Instituto Infnet

Segurança da Informação

FABIANO GISBERT

Etapa 05

Controles

Segurança

Máximas da Segurança da Informação

Alguns pontos são importantes determinar, e a empresa deve sempre tê-los em mente:

- O que deve ser protegido?
- Contra o que será necessário proteger?
- Como será feita a proteção?

Controles de Segurança

Instituto Infnet

Controles

CONTROLE é um mecanismo que possibilita a redução de uma determinada vulnerabilidade de um ativo de informação.

Controles de Segurança

Instituto Infnet

Alcance do Controle

É necessário determinar que nível de segurança é mais adequado para as organizações, bem como avaliar a questão custo X benefício.

Ou seja, se o custo da implementação de um sistema de segurança justifica os benefícios obtidos com a proteção dos ativos tratados.

Tendo em foco, onde se quer chegar, o objetivo principal ao implementar controle de segurança é a redução da probabilidade de ocorrência de incidentes de segurança.

Controles de Segurança

Instituto Infnet

Controles

A palavra controle define o domínio de fiscalizar e administrar determinada coisa; ter o controle da situação é dominar ou ter influencia sobre o que está acontecendo. Condições essenciais para qualquer sistema de segurança.

O objetivo maior do controle de segurança é o de prover segurança aos ativos da organização, possibilitar o correto uso dos recursos disponíveis e contribuir para o atingimento dos objetivos estratégicos da organização.

De forma geral, o controle de segurança faz parte da estratégia de segurança da organização, é voltado para mitigar riscos e manter a conformidade com requisitos legais, normativos, contratuais e internamente desenvolvidos.

Controles de Segurança

Instituto Infnet

Funções dos Controles de Segurança

Os controles de segurança podem ter funções diferentes e complementares dentro de um sistema integrado de segurança, que podem ser as funções de:

Dissuadir: refere-se a ideia de que a possibilidade de ser descoberto, detido e sofrer eventual punição dissuadirá as pessoas de cometer infrações e crimes. Está relacionado a capacidade que a segurança tem de detectar e responder a violações de segurança;
Dificultar: refere-se a capacidade da segurança de tornar tão difícil o acesso do invasor ao bem protegido, a ponto de causar desistência da intenção do acesso não permitido;
Detectar: refere-se a capacidade da segurança de identificar e dar alarme sobre uma tentativa de violação de segurança. A detecção da intenção criminosa em sua faze inicial permite uma pronta resposta mais eficiente;
Responder: refere-se aos procedimentos, meios e condições de responder e conter a uma violação de segurança, no menor tempo possível, reduzindo seu impacto ao bem protegido;
Recuperar: evolve ações para recuperação da normalidade na organização após a violação de segurança e sua contenção.

Controles de Segurança

Instituto Infnet

Categorias de Controles

Os controles de segurança em computadores é frequentemente dividida em três categorias principais:

- Físicos
- Técnicos ou Lógicos
- Administrativos

Controles de Segurança

Instituto Infnet

Controles Físicos

O controle físico é a implementação de medidas de segurança em uma estrutura definida usada para deter ou evitar acesso não autorizado a material delicado. Alguns exemplos de controles físicos:

- Câmeras de vigilância de circuito fechado;
- Sistemas de alarme térmicos ou de movimento;
- Guardas de segurança;
- Identidades com foto;
- Portas de aço trancadas com fechaduras eletrônicas;
- Biométrica (inclui impressão digital, voz, rosto, íris, manuscrito e outros métodos automatizados usados para reconhecer indivíduos).

Controles de Segurança

Instituto Infnet

Controles Técnicos

O controle técnico utiliza a tecnologia como base para controlar o acesso e o uso de dados delicados através de uma estrutura física e através de uma rede. Os controles técnicos têm um escopo de grande alcance e incluem tecnologias como:

- Criptografia;
- Cartões inteligentes;
- Autenticação de rede;
- Listas de controle de acesso (Access control lists - ACLs);
- Software de auditoria de integridade de arquivos.

Controles de Segurança

Controles Administrativos

Os controles administrativos definem os fatores humanos da segurança. Envolvem todos os níveis de pessoal em uma empresa e determinam quais usuários têm acesso a quais recursos e informações, através dos seguintes meios:

- Treinamento e conscientização;
- Preparação para desastres e planos de recuperação;
- Recrutamento de pessoal e estratégias de separação;
- Registro e avaliação de pessoal.

Controles de Segurança

Instituto Infnet

Tipos de Controle

Controles de Segurança de Detecção: Detectam desvios da normalidade e alertam e registram esta ocorrência. Aqui o evento de risco aconteceu mas o gestor é alertado para as devidas tomadas de ações corretivas.

Exemplos de controles de detecção:

- Sensores de presença, sísmicos, ruído, temperatura, incêndio, etc.;
- Sistema de Videomonitoramento;
- Vigilância patrimonial;

Controles de Segurança

Instituto Infnet

Tipos de Controle

Controles de Segurança Preventivos: O controles preventivos são os controles usados com o objetivo de evitar/impedir a violação de segurança. Refere-se ao conjunto de atividades e medidas que, feitas com antecedência, busca evitar uma ocorrência ou um dano maior.

Exemplos de controles preventivos:

- Avaliações e tratamento de riscos;
- Planos de segurança;
- Procedimentos de segurança;
- Contratação de seguro;

Controles de Segurança

Instituto Infnet

Tipos de Controle

Controles de Segurança Corretivos: Os controles corretivos incluem quaisquer medidas tomadas para para o interromper o evento indesejado e reparar danos ou restaurar recursos e capacidades ao seu estado anterior após uma atividade não autorizada ou indesejada.

Exemplos de controles corretivos:

- Plano de contingência;
- plano de gerenciamento de incidentes;
- Plano de emergência contra incêndio;
- Plano de recuperação de desastres;

Controles de Segurança

Instituto Infnet

Objetivos de Controle

- Preventivo: Evita que incidentes ocorram;
- Desencorajador: Tem como objetivo inibir a prática de ações inadequadas;
- Limitador: Diminuí danos causados;
- Monitorador: Monitora estado e funcionamento;
- Detector: Detecta a ocorrência de incidentes;
- Reativo: Reage a determinados incidentes;
- Corretivo: Repara falhas exploradas;

Controles de Segurança

Instituto Infnet

Aplicação

A aplicação de controles de segurança deve ser realizada em camadas. Não existe um único controle de segurança que atenda a todas as necessidades de segurança envolvidas na proteção de uma ativo.

A Segurança em camadas é o modelo de combinação de vários controles de segurança para proteção, envolve aplicação de diversas camadas de segurança em torno do ativo a ser protegido. É um dos princípios básicos da segurança.

As camadas incluem controles administrativos, técnicos e físicos, integrados e trabalhando em conjunto. Existem vários tipos de controles de segurança e todos eles precisam trabalhar juntos.

Controles de Segurança

Instituto Infnet

Aplicação

A aplicação de controles de segurança deve ser realizada em camadas. Não existe um único controle de segurança que atenda a todas as necessidades de segurança envolvidas na proteção de uma ativo.

A Segurança em camadas é o modelo de combinação de vários controles de segurança para proteção, envolve aplicação de diversas camadas de segurança em torno do ativo a ser protegido. É um dos princípios básicos da segurança.

As camadas incluem controles administrativos, técnicos e físicos, integrados e trabalhando em conjunto. Existem vários tipos de controles de segurança e todos eles precisam trabalhar juntos.

Controles de Segurança

Instituto Infnet

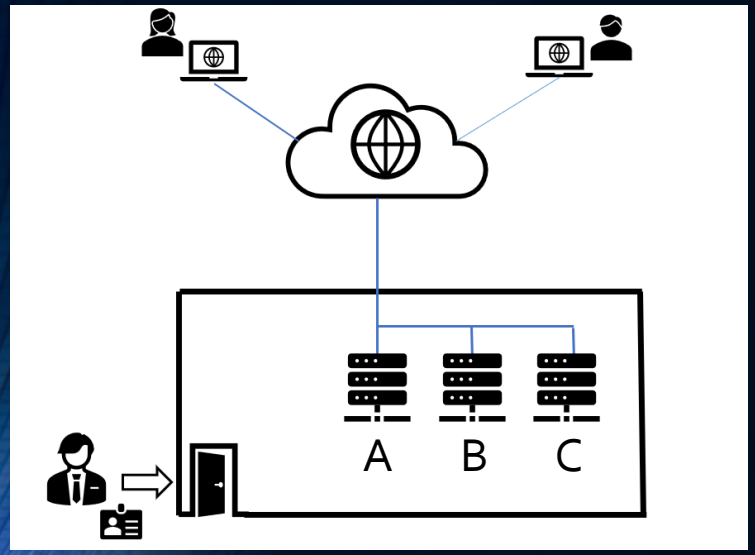
Aplicação

- O que deve ser protegido?
- Qual serviço deve ser garantido?
- Contra qual ameaça?
- Qual o objetivo da proteção?
- Quem usa a informação/serviço?
- Qual a verba disponível?
- Qual a importância dos riscos para o ativo?

Controles de Segurança

Instituto Infnet

Estudo de Caso



Servidor A – Operações Financeiras Online (CORE)
Servidor B – Base de dados dos clientes
Servidor C – Conteúdo de Comunicação e Marketing

Externo: Diretoria, Gestores financeiros e clientes
Interno: CEO, Administradores, Suporte

- Considere Custo de implementação vs impacto (custo x benefício);
- Considere os aspectos Físicos, Lógicos e Administrativos;
- Proteja as finanças e a imagem da organização;
- Considere aspectos legais, comportamentais, culturais.

Controles de Segurança

Instituto Infnet

Estudo de Caso (DICAS)

- Acessos físicos e lógicos;
- Meios de acesso a informação;
- Meios de comunicação da informação;
- Meios de armazenamento da informação;
- Meios de processamento de informação;
- Criptografia é necessária?
- Pessoas envolvidas(internas e externas);
- Política de salvaguarda da informação;
- Contingência operacional;
- Conscientização, comunicação e treinamento.

ISO 27001

ISO 27001

O que é

A ISO 27001 é uma norma internacional publicada pela International Standardization Organization (ISO) e descreve como gerenciar a segurança da informação em uma organização

A norma ISO 27001 é o padrão e a referência Internacional para a gestão da Segurança da informação, assim como a ISO 9001 é a referência Internacional para a certificação de gestão em Qualidade.

Ela também possibilita que organizações obtenham certificação, o que significa que um organismo certificador independente confirmou que uma organização implementou a segurança da informação em conformidade com a ISO 27001.

ISO 27001

Histórico

A primeira versão desta norma foi publicada em 2005, e foi desenvolvida com base na Norma Britânica BS 7799-2. A ISO 27001 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grandes.

A norma ISO 27001 tem vindo, de forma continuada, a ser melhorada ao longo dos anos e deriva de um conjunto anterior de normas, nomeadamente a ISO 27001 e a BS7799 (British Standards).

A sua origem remota na realidade a um documento publicado em 1992 por um departamento do governo Britânico que estabelecia um código de práticas relativas à gestão da Segurança da Informação.

Ao longo dos anos, milhares de profissionais contribuíram com o seu know-how e experiência para o estabelecimento de um Standard estável e maduro, mas que certamente continuará a evoluir ao longo dos tempos.

Ela é escrita pelos melhores especialistas mundiais no campo de segurança da informação e provê metodologia para a implementação da gestão da segurança da informação em uma organização.

ISO 27001

Propósito

O foco da ISO 27001 é proteger a confidencialidade, integridade e disponibilidade da informação de uma organização.

A norma tem como principio geral a adoção pela organização de um conjunto de requisitos, processos e controles com o objetivo de mitigarem e gerirem adequadamente o risco da organização.

Identificar quais potenciais problemas podem ocorrer com a informação (avaliação de risco), e definir quais necessidades devem ser atendidas para prevenir tais problemas de ocorrerem (mitigação de risco ou tratamento de risco).

A adoção da norma ISO 27001 serve para que as organizações adotem por um modelo adequado de estabelecimento, implementação, operação, monitoração, revisão e gestão de um Sistema de Gestão de Segurança da Informação.

ISO 27001

Estrutura de Atuação

A principal filosofia da ISO 27001 é baseada na gestão de riscos: descobrir onde os riscos estão, e então trata-los sistematicamente.

As salvaguardas (ou controles) que são implementadas em geral estão na forma de políticas, procedimentos e implementações técnicas (i.e. software e equipamento)

ISO 27001

Instituto Infnet

Benefícios

Conformidade com requisitos legais – A Implementação da ISO 27001 implementa metodologias que estão em conformidade com leis, regulamentações e requisitos contratuais relacionados a segurança da informação.

Obter vantagem de marketing – A certificação ISO 27001 pode proporcionar vantagem competitiva sobre concorrentes na visão de clientes que são sensíveis a questão de manter suas informações seguras.

Reduzir custos – a principal filosofia da ISO 27001 é prevenir incidentes de segurança de ocorrerem e, ao prevenir incidentes, a organização economizará uma quantidade significativa de dinheiro.

Melhor organização – tipicamente, organizações que crescem rápido não tem tempo para fazer uma pausa e definir seus processos e procedimentos – e como uma consequência, muito frequentemente os empregados não sabem o que precisa ser feito, quando e por quem.

ISO 27001

Abordagens

A segurança da informação é parte da gestão geral de riscos em uma organização, com sobreposição em áreas de cyber segurança, gestão da continuidade do negócio e gestão de TI.

A ISO 27001 permeia estas abordagens.

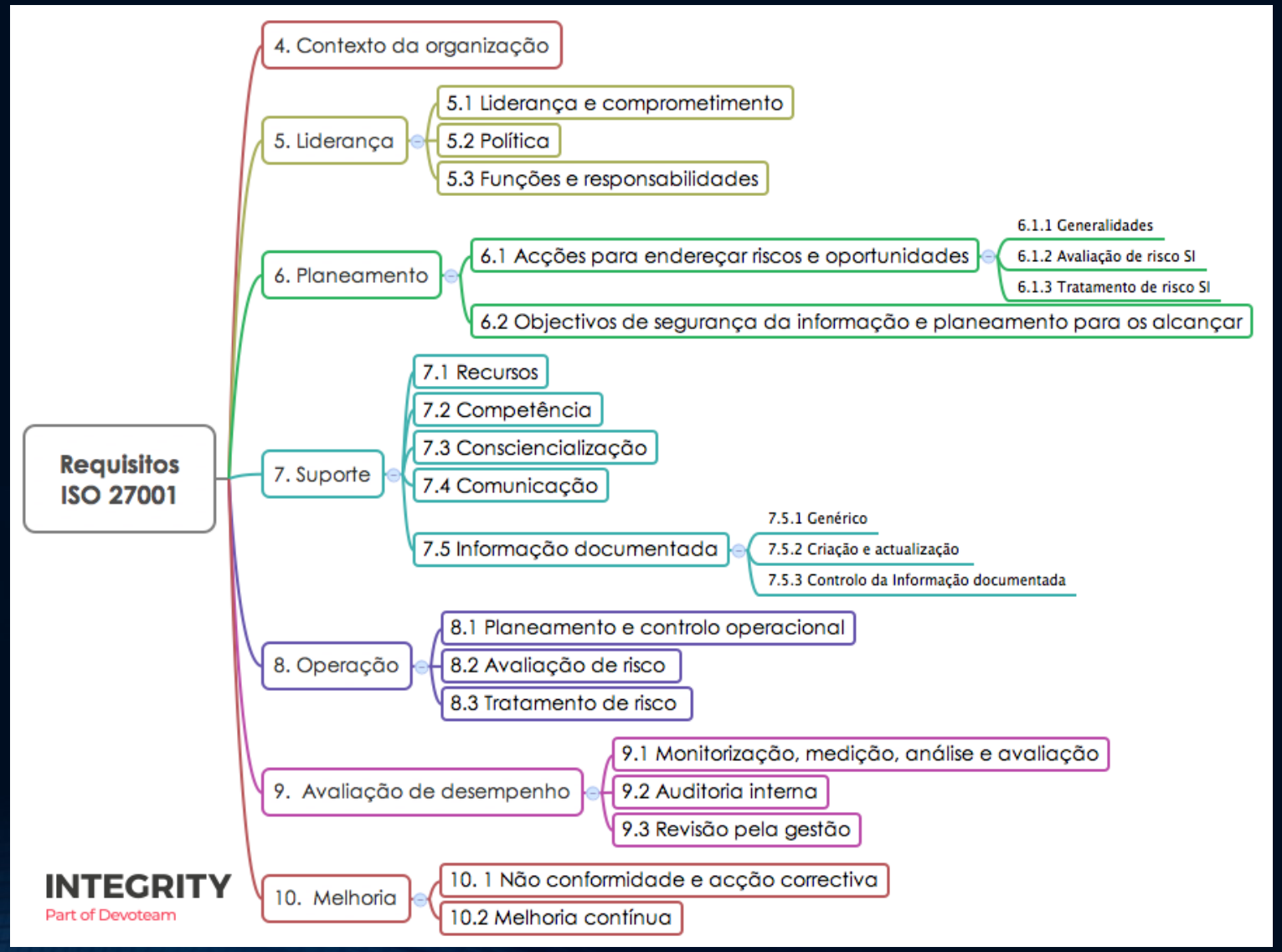
ISO 27001

Estrutura

norma padrão (Standard) ISO 27001 é composta por duas estruturas relativamente distintas:

A primeira é onde são definidas as regras e os requisitos de cumprimento da norma.

Nesta estrutura, são endereçados os aspectos explícitos no seguinte diagrama:



ISO 27001

Estrutura

A segunda estrutura da norma, é denominada de ANEXO A e é composta por um conjunto de controles que as organizações devem adotar, em diferentes temas:

ISO 27001

Instituto Infnet

Implementação

Para implementar a ISO 27001 em uma organização, é preciso seguir estas 16 etapas:

1) Obter apoio da Alta Direção
2) Utilizar metodologia de gerenciamento de projeto
3) Definir o escopo do SGSI
4) Escrever a política de segurança da informação de alto nível
5) Definir a metodologia de avaliação de risco
6) Realizar a avaliação de risco de o tratamento de risco
7) Escrever a Declaração de Aplicabilidade
8) Escrever o Plano de tratamento de risco

ISO 27001

Instituto Infnet

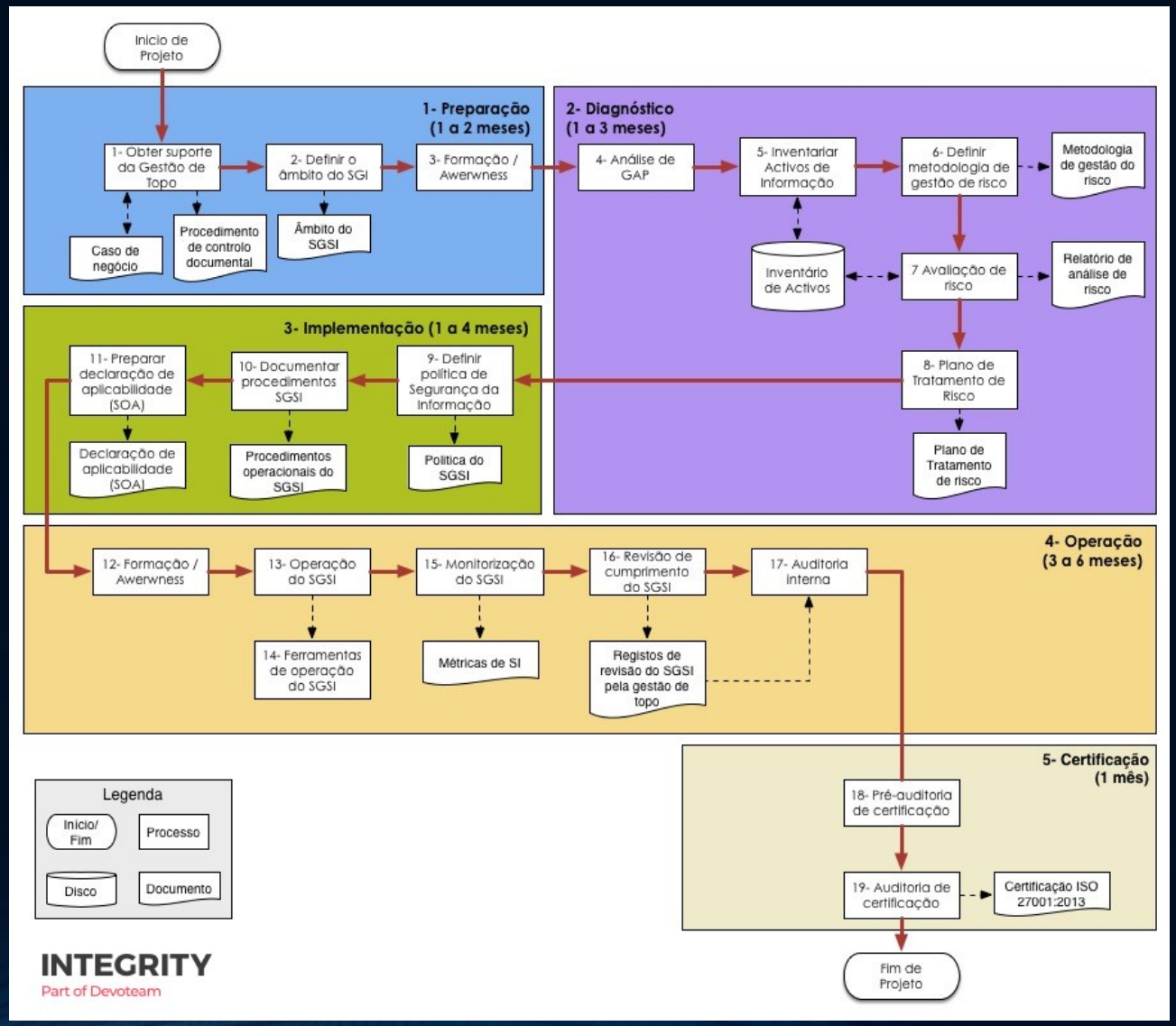
Implementação

Para implementar a ISO 27001 em uma organização, é preciso seguir estas 16 etapas:

9) Definir como medir a eficácia de seus controles e do seu SGSI
10) Implementar todos os controles e procedimentos aplicáveis
11) Implementar programas de treinamento e conscientização
12) Realizar todas as operações diárias prescritas pela documentação do seu SGSI
13) Monitorar e medir seu SGSI
14) Realizar auditoria interna
15) Realizar análise crítica pela direção
16) Implementar ações corretivas

ISO 27001

Roadmap



ISO 27001

Entregáveis

A ISO 27001 requer o estabelecimento das seguintea documentações :

- 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 e Plano de tratamento de risco (cláusula 6.1.3 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 e uso aceitável dos ativos (cláusula A.8.1.1 e 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)

ISO 27001

Entregáveis

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)

ISO 27001

Como obter a Certificação

Existem dois tipos de certificação ISO 27001:

Organização: Para obter a certificação como uma organização, ela deve implementar a norma como explicado nas seções anteriores, e então se submeter a uma auditoria de certificação realizada por um organismo de certificação.

Individual: Indivíduos podem obter certificados através de exames de certificação em entidades registradas pela ISO.

Para saber mais: https://advisera.com/27001academy/pt-br/blog/2010/12/30/como-aprender-sobre-a-iso-27001-e-a-bs-25999-2/

ISO 27002

ISO 27002

Instituto Infnet

O que é

A Norma NBR ISO/IEC 27002 faz parte de uma família de normas de Segurança da Informação, que adota um esquema de numeração usando a série de números 27000 em sequência.

Foi originada da NBR ISO/IEC 17799:2005 sem modificação do conteúdo.
É um código de boas práticas para a segurança da informação.

NÃO é uma norma voltada para fins de certificação de uma organização, pois tem uma aplicação mais restrita que a 27001

ISO 27002

Instituto Infnet

O que é

A ISO 27002 Inclui normas sobre:

- Requisitos de SGSI;
- Gestão de riscos;
- Métricas e medidas;
- Diretrizes para implementação.

ISO 27002

Instituto Infnet

ISO 27001 x ISO 27002

A Norma ISO/27001 é uma norma que trata de Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão de Segurança da Informação.

Já a norma ISO 27002 aborda a prática para Gestão de Segurança da Informação.

De forma resumida a ISO 27001 trata **dos requisitos de sistemas de gestão da informação**, a Norma ISO 27002 é um **guia que orienta a utilização de controles de segurança da informação**.

A norma ISO, dentre outras ações empresariais, apoia na evolução da Governança Corporativa das organizações.

ISO 27002

Instituto Infnet

Organização

A 27002 é organizada da seguinte forma:

- Objetivo do controle – O que deve ser alcançado;
- Controle – O que é implementado para atender o objetivo do controle;
- Diretrizes – Apresenta informações mais detalhadas para apoiar a implementação do controle;
- Informações adicionais – São informações que podem ser consideradas na implementação do controle (aspectos legais e referências a outras normas).

certificação ISO 27002

Instituto Infnet

O que é

Trata-se de uma certificação em nível “Foundation”, “Fundamentos” que provará perante o mercado e junto as empresas que você adquiriu conhecimento nos seguintes aspectos: conheceu a organização ISO e as normas ISO 27001 e ISO 27002

Avaliação:

- Conceito de informação e os requisitos da informação,
- Conceitos sobre ameaças e riscos da informação,
- Ativos da informação,
- Medidas de controle físicas e técnicas,
- Visão sobre legislação e regulamentações.

Fim da Etapa 05