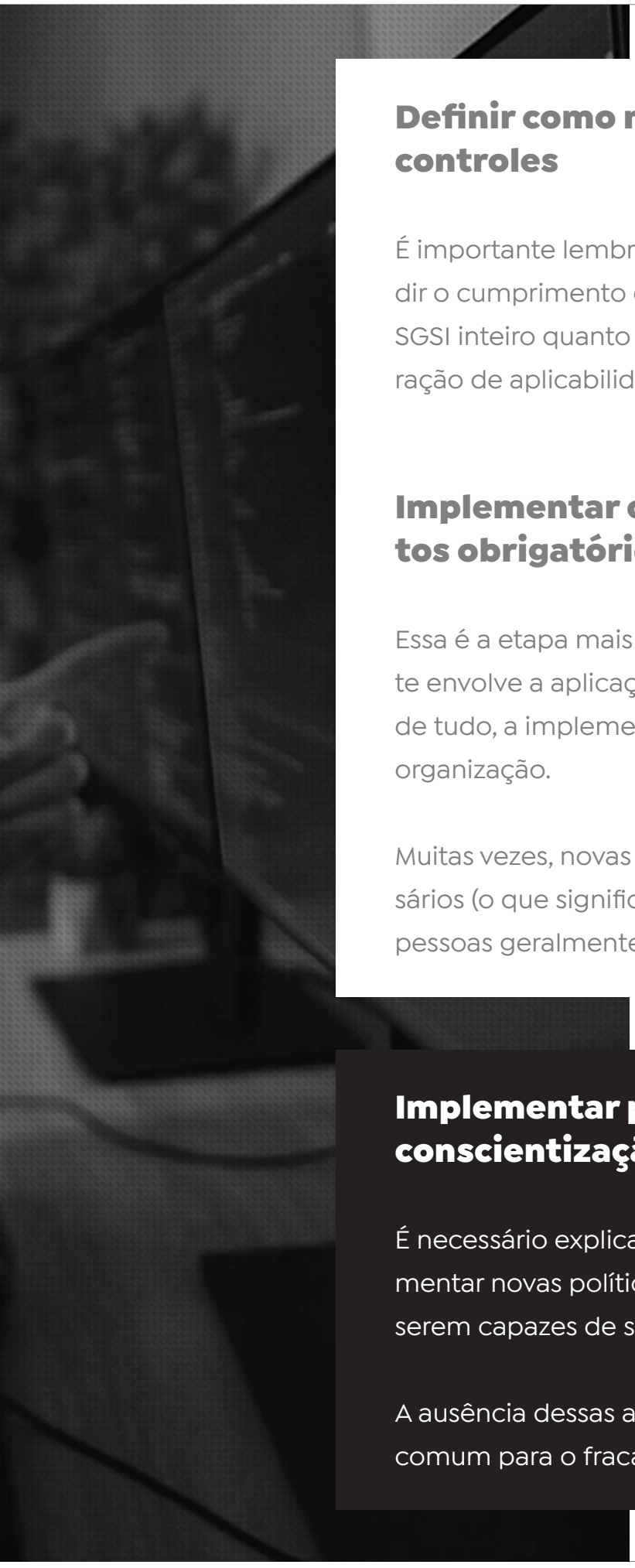
Escrever a Declaração de aplicabilidade

Depois de terminar a etapa anterior, você saberá exatamente quais controles do Anexo A precisará (há um total de 114 controles, mas provavelmente não será necessário todos eles).

Este documento tem como objetivo listar todos os controles para definir quais são aplicáveis e quais não são, e as razões para essa decisão, os objetivos a serem alcançados com os controles e uma descrição de como eles serão implementados. A Declaração de aplicabilidade também é o documento mais adequado para obter autorização da gerência para implementar o SGSI.

Elaborar o Plano de tratamento de riscos

O objetivo do plano de tratamento de riscos é definir exatamente como os controles do SoA devem ser implementados. Esse documento é um plano de implementação focado em seus controles.



Definir como medir a eficiência dos controles

É importante lembrar de definir a forma como você irá medir o cumprimento dos objetivos que definiu, tanto para o SGSI inteiro quanto para cada controle aplicável na Declaração de aplicabilidade.

Implementar os controles e procedimentos obrigatórios

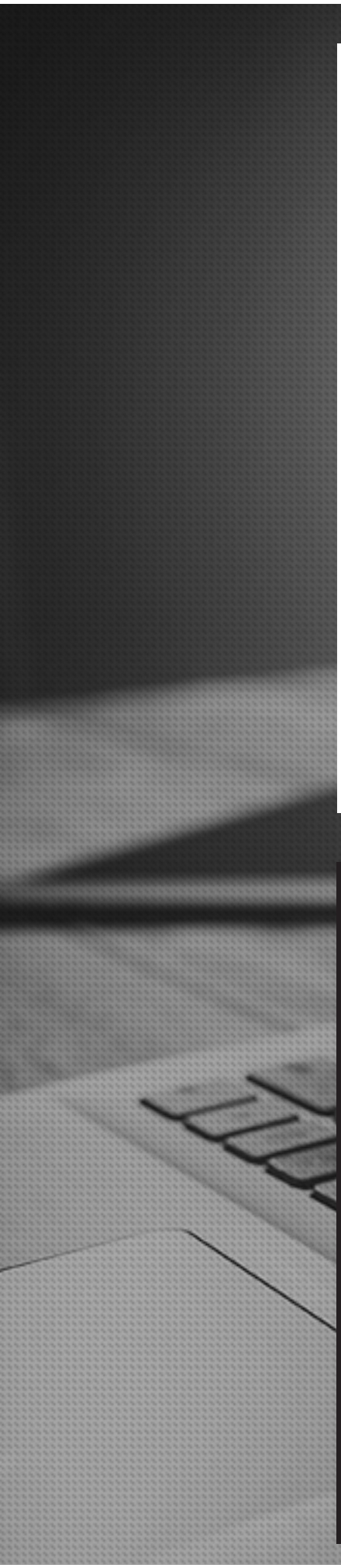
Essa é a etapa mais arriscada do projeto. Ela normalmente envolve a aplicação de novas tecnologias, mas acima de tudo, a implementação de novos comportamentos na organização.

Muitas vezes, novas políticas e procedimentos são necessários (o que significa que uma mudança é necessária), e as pessoas geralmente resistem à mudança.

Implementar programas de treinamento e conscientização

É necessário explicar a equipe porque é necessário implementar novas políticas e procedimentos e treiná-los para serem capazes de seguir o planejamento.

A ausência dessas atividades é a segunda razão mais comum para o fracasso do projeto da ISO 27001.



Operar o SGSI

Essa é a etapa em que a ISO 27001 se torna uma rotina diária dentro da organização. Devem se realizar registros, pois sem registros, será muito difícil provar que qualquer atividade foi realmente executada. Os registros devem ajuda-lo, pois com eles é possível monitorar o que está acontecendo.

Monitorar o SGSI

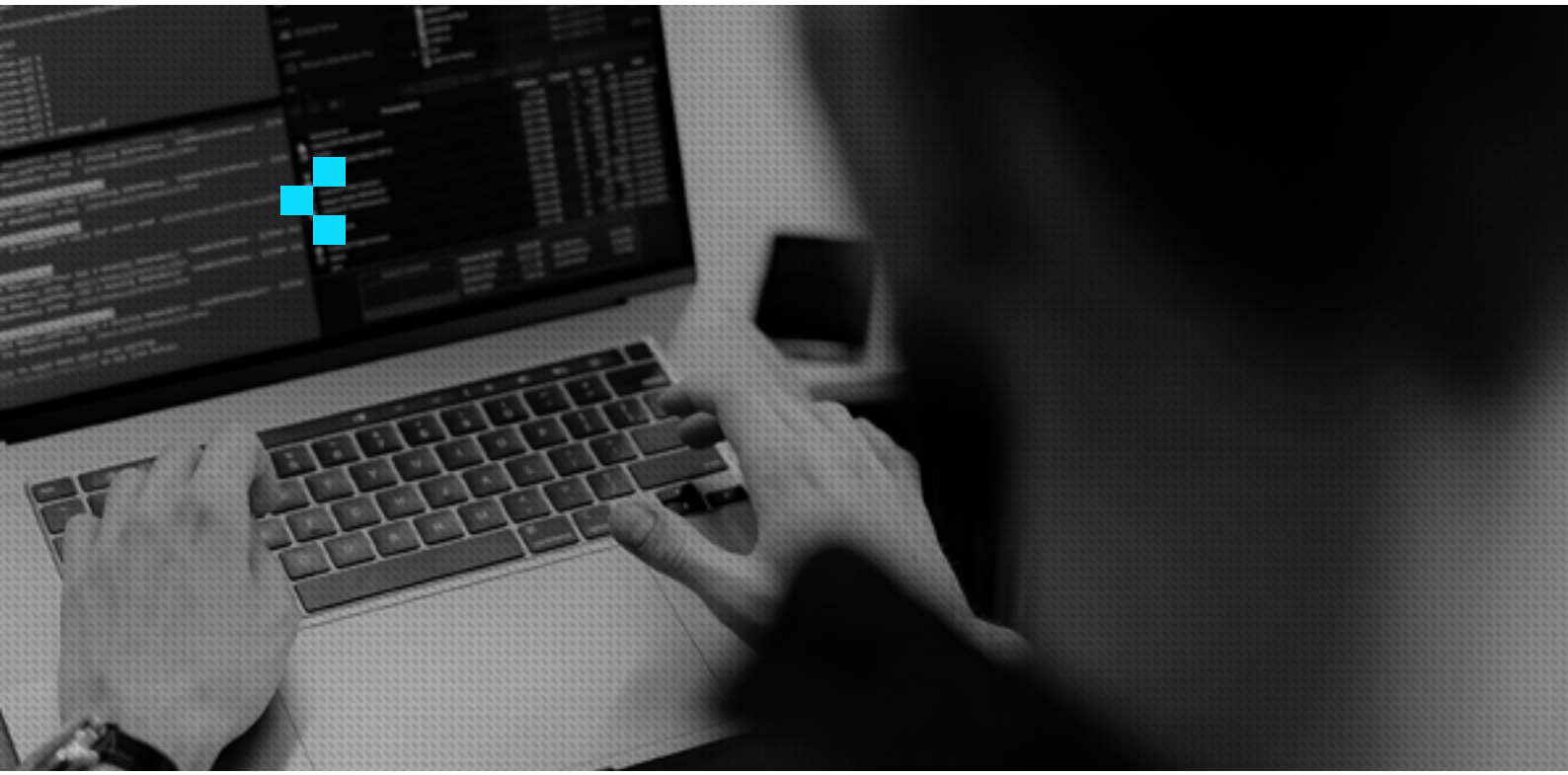
Nessa etapa, os objetivos para seus controles e metodologias de medição se unem, e você tem que verificar se os resultados obtidos estão alcançando o que foi definido em seus objetivos. Caso não estejam, é necessário executar ações corretivas e/ou preventivas.

Realizar auditoria interna

Desconhecer problemas existentes ou possíveis pode prejudicar sua organização. Portanto, é necessário realizar auditorias internas para descobrir possíveis problemas. O objetivo é tomar ações corretivas e preventivas.

Executar análise crítica da gestão

A gerencia deve saber o que está acontecendo no SGSI, se todos realizaram suas funções, se o SGSI está obtendo os resultados desejados, etc. Com base nisso, a gerencia deve tomar algumas decisões cruciais.



Ações corretivas e preventivas

O objetivo dessa etapa é assegurar que todas as inconformidades sejam corrigidas e de preferência prevenidas.

Portanto, a ISO 27001 exige que as ações corretivas e preventivas sejam realizadas de forma sistemática, o que significa que a causa básica de uma inconformidade deve ser identificada e, então, resolvida e verificada.

Documentação obrigatória para a ISO 27001

A ISO 27001 requer que a seguinte documentação seja escrita:

- Escopo do SGSI (cláusula 4.3)
- Política de segurança da informação e objetivos (cláusulas 5.2 e 6.2)
- Metodologia de avaliação de risco e de tratamento de risco (cláusula 6.1.2)

_ Declaração de aplicabilidade (cláusula 6.1.3 d)
_ Plano de tratamento de risco (cláusulas 6.1.3 e e 6.2)
_ Relatório de avaliação de risco (cláusula 8.2)
_ Definição de papéis e responsabilidades de segurança (cláusulas A.7.1.2 e A.13.2.4)
_ Inventário de ativos (cláusula A.8.1.1)
_ Uso aceitável dos ativos (cláusula A.8.1.3)
_ Política de controle de acesso (cláusula A.9.1.1)
_ Procedimentos operacionais para a gestão de TI (cláusula A.12.1.1)
_ Princípios para projetar sistemas seguros (cláusula A.14.2.5)
_ Política de segurança para fornecedores (cláusula A.15.1.1)
_ Procedimento para gestão de incidente (cláusula A.16.1.5)
_ Procedimentos de continuidade do negócio (cláusula A.17.1.2)
_ Requisitos estatutários, regulatórios e contratuais (cláusula A.18.1.1)

E estes são os registros obrigatórios:

_ Registros de treinamento, habilidades, experiência e qualificações (cláusula 7.2)
_ Resultados de monitoramento e medição (cláusula 9.1)
_ Programa de auditoria interna (cláusula 9.2)
_ Resultados de auditorias internas (cláusula 9.2)
_ Resultados de análises críticas pela direção (cláusula 9.3)
_ Resultados de ações corretivas (cláusula 10.1)
_ Registros (logs) de atividades de usuários, de exceções e de eventos de segurança (cláusula A.12.4.1 e A.12.4.3)

Claro, uma organização pode decidir escrever documentos de segurança adicionais se considerar necessário.

Como uma organização pode obter a certificação ISO 27001?

Para obter a certificação IS0 27001, após passar pelas etapas de implementação, a empresa deve se submeter a uma auditoria externa de certificação através de uma organização credenciada.

Essa auditoria possui os seguintes estágios:

Estágio 1 (Análise de lacunas)

É o estágio onde os auditores verificam se os procedimentos e controles da ISO 27001 foram desenvolvidos. A entidade certificadora compartilha os resultados e, se caso for identificada alguma lacuna, poderá ser sanada.

Estágio 2 (Avaliação Formal)

Se todas as exigências sido cumpridas, a entidade certificada inicia o 2º estágio que consiste em avaliar a implementação dos procedimentos e controles de sua empresa para certificar que eles estão funcionando efetivamente conforme a certificação exige.

Geralmente os auditores realizam uma visita no local para auditar se todas as atividades da organização estão em conformidade com a ISO 27001 e com a documentação analisada previamente.

Visitas de supervisão

Após emissão do certificado ISO/IEC 27001, e durante sua validade, a organização receberá visitas regulares dos auditores para garantir que seu sistema de gestão não apenas permaneça em conformidade, mas que também melhore continuamente.

Seja através da implementação e certificação da ISO-27001 em sua empresa ou a utilização das melhores práticas, softwares e soluções de segurança, o fundamental é compreender que manter seus dados seguros precisa ser uma prioridade.

A OSTEC oferece consultoria ISO 27001, para saber mais, entre em contato com um de nossos especialistas.

CONTINUE LENDO

SE VOCÊ GOSTOU DO ASSUNTO E GOSTARIA DE NOVAS LEITURAS, FIQUE A VONTADE PARA CONSULTAR ATRAVÉS DOS LINKS ABAIXO TEMAS RELACIONADOS EM NOSSO PORTAL.

VOCÊ SE INTERESSOU PELO CONTEÚDO?

ESCLAREÇA SUAS DÚVIDAS COM ESPECIALISTAS NO ASSUNTO

CONVERSE COM ESPECIALISTA


facebook.com/ostec


linkedin.com/company/ostec-business-security


contato@ostec.com.br


www.ostec.com.br


ostec.blog/

ostec
Segurança digital de resultados