Manual de Segurança da Informação

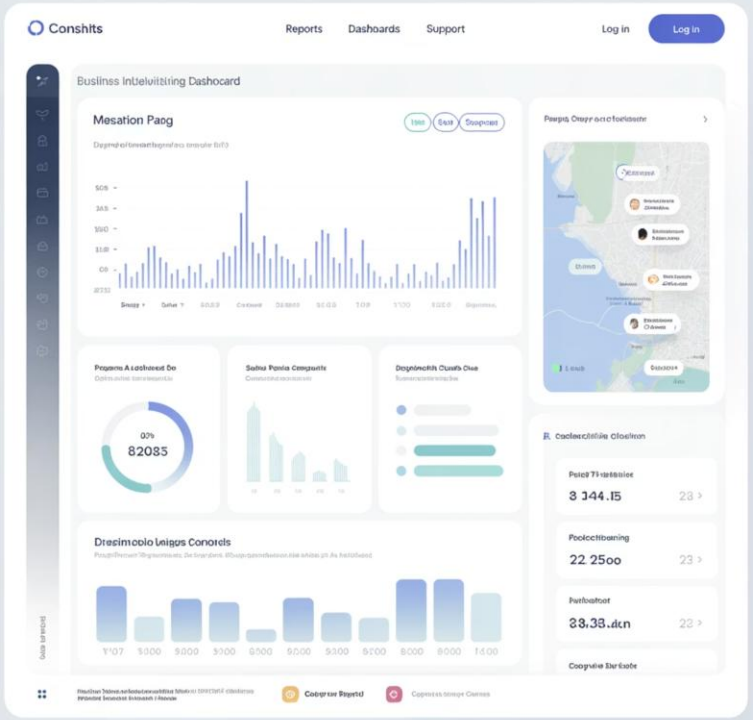
Segurança da Informação

O MA-001 – Manual de Segurança da Informação da Toccato LTDA foi elaborado com base nos requisitos da norma internacional ISO/IEC 27001:2022, que define os parâmetros para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI). Este documento reflete o compromisso institucional da Toccato com a proteção de seus ativos de informação, alinhando-se também às exigências legais da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e demais normativos nacionais e internacionais pertinentes.

Apresentação

A Toccato, como empresa referência na implementação de soluções de Business Intelligence com foco em Produtos Qlik, reconhece a segurança da informação como pilar estratégico para garantir a confiabilidade dos seus serviços, a integridade dos dados tratados e a confiança de seus clientes, parceiros e colaboradores.

Este manual é parte integrante do Programa de Conformidade em Segurança da Informação e serve como documento orientador para os colaboradores, parceiros, prestadores de serviço e demais partes interessadas.



Objetivos e Abrangência

Objetivo Geral

Definir, sistematizar e documentar as diretrizes, práticas, controles e responsabilidades que regem a proteção das informações da Toccato LTDA, em conformidade com os requisitos estabelecidos pela ISO/IEC 27001:2022.

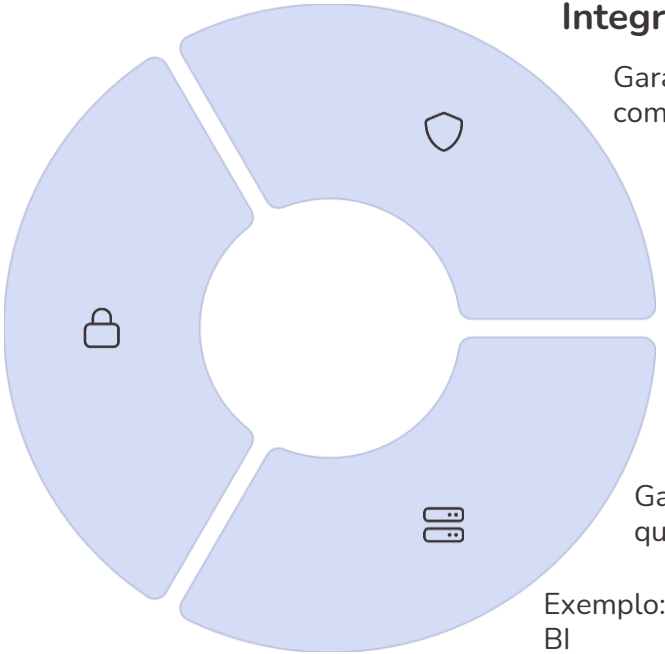
Objetivos Específicos

Estabelecer princípios fundamentais de segurança, garantir confidencialidade, integridade e disponibilidade dos ativos, promover cultura de segurança institucional e delimitar responsabilidades dos envolvidos.

Abrangência

Aplica-se a todas as unidades, colaboradores, equipamentos de TI, ambientes virtuais e em nuvem, informações corporativas, processos institucionais, documentos internos e terceiros com acesso autorizado.

Fundamentos e Referenciais Normativos



Integridade

Garantia de que a informação é precisa, completa e não foi alterada indevidamente

Exemplo: Logs de auditoria em relatórios e sistemas

Confidencialidade

Garantia de que a informação é acessível apenas a pessoas autorizadas

Exemplo: Controle de acesso por perfis no BI e rede

Disponibilidade

Garantia de que a informação estará acessível quando necessária

Exemplo: Backup em nuvem e alta disponibilidade do BI

Esses princípios são complementados por outros valores organizacionais, como autenticidade, rastreabilidade e responsabilidade, alinhados às normas ISO/IEC 27001:2022, ISO/IEC 27002, ISO/IEC 27005 e legislações como a LGPD.

Estrutura do Sistema de Gestão da Segurança da Informação

Política de Segurança da Informação

"A Toccato LTDA, em conformidade com a ISO/IEC 27001:2022 e a legislação nacional aplicável, reforça seu compromisso com a proteção da informação e com a construção de uma cultura organizacional segura, pautada pela ética, transparência, responsabilidade digital e melhoria contínua."

Missão, Visão e Valores

- Missão: Proteger as informações da Toccato e de seus clientes
- Visão: Ser referência nacional em práticas seguras
- Valores: Integridade, confidencialidade, transparência

Gestão de Riscos de Segurança da Informação

Identificação

Mapeamento de ativos, processos e ameaças aplicáveis

Análise de Riscos

Avaliação da probabilidade e impacto de eventos adversos

Avaliação de Riscos

Classificação por criticidade e priorização de tratamento

Tratamento de Riscos

Seleção de estratégias: aceitar, mitigar, transferir ou evitar

Monitoramento

Acompanhamento contínuo de indicadores, eficácia de controles e novas ameaças

A gestão de riscos é baseada nas diretrizes da ISO/IEC 27005:2022, complementada pela ISO 31000 e em conformidade com os requisitos da ISO/IEC 27001:2022, Anexo A e seus 93 controles.

Gestão de Ativos e Controles de Acesso

Inventário e Classificação

Todos os ativos relevantes ao SGSI são inventariados e classificados conforme o grau de sensibilidade, criticidade e impacto em caso de perda ou exposição.

Controle de Acesso

Os acessos aos ativos são controlados por autenticação baseada em perfis, conforme os princípios do menor privilégio e necessidade de conhecimento.

Proteção Física

A entrada nas dependências físicas críticas é restrita por crachá, biometria ou chave física controlada, com ambientes técnicos monitorados por cameras, identificação e/ou biometria.

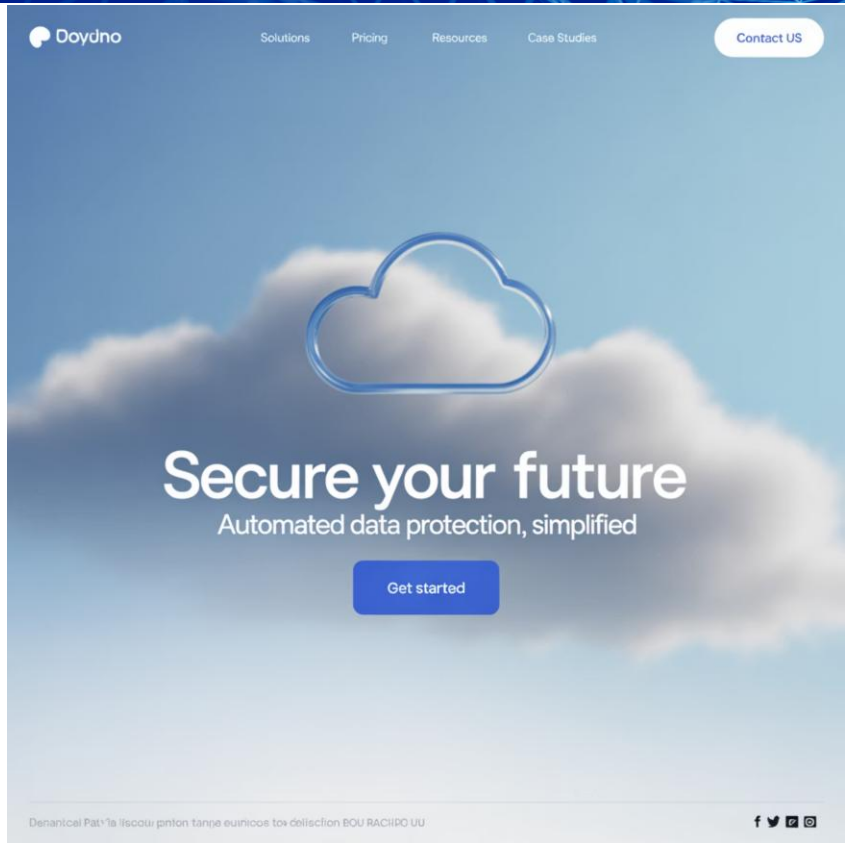
Proteção contra Malware e Continuidade Operacional

Política de Proteção contra Malware

- Antivírus corporativo com atualizações automáticas
- Filtro de navegação para sites maliciosos
- Controle de dispositivos USB
- Patch management centralizado
- Ferramentas EDR e logs de eventos atípicos

Continuidade Operacional

- Plano de Continuidade de Negócio (PCN)
- Testes e simulados semestrais
- RPO (Recovery Point Objective) de até 4h
- RTO (Recovery Time Objective) de até 8h



Gestão de Incidentes de Segurança

Detecção

Identificação por sistemas, usuários ou equipe de TI

Registro

Notificação formal via canal interno (sistema, e-mail ou formulário)

Análise

Coleta de evidências, análise de logs e impactos operacionais e legais

Resposta

Ações imediatas para conter, erradicar ou mitigar o incidente

Registro Final

Registro consolidado do incidente, lições aprendidas e plano de melhoria

A Toccato adota uma abordagem sistemática e proativa para o tratamento de incidentes de segurança da informação, em conformidade com o controle 5.25 da ISO/IEC 27001:2022.

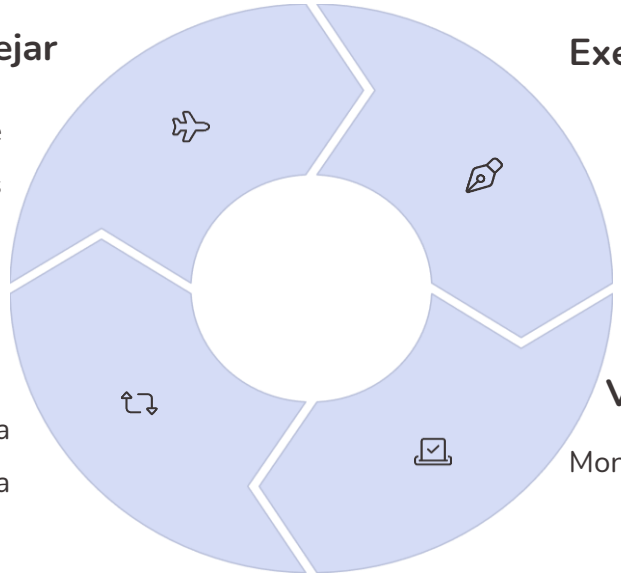
Avaliação de Conformidade e Melhoria Contínua

Planejar

Identificação da causa-raiz e planejamento de auditorias internas

Executar

Implementação de ação corretiva ou preventiva e condução de auditorias



Agir

Revisão de políticas ou processos para melhoria contínua

Verificar

Monitoramento da eficácia das ações implementadas

As auditorias internas são planejadas e conduzidas anualmente para todos os controles da ISO 27001:2022 e matriz SOA, com verificações semestrais para áreas críticas como TI, Jurídico, Compliance e Comercial.

A Toccato está apta e disposta a receber auditorias conduzidas por órgãos certificadores credenciados na ISO 27001, clientes corporativos e parceiros estratégicos.