Apresentação Comercial

IT ASSURANCE
SEGURANÇA & COMPLIANCE

Apresentação de Adequação de
Processos ISO/IEC 27001:2022

IT ASSURANCE
SEGURANÇA & COMPLIANCE

Um pouco **sobre nós**

A IT Assurance nasceu com o propósito de adequar e aperfeiçoar os controles de Segurança da Informação em pequenas e médias empresas.

Com um cenário tecnológico de constante evolução, a exposição à ameaças não está mais focada nas grandes corporações e as informações consideradas pessoas e/ou sensíveis são o novo tesouro mundial.

Com uma metodologia e processos didáticos, permitiremos que sua empresa adeque-se a este novo cenário e esteja em conformidade com leis regulamentares e estatutárias, garantindo boa Governança e Compliance Tecnológico.

Mantenha sua Empresa um Passo a Frente!

Nossos **Serviços**

Adequação ISO/IEC 27001:2022

Adequação que fornece diretrizes práticas para a implementação dos controles de segurança da informação estabelecidos na ISO/IEC 27001. É projetada para ajudar as organizações a selecionar, implementar e gerenciar controles de segurança da Informação.

Adequação Lei 13.709/2018 LGPD

Metodologia prática e experiência em órgãos públicos e setor privado, provendo adequação Tecnológica, Jurídica e Governança em Proteção de Dados.

Assessment e Compliance Tecnológico

Provemos análise do ambiente atual tecnológico que são componentes críticos na gestão empresarial moderna. Ajudamos as organizações a atingir seus objetivos, manter a conformidade com as regulamentações e mitigar riscos.

O que é Adequação em Tecnologia?

A ISO/IEC 27002 é uma norma internacional complementar à ISO/IEC 27001, fornecendo diretrizes práticas para a implementação dos controles de segurança da informação estabelecidos na ISO/IEC 27001. Publicada pela Organização Internacional para Padronização (ISO) e pela Comissão Eletrotécnica Internacional (IEC), a ISO/IEC 27002 é projetada para ajudar as organizações a selecionar, implementar e gerenciar controles de segurança da informação. A Adequação visa elaborar e implementar controles e processos para que a empresa certifique-se, garantindo vantagem competitiva, proteção e valor ao negócio.

Benefícios **da Adequação**

1

Adequação e Melhoria da Segurança da Informação, bem como mitigação dos Incidentes Cibernéticos e custos associados.

2

Conformidade com Requisitos Legais e Regulamentares.

3

Aumento da confiança dos clientes, investidores e partes interessadas no Negócio da Empresa.

4

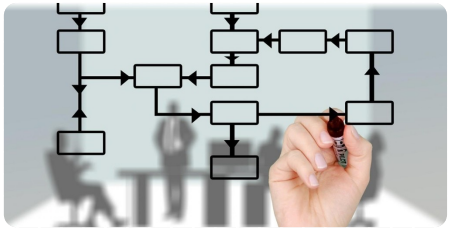
Inovação e Vantagem Competitiva

O processo de Adequação em Segurança da Informação ajuda a implementar controles eficazes para proteger as informações da Empresa, proporcionando uma referência detalhada e prática para melhorar a Segurança da Informação.

Uma Adequação bem aplicada permite a Conformidade com a ISO/IEC 27001, facilitando a Certificação, melhorando a Gestão de Riscos e aumentando a Confiança de Clientes, Investidores e outras Partes Interessadas.

Processo de Adequação

A ISO/IEC 27001 facilita a integração com outras normas de sistemas de gestão, como a ISO 9001 (gestão da qualidade). A norma especifica os requisitos para a implementação de controles de segurança com base nas necessidades da organização. Isso inclui:



Políticas e Controles de Segurança aplicáveis

Assessment do ambiente e detalhamento dos processos tecnológicos e administrativos que envolvem a operação da Empresa com base na ISO/IEC 27001.

Avaliação e Tratamento dos Riscos

Assessment, avaliação e tratamento dos riscos inerentes aos processos, provendo mitigação e documentação destes pela Alta Gestão.

Gestão de Recursos (Humanos, Técnicos e Organizacionais)

Treinamento e disseminação dos processos com as áreas e responsáveis envolvidos, mantendo o processo adequado e com melhoria contínua.

93 Controles para **Implantação**

Controles Organizacionais (37)

Os controles organizacionais são aqueles que envolvem a estrutura da organização, suas políticas, processos e práticas administrativas que suportam a segurança da Informação.

Controles de Pessoas (8)

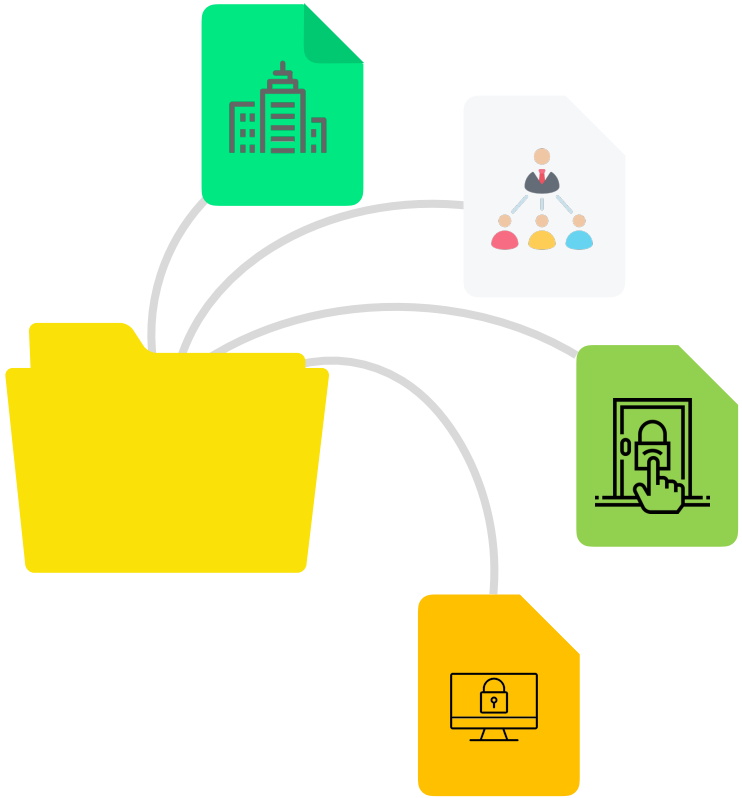
Esses controles focam nas pessoas que têm acesso e manipulam informações dentro da organização. Eles garantem que as pessoas sejam conscientes de suas responsabilidades e estejam adequadamente treinadas e monitoradas.

Controles Físicos (14)

Os controles físicos dizem respeito à proteção dos ambientes onde as informações são armazenadas e processadas, incluindo proteção contra ameaças físicas.

Controles Tecnológicos (34)

Os controles tecnológicos abrangem as medidas e ferramentas tecnológicas que ajudam a proteger a informação digital contra ameaças cibernéticas.



Controles **Organizacionais**

Segurança da Informação

Desenvolvimento de uma Política de Segurança da Informação para controle Preventivo.

Papel / Responsabilidade

Definição do Papel e Responsabilidade de cada colaborador dentro da estrutura da organização.

Segregação de Funções

Documentação de funções conflitantes visando reduzir o risco de fraude, erro e desvio de Segurança da Informação.

Responsabilidade Direção

Assegurar o entendimento da Direção na cobrança e estabelecimento de políticas específicas, bem como seu cumprimento.

Contato Autoridades

Assegurar as informações referentes à Segurança da Informação entre a organização e as autoridades legais, regulatórias e fiscalizadoras.

Contato Grupos Especiais

Contato com grupos especiais e fóruns de especialistas em Segurança da Informação para constante atualização.

Inteligência de ameaças

Informações sobre ameaças à Segurança da Informação sejam coletadas para produzir inteligência de ameaças.

Segurança em Projetos

Processo referente ao desenvolvimento e aquisição de serviços e softwares sejam integrados com Segurança da Informação

Inventário de Ativos

Inventário atualizado com proprietário do Ativo e termo de responsabilidade sobre o correto uso.

Política de Uso Ativos

Política com regras para uso aceitável de ativos e informações sobre o manuseio correto destes. Deve ser adicionado ao kit de integração.

Controles **Organizacionais**

Devolução de ativos

Termo de devolução de todos os ativos após a mudança ou encerramento da contratação. Deve ser integrado ao processo de desligamento.

Classificação de Dados

Política de classificação das informações com base na Segurança da Informação , Confidencialidade e integridade.

Rotulagem de Dados

Implantação de mecanismo de rotulagem das informações com base no nível de confidencialidade, evitando divulgação indevida.

Transferência de Dados

Política de compartilhamento de dados considerando Sharepoint, Dispositivos removíveis, e-mails e malotes. Foco na proteção e dados pessoais.

Controle de Acesso

Assegurar o acesso autorizado seja este físico ou lógico aos ativos e informações da Empresa.

Gestão de Identidade

Matriz de acesso com identificação única dos indivíduos e sistemas que acessam as informações da organização.

Dados de Autenticação

Método de autenticação que assegurará a conexão adequada e redução de falhas no processo de autenticação.

Direitos de Acesso

Processo de concessão de acesso estar de acordo com as regras de negócio e respaldados na Política de Segurança da Informação.

S.I com fornecedores

Manter via contrato um nível de segurança da informação na relação com fornecedores.

Due Diligence Fornecedor

Estabelecer e documentar a responsabilidade e recursos de Segurança da Informação junto aos fornecedores de serviços e sistemas.

Controles **Organizacionais**

Monitoramento Mudanças

Monitorar e controlar regularmente a mudança nas práticas de Segurança da Informação dos fornecedores.

Segurança em Nuvem

Processos de aquisição, uso e processamento em servidores em nuvem atendam requisitos específicos de Segurança da Informação.

Comitê de Incidentes

Processo com plano de gestão e atuação em incidentes de Segurança da Informação aprovado pelo comitê.

Avaliação Eventos de S.I

Processo que define e categorize de maneira adequada, bem como colete evidências de incidentes de Segurança da Informação.

Plano Gestão Incidentes

Plano de Gestão de Incidentes que permita uma resposta eficiente e eficaz incidentes cibernéticos.

Propriedade Intelectual

Política e Propriedade Intelectual para serviços e softwares utilizados pela Empresa.

Proteção de Registros

Proteção de registros contra perdas, destruição, falsificação e acesso não autorizado.

Proteção Dados Pessoais

Processo de identificação e proteção de dados considerados pessoais e respaldados pela LGPD (Coletas de sites, e-mails e Recursos Humanos).

Revisão Anual Processos

Revisão anual dos processos de concessão de acesso, proteção cibernética e de integração / desligamento.

Base de Conhecimento

Criação de uma base de conhecimento para suporte e consulta de informações no processo de suporte e operação.

Controles de **Pessoas**

Processo de Seleção

Verificação de antecedentes e garantia de pessoal elegível para os papéis que serão desempenhados.

Termos de Contratação

Cláusulas contratuais que declarem responsabilidades do pessoal para com a Segurança da Informação.

Treinamento em S.I

Assegurar que recebam treinamento, educação e conscientização em Segurança da Informação e cumpram com suas responsabilidades no processo.

Processo Disciplinar

Formalização de um processo disciplinar para ações contra pessoal e outras partes que cometam violação de Segurança da Informação.

Sigilo e Confidencialidade

Política que garanta as responsabilidades pelo sigilo e confidencialidade das informações durante e após o encerramento do processo de trabalho.

Trabalho Remoto

Implantação de medidas de segurança quando colaboradores estiverem trabalhando remotamente, assegurando a proteção cibernética dos dados.

Relato de Eventos em S.I

Estruturação de um canal onde a organização forneça um mecanismo para relatar eventos de Segurança da Informação.

Controles **Físicos**

Perímetros Físicos

Processos de segurança física para evitar acesso não autorizado, danos e interferências nas informações e ativos da Empresa.

Entrada Física

Processo de identificação e gestão de acesso físico com controle de logs e monitoramento.

Segurança de Instalações

Implementação de mecanismos de segurança e acesso físico em salas de reunião e demais instalações sem controle de acesso interno.

Monitoramento ambiente

Instalação e posicionamento de câmeras em locais estratégicos e considerados críticos na Empresa.

Proteção ameaças

Proteção contra ameaças físicas e ambientais, como por exemplo desastres naturais ou à infraestrutura (incêndios alagamentos e descargas elétricas).

Trabalho em Área Segura

Implantação de medidas de segurança para trabalhos em áreas externas e/ou eventos (Proxy, cases e etc).

Mesa Limpa e Tela Limpa

Políticas para mesa limpa, documentos impressos e mídias de armazenamento que podem expor dados confidenciais da Empresa.

Localização Dispositivos

Armazenamento e identificação da localização dos equipamentos ativos e de estoque provendo segurança e continuidade operacional.

Mídias de Armazenamento

Política que delimita como e quando informações serão armazenadas em mídias físicas, bem como definição do ciclo de vida.

Serviços Infraestrutura

Alta disponibilidade da infraestrutura para situações de falha elétrica, ou disrupção dos serviços de comunicação.

Controles **Físicos**

Segurança Cabeamento

Proteção dos cabos que transportam energia e dados dentro da Empresa contra interceptação, interferência ou danos.

Manutenção Dispositivos

Manutenção, atualização e armazenamento dos ativos para garantir disponibilidade, integridade e confidencialidade de informações.

Descarte Seguro

Evitar o vazamento de informações devido reutilização de equipamentos ou descarte incorreto.

Controles **Tecnológicos**

Dispositivos Endpoint

Política e recursos de proteção para endpoints utilizados pelos colaboradores (Celulares, iPADs, etc).

Acessos Privilegiados

Implementar mecanismo para assegurar que apenas usuários e softwares autorizados recebam direitos de acesso privilegiados.

Acesso a Código Fonte

Restringir o acesso a códigos fonte e gerenciar uma biblioteca de software segura, prevenindo mudanças não intencionais ou maliciosas.

Autenticação Segura

Com base na classificação de informações e sistemas privilegiados, implementar método de autenticação segura (Token, Biometria, etc).

Gestão de Capacidade

Assegurar a escalabilidade e adaptação necessária para recursos de armazenamento, internet e controle sobre Segurança da Informação.

Proteção Contra Malware

Implantação de proteção contra malware e conscientização adequada dos colaboradores.

Gestão Vulnerabilidades

Avaliação de riscos e vulnerabilidades na rede e sistemas para análise de medidas para aceite ou mitigação.

Gestão Configuração

Documentação das configurações de segurança, hardware, software, serviços e rede para revisão e a gestão de mudanças.

Exclusão Informações

Processo de exclusão de informações de sistemas da informação, dispositivos ou qualquer mídia de armazenamento quando estas não forem mais necessárias.

Mascaramento de Dados

Implantação de processo de mascaramento de dados em controles de acesso, considerando a LGPD e protegendo dados confidenciais e pessoais.

Controles **Tecnológicos**

Prevenção Vazamento

Implantação de mecanismo para monitoramento e bloqueio de vazamento de dados em serviços que transitam dados pessoais ou sensíveis.

Backup de Informações

Política de backup de informações, bem como testes regulares de restauração para situações de *Disaster*.

Redundância de Dados

Implantação de mecanismo de redundância de dados que atendam aos requisitos de disponibilidade e continuidade operacional.

Registro de Logs

Garantir o registro de logs para atividades, exceções de segurança, falhas e outros eventos, garantindo integridade e proteção destes registros.

Monitoramento Serviços

Monitoramento da rede, sistemas e aplicações para comportamentos anômalos visando identificar incidentes de Segurança da Informação.

Sincronização de Relógio

Garantir a sincronização dos relógios de servidores e sistemas para rastrabilidade e investigações sobre incidentes.

Programas Utilitários

Avaliar e garantir que sistemas que possam substituir os controles de Segurança da Informação sejam restritos e controlados.

Instalação de Softwares

Restringir a instalação de softwares por usuários e evitar a exploração de vulnerabilidades, dano à propriedade intelectual e infecção por malware.

Segurança de Redes

Avaliação das regras de Firewall, acesso Wi Fi e camadas de hardware e serviços dentro da Empresa.

Segregação de Redes

Segregação da rede em zonas de acesso e delimitação de navegação dentro do ambiente.

Controles **Tecnológicos**

Filtragem Web

Análise e revisão de acessos a sites para redução a exposição de conteúdo malicioso.

Uso de Criptografia

Implantação de chaves de criptografia para serviços e dispostivos que transitem informações pessoais ou sensíveis.

Privacy by Design

Garantir que todo novo produto, processo ou serviço esteja em conformidade com as regras de negócio e Segurança da Informação definidas.

Requisitos para Software

Garantir que os softwares e/ou sistemas desenvolvidos / adquiridos atendam as regras de Segurança da Informação.

Codificação Segura

Assegurar que serviços desenvolvidos, como por exemplo Power B.I tenham recursos de Segurança da Informação aplicados.

Testes de Segurança

Realização de testes de segurança para implantação de novos processos ou serviços dentro da Empresa.

Desenvolv. Terceirizado

Garantir a gerenciam monitoração e análise crítica de atividades relacionadas a terceirização do desenvolvimento de sistemas.

Divisão Teste e Produção

Segregação do ambiente para testes no processo de desenvolvimento de serviços. O ambiente precisa ser separado e protegido.

Registro Planos de Teste

Desenvolvimento de modelos de teste para implantação de processos, serviços e sistemas.

Envolvimento Gestão T.I

Envolvimento direto da Gestão de Tecnologia em todos os processos que envolvam mudanças em serviços, processos e/ou sistemas.

Metodologia **Processo de Auditoria**

1

Assessmente Geral e Análise SoA

Assessment do SoA
Triskle GRC Checklist
Recebimento de Políticas e Processos
Entrevistas

2

Auditoria Remota

Análise dos Processos e documentações recebidas;
Leitura e compreensão SoA

3

Auditoria Presencial

Validação da aplicação dos Processos e Políticas;
Retorno entrevistas e coleta de evidências

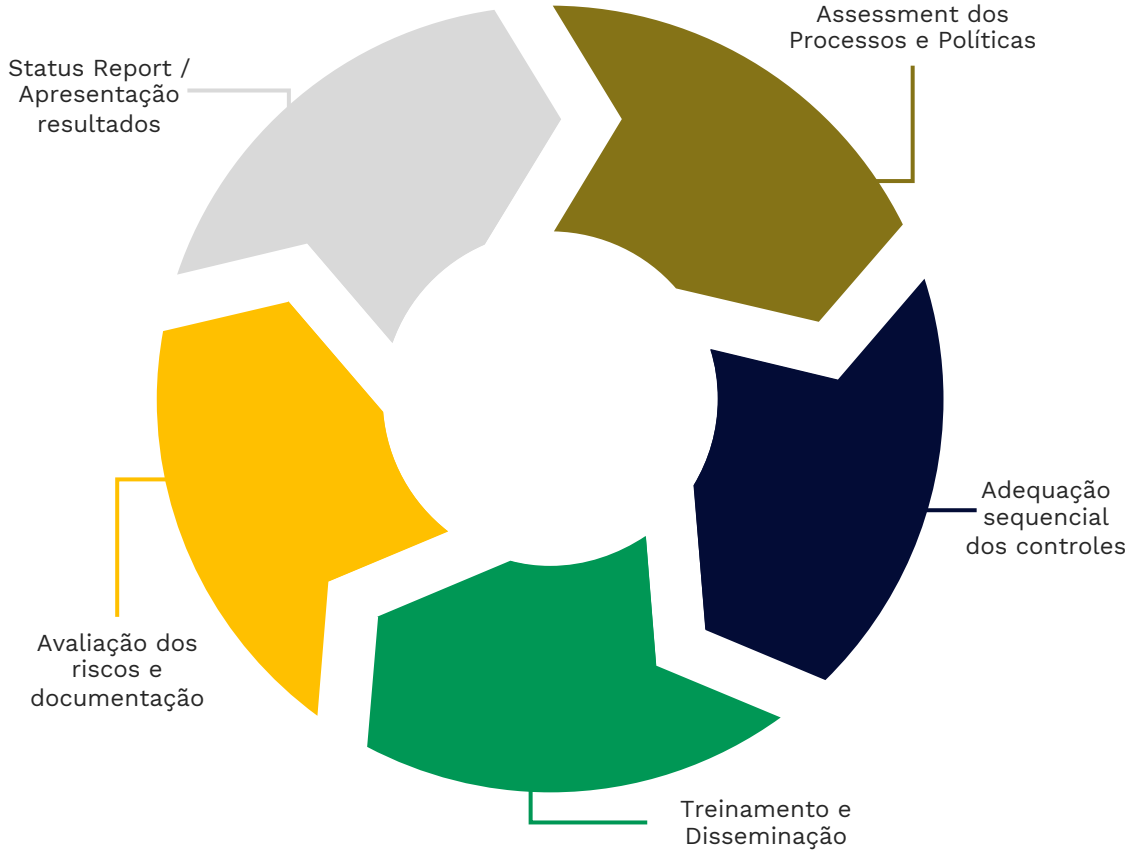
4

Relatório de Conclusão

Análise dos Documentos e relatório de Conformidade.

Metodologia **do Processo de Implantação**

Trabalharemos com 5 etapas macro do processo de adequação onde estas se interligam para conclusão do ciclo do projeto.



Agenda e **Envolvidos**

AGENDA

A Auditoria dos processos envolve um total aproximado de 93 documentos baseados no SoA que possivelmente serão desmembrados em **x** meses de projeto, considerando as 4 etapas da Metodologia.

ENVOLVIDOS

- Gestão Administrativa / Governança;
- Gestão de Sistemas;
- Gestão de Facilities;
- Gestão Operacional e Tecnológica;
- Gestão Recursos Humanos;
- Gestão Jurídica.

Comprovação **Técnica**

Rodrigo Fructos Lima

Bacharel em Ciência da Computação pela Universidade Nove de Julho, MBA em Gestão de Projetos com Ênfase no PMI pelo IBTA, Pós Graduado em Governança de T.I e Especialista em Segurança da Informação pela Anhembi Morumbi, realizei a gestão de programas e portfólios em empresas do Brasil e América Latina (Implantações de Sedes, Filiais, Projetos de Infraestrutura e Adequação de Processos em Órgãos Públicos e Setor Privado.

Certificações: Lead Auditor, ISO/IEC 27001 e 27002, 27001, 27002, 27005, 27007, 37301, ITIL V3, Ethical Hacking, Cyber Security, Computer Security Incident Response Team (CSIRT) e Elaboração de Planos em Segurança da Informação pela FGV.

IT ASSURANCE
SEGURANÇA & COMPLIANCE

Outras **considerações**

- Recursos Tecnológicos e soluções adicionais não estão inclusos na proposta;
- O prazo para conclusão da adequação dependerá da agenda dos envolvidos e acesso às informações necessárias;
- Todas as entregas serão apresentadas em reuniões de Status Report com os envolvidos.

Contate-nos

Endereço

Avenida Paulista, 1471, CJ 511- Bela Vista

Horário

Segunda à Sexta Feira das 08h às 17h

E-mail

rodrigo.lima@itassurance.com.br

Telefone

(11) 9 6317-8427

Instagram

@itaassurance

Website

https://www.itassurance.com.br

Obrigado!

IT ASSURANCE
SEGURANÇA & COMPLIANCE